Mapeo correlativo de incidentes de STICs en el Derecho Penal Argentino.

a) **Nombre y Apellido del Alumno**: Sergio Diego Carriquiriborde

b) **Nombre y Apellido de Director**: Dra. Lía Hebe Molinari

b')**Nombre y Apellido de Co-Director**: Lic. Paula Venosa

c)**Título del Trabajo Final**: Mapeo correlativo de Incidentes de Seguridad en las TICs (Tecnologías de la Información y la Comunicación) en el Derecho Penal Argentino.

d)**Objetivos**: 1) Investigar sobre incidentes de seguridad en las TICs y relacionarlos y/o encuadrarlos en la normativa penal vigente.-

2) Aportar una guía de intervención urgente para padres y docentes que indique cómo proceder ante un hecho de grooming y/o cyberbullying para facilitar al personal competente la obtención de evidencia para su posterior proceso.-

e) **Justificación del Trabajo**: En el **delito**[1] de pedofilia se evidencia necesidad de analizar el **contexto tecnológico** en el que se despliega una conducta delictiva vinculada a la informática a fin de poder investigarla penalmente, defender al imputado y dictar sentencia condenatoria o absolutoria. Este tema será abordado en la Introducción.

Por otro lado, la finalidad del derecho penal, consiste en prevenir el delito, disuadiendo la realización de conductas disvaliosas, a través de la imposición de una pena; y al mismo tiempo limitando el castigo del delito a la escala penal legislada. Se propone en este escrito extender la lista de mecanismos de protección (firewall, IDP, IPS, criptografía, honeypots) incluyendo al Derecho Penal como un elemento más de la Seguridad Informática, que desde una posición extrínseca a la Informática coadyuva a este objetivo de Seguridad. La existencia de penas es un elemento que desde fuera de lo propiamente informático incide en la disuasión de la realización de conductas disvaliosas que amenazan los activos informáticos y que afectan directa o indirectamente a las personas.

Desde una perspectiva subjetiva, se agrega que el autor posee un perfil de informático y abogado, con doble titulación y esta circunstancia genera el interés de llegar a una síntesis que vincule coherentemente conceptos de ambas disciplinas. La descomplejización de una multitud de tareas de la vida, a la que lleva la tecnología es compatible con el objetivo del Derecho, de lograr un orden social justo y una convivencia pacífica.

[1] **Delito: es una acción típica, antijurídica y culpable**. Típica porque tiene que estar descripta en el código penal. Antijurídica porque debe ser contraria al derecho en su totalidad (matar en legítima defensa podría no ser un delito si la defensa es proporcional al ataque). Culpable significa que debe ser reprochable al autor

I. Introducción

El tema central a investigar es la correlación entre incidentes de STICS (Seguridad en la Tecnologías de la Información y la Comunicación) y los delitos previstos en el ordenamiento jurídico nacional. Este mapeo consiste en hallar la relación o encuadre entre los incidentes de STICS y las conductas penadas en el Derecho[2] Penal[3] , es decir encontrar, en caso de existir, la calificación penal de una conducta[4] o la subsunción penal[5] de una conducta humana. Luego se clasifican los delitos de

[2]La definición de **Derecho**, es un tema de extensas reflexiones y distinciones que no son el objeto de este trabajo. No obstante se puede entender por Derecho al "conjunto de normas de conducta humana obligatorias y conformes con la justicia" (Borda, G, *Tratado de derecho Civil - Parte general* Tomo I, p. 12, Abeledo Perrot, Buenos Aires, 1987).

Otra definición clásica conceptualiza al Derecho como "Un orden coactivo, un sistema de normas que prescriben o permiten actos coactivos bajo la forma de sanciones socialmente organizadas" (Kelsen, H, *Teoría Pura del derecho*, p. 71, Eudeba, Buenos Aires, 1986). Simplificando, podemos definir al ordenamiento jurídico, como el conjunto organizado de normas emanadas de un poder estatal competente, las cuales son percibidas por la población como obligatorias (Gonzalo Iglesias, Aspectos Legales y Profesionales de la informática).

El autor de este trabajo, sugiere una definición desde una perspectiva sistémica-informática. Se podría concebir el Derecho aplicando el modelo básico de sistemas: un conjunto de Entradas, Procesos y Salidas. La entrada serían las conductas de las personas, sus intereses y necesidades. Los procesos podrían ser las interacciones entre las personas, lo que en filosofía del Derecho se denomina interferencia intersubjetiva de las acciones humanas (Cossio, C, *La teoría egológica del derecho y el concepto jurídico de libertad, Abeledo Perrot, 1964*). En estos procesos las personas satisfacen sus necesidades de bienes, valores y/o vínculos con otras personas, dentro del ámbito de lo justo. Las salidas posibles de este sistema serían los contratos entre las personas (compraventa, alquiler, etc), la imposición de penas (entendiendo que el Estado es un persona jurídica de derecho público y privado), etc.

[3] El **Derecho Penal**, que nos ocupa, es "la rama de saber jurídico que mediante la interpretación de las leyes penales, propone a los jueces un sistema orientador de decisiones que contiene y reduce el poder punitivo, para impulsar el progreso del Estado constitucional de Derecho (Zaffaroni, E, *Manual de Derecho Penal*, Ed. Ediar, 2006).

Finalidad del Derecho Penal: asume una doble función preventiva: prohíbe y pena conductas humanas enumeradas en el Código Penal, es una **prevención general de los delitos: la pena sirve para prevenir el delito** (límite mínimo de prevención), y prohíbe conductas del Estado que sean arbitrarias y desproporcionadas (límite máximo del Derecho Penal). (Síntesis extraída de Ferrajoli, L, *Derecho y Razón*, p 331, Trotta, Madrid, 1995). Este segundo fin distingue al Derecho Penal de otros sistemas de control social, como el policial o el terrorista. (ibídem Pág 335).

Lo expresado anteriormente busca responder a la pregunta ¿por qué castigar?, cuyos extremos de debate son el abolicionismo penal y el justificacionismo. Este *por qué* encierra una triple pregunta: por qué existe el fenómeno de la pena de hecho, por qué existe el deber jurídico de la pena y por qué debe existir la pena. Históricamente el Derecho Penal, nació como negación de la venganza, así la ley del Talión limitó el derecho de reacción. Posteriormente surge la prohibición de linchamientos, duelos y ejecuciones sumarias. El Derecho Penal nace cundo esta relación bilateral (ofendido / ofensor), se convierte en una relación trilateral integrando al Juez con sus leyes y precedentes.

[4]Operación de la inteligencia consistente en referir un acto, un hecho o una situación jurídica al Código Penal, Enciclopedia Jurídica, 2014, Interpretación de la Norma, 17/03/2018, http://www.enciclopedia-juridica.biz14.com/d/interpretacion-de-la-norma-juridica/interpretacion-de-la-norma-juridica.htm.

[5]Operación lógica en que se establece una dependencia entre un hecho y la ley. (Enciclopedia Juríaidca, 2014, *Calificación*, 17/03/2018, http://www.enciclopedia-juridica.biz14.com /d/calificaci%C3%B3n/calificaci%C3%B3n.htm)

acuerdo al atributo de la información que afecten. Finalmente, como aporte se realizará una guía de intervención urgente ante casos de grooming y cyberbullying.

Teniendo a la vista las nociones de seguridad informática (manejo de las vulnerabilidades y las **amenazas** que se presentan en forma de ataques a sistemas informáticos) y seguridad de la información (que busca mitigar los **riesgos** de los activos de una organización), se ve que ambas nociones[6], diferentes en su amplitud, resultan insuficientes para abordar la Informática desde el Derecho Penal. Ello es así dado que, por ejemplo, el delito de Grooming, que se explicará más adelante, no encuadra en las nociones antedichas, debido a que consiste en un ataque a una persona y no a un sistema informático, además, por otro lado, resulta indiferente si la persona pertenece o no a alguna organización.

Existe una relación entre las nociones de vulnerabilidad-amenaza-incidente a las que se agregó el concepto de riesgo en el Top 10 de vulnerabilidades del año 2010 realizado por OWASP. Se delimitan dichos conceptos a continuación tomando como referencia la RFC 2828, titulada Internet Security Glossary, May 2000 y escribiendo en letra cursiva las nociones tomadas de dicho documento.

La **amenaza** informática es una *violación potencial de la seguridad, es decir un posible peligro que podría explotar una vulnerabilidad*.

Las amenazas utilizan las **vulnerabilidades** o *debilidades de un sistema* o activo, *con el fin de producir un evento adverso que afecte o dañe al mismo*. Nótese que se habla de vulnerabilidad de activos en sentido amplio, por ejemplo la falta de capacitación del personal puede ser una vulnerabilidad.

Un **ataque** *es un acto inteligente, un intento deliberado para evadir servicios de seguridad y violar la política de seguridad de un sistema*. Las amenazas se materializan en **ataques** realizados por personas, a través de rutas o riesgos existentes en las aplicaciones informáticas, en las bases de datos, en los sistemas operativos o en la infraestructura de comunicaciones. Los ataques, en principio, son realizados por personas, solo se le puede imputar responsabilidad a una persona. Existen distintos grados de autoría de los delitos: autor primario, coautor, autor mediato o instigador, cómplice y cómplice secundario. Si bien asistimos a un proceso de despesonalización de los ataques, es decir no es una persona la que realiza el ataque propiamente dicho, subsiste la idea de la RFC 2828 de que un ataque es un acto inteligente y siempre hay una persona atrás del mismo asumiendo algún grado de autoría penal. Esto es así aun en los casos de botnets dado que hubo una persona que programó y configuró el ataque.

Se entiende por agente de **riesgo** a los caminos o rutas que los atacantes pueden potencialmente usar para realizar un daño en los activos informáticos. El riesgo e*s la expectativa o probabilidad de que una amenaza impacte en una vulnerabilidad*. En la definición de riesgo intervienen los conceptos de vulnerabilidad, amenaza, impacto y probabilidad. Por su lado, OWASP define riesgo como la probabilidad de que ocurra un

[6] SGSI, 29/12/2014, *ISO 27001: ¿Qué diferencia existe entre la seguridad informática y la seguridad de la información?,* 11/09/2017, http://www.pmg-ssi.com/2014/12/iso-27001-que-diferencia-existe-entre-la-seguridad-informatica-y-la-seguridad-de-la-informacion/.

ataque sobre una vulnerabilidad por el impacto en el negocio. La definición que establece OWASP en su glosario es la siguiente:

> *"El riesgo es la posibilidad de una ocurrencia negativa o indeseable. Hay dos partes independientes de riesgo: impacto y probabilidad. Para reducir el riesgo, uno puede reducir el impacto, reducir la probabilidad o ambos. El riesgo también puede ser aceptado (lo que significa que el impacto total del resultado negativo será asumido por la entidad en riesgo). El impacto y la probabilidad de un riesgo generalmente se combinan para crear una estimación de su Gravedad."* (Cfr. https://www.owasp.org/index.php/Glossary, 17/03/2018).

Un incidente de seguridad es un *evento adverso que afecta los activos de la organización, que viola la seguridad*. Se puede ampliar esta definición diciendo que **un incidente de seguridad es un evento adverso que afectando los activos de una organización puede causar un daño en una persona o cosa**.

Actualmente se usa el acrónimo TICs, Tecnologías de la Información y la Comunicación en el ámbito de las ciencias sociales. En particular, el autor lo comenzó a escuchar en Congreso Pedagógico Nacional de 1984 y en las capacitaciones docentes que se realizaron posteriormente. Luego este concepto ingresó en el ámbito jurídico para afincarse como nombre del nuevo **fenómeno de la convergencia** de la Informática con las Comunicaciones y de distintos servicios en un mismo dispositivo informático. (Cfr. Ley 27.078 – Ley Argentina Digital, 18/12/2014)

Teniendo en consideración lo expuesto en las definiciones que anteceden, se opta por usar la locución "**incidentes de seguridad en las TICs**" (o **incidentes de STICs**) dado que abarca todas las conductas penalmente reprochables, involucra los aspectos tecnológicos mencionados (seguridad informática y seguridad de la información, vulnerabilidad, amenaza, incidente y riesgo) y atiende a la actual convergencia legal y tecnológica entre los conceptos de información y comunicaciones. Se usará el acrónimo STICS, para referirse a esta noción. Volviendo al ejemplo del Gooming, se puede afirmar que el mismo es un incidente de seguridad que afecta a una persona por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos.

El sistema penal prevé la punición de ciertas conductas humanas desplegadas en el ámbito del quehacer informático, considerando dentro de esta disciplina la programación, el uso y acceso a sistemas y a bases de datos, la configuración y manipulación de redes y protocolos de comunicación, el uso de las comunicaciones y los programas P2P, etc. Esta previsión se dio especialmente desde el día 24 de Junio de 2008 en que se promulgó la Ley 26.388 que modifica el Código Penal incorporando **tipos penales**[7] nuevos o modificando tipos ya existentes. Este ámbito especial requiere

[7] Se entiende por **Tipo Penal** a la descripción realizada en una ley de una conducta punible descripta en el Código Penal. Es el conjunto de elementos, definidos por la ley, constitutivos de un delito. Enciclopedi Jurídica, 2014, *Tipo Penal*, 17/03/2018, http://www.enciclopedia-juridica.biz14.com/d/tipo-penal/tipo-penal.htm

Una "conducta típica" es una conducta penada explícitamente en el Código Penal. Simplificando, **cada artículo del código penal describe una o varias conductas típicas o delitos**, que son sinónimos.

por parte de los Abogados Defensores, Fiscales y Jueces un conocimiento preciso de las áreas mencionadas para poder delimitar la conducta punible o delito.

Habiendo definido los términos delito e incidente de seguridad en TICS, cabe destacar que la creación del tipo penal que une ambos conceptos la realiza el legislador y la aplicación del mismo es tarea del Juez.

A fin de poder determinar si una conducta se subsume en un tipo penal determinado, el Juez necesita tener un cabal entendimiento de los elementos presentes en el ámbito de despliegue de la conducta disvaliosa. Por ejemplo, a fin de determinar qué conductas típicas (delitos) desarrolla una persona que utiliza programas P2P para intercambiar representaciones de pedofilia, es necesario conocer el funcionamiento de los programas Ares o Bitorrent (entre otros), dado que las conductas previstas como delictivas son varias. Estas conductas reprochables son: producir, financiar, ofrecer, comerciar, publicar, facilitar, divulgar o distribuir, por cualquier medio toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales; organizar espectáculos en vivo; tener en su poder con fines inequívocos de distribución o comercialización, facilitar el acceso a espectáculos pornográficos o suministrar material pornográfico a menores de 14 años.

El conocimiento del funcionamiento del programa usado y de su protocolo de comunicación permitirá al Juez discernir si el imputado[8] comete el delito de facilitación, divulgación o distribución de estas representaciones. Los delitos que se castigan con la pena[9] de privación de la libertad, tiene una escala penal[10] graduada que indica los montos de tiempo máximo y mínimo con los que corresponde punir al infractor. El Juez aplicará un quantum de pena según su estimación de qué conducta se verifica, si sólo se facilitó la pedofilia o si distribuyeron las representaciones. A esta conclusión podrá llegar luego de analizar el **contexto tecnológico** de la conducta reprochada y el rol o responsabilidad del imputado en ese contexto. Para ello deberá interiorizarse de temas técnicos, o contar con personal capacitado y concientizado, con experiencia acreditada en estos temas, que lo asesore al respecto, como Peritos Informáticos que cumplan con la normativa vigente (Ley Provincial N° 13.016), en especial ser graduados universitarios en carreras Informáticas (arts. 2 y art. 7 inc. 13 de la citada Ley).

Continuando con el ejemplo del uso de redes P2P, se pone de manifiesto que el mismo constituye un tópico de debate en el que se discute el funcionamiento del

8 **Imputado** se define en el Código de Procedimiento Penal de la Provincia de Buenos Aires en su ARTÍCULO 60.- (Texto según Ley 13943) "Se considerará imputado a toda persona que en cualquier acto o procedimiento se lo indique o detenga como autor o partícipe de la comisión de un delito". Se distingue entre Código Penal, en el que se definen los delitos y unas disposiciones generales, del Código de Procedimiento Penal que es la regla o rito que se debe seguir para producir los distintos actos procesales como aprehensión detención, investigación penal preparatoria, juicio. Cada Jurisdicción (cada provincia y la nación) tiene su Código de Procedimiento, porque el dictado de este Código es una atribución originaria de las provincias no delegadas en el gobierno central.

[9] **Pena**: Es una privación o restricción de bienes jurídicos establecida por la Ley e impuesta por el órgano jurisdiccional competente al que ha cometido un delito. Nuestro Código Penal establece cuatro especies de pena: reclusión , prisión, multa e inhabilitación.

[10] **Escala Penal**: intervalo de tiempo con el que se puede penar a un penado, el Código Penal establece un máximo y un mínimo de pena que lo establecerá el Juez en el caso particular.

protocolo de comunicación y del programa, que por lo general comparte datos desde el momento que un nodo receptor recibe la primera porción de la representación transmitida. En este punto se discute la voluntabilidad[11] de la persona respecto del envío de datos: se puede argumentar que la persona no tenía intención de compartir los archivos, sino sólo bajarlos o que el usuario del programa no tenía conocimiento de que estaba enviando datos. Sin voluntad de cometer el delito, este no existiría. Contra ello se puede afirmar que el usuario del programa fue advertido en repetidas oportunidades respecto que el programa compartirá datos una vez instalado. De este modo, los portales de descarga indican que los programas P2P sirven para compartir datos, las pantallas de instalación indican que se compartirán datos y las ventanas del programa muestran los datos que se están compartiendo. Por otro lado si el usuario de un programa P2P deja de compartir archivos, baja la velocidad de descarga o se puede bloquearse la descarga. Todos estos conocimientos específicos del ámbito informático deben ser puestos a consideración del Juez para que evalúe si el penalmente imputado tenía conocimiento acerca de si al descargar representaciones las estaba compartiendo, y que las mismas quedaban compartidas en el programa. Por otro lado, además, evalúe si el imputado tenía voluntad de compartir.

A modo introductorio se conceptualizan los atributos de la información que serán retomados hacia el final del trabajo. La confidencialidad garantiza que la información sólo sea accesible por las personas autorizadas. La Integridad garantiza que la información sólo pueda ser modificada por quien está autorizado a hacerlo. La disponibilidad garantiza que los usuarios autorizados tienen acceso a la información y a los recursos relacionados cuando lo necesiten.

[11] Al mencionar la voluntabilidad es necesario aclarar que existen **tres tipos de delitos** desde el punto de vista del conocimiento y voluntad de cometerlo y realizar la acción típica. Ellos son los delitos culposos, en los que no se exige la voluntad o intención de cometerlos como elemento conformador del delito, consisten en la infracción de un deber de cuidado o en conductas imprudentes, negligentes; estos delitos deben estar específicamente tipificados como tales. Los delitos omisivos y los delitos dolosos en los que el infractor tiene que tener la "voluntad realizadora del tipo guiada por el conocimiento" del resultado que se va a obtener y aceptando la posibilidad de imputación del resultado. El dolo es saber y querer cometer un delito. (Zaffaroni, Eugenio, "Estructura básica del Derecho Penal", Ed. Ediar, Buenos Aires, 2009, Pags 83 y 108 - 109).

II. Clasificación de los Delitos Informáticos

Introducidos al comienzo y a través del ejemplo de las redes P2P, los conceptos de Derecho, Derecho Penal, finalidad del Derecho Penal, Tipo penal, conducta típica, imputado, pena, escala penal, delitos dolosos, culposos y omisivos; resulta necesario, antes de realizar el mapeo de los delitos en los incidentes de STICS, realizar una breve reseña de los delitos informáticos tipificados en nuestro ordenamiento penal, para luego realizar la calificación legal de las conductas disvaliosas, aunque pueda resultar redundante. Dicha redundancia se justifica por el abordaje del tema desde distintos puntos de partida.

Los delitos informáticos, en su mayoría fueron incorporados al Código Penal por la Ley 26.388. Esta Ley viene a compatibilizar el derecho penal nacional con el Convenio Sobre Ciberdelito del Consejo de Europa, adoptado en la Ciudad de **Budapest**, Hungría, el 23 de noviembre de 2001. La República Argentina aprobó y suscribió a este Convenio, recientemente, el 22 de Noviembre de 2017 por la Ley 27.411. A continuación se enumeran los delitos informáticos incorporados al Código Penal por la ley 26.388: (se mencionarán incidentes de STICs que serán explicados en el punto siguiente)

1. Delito de Pedofilia (Art.128 del Código Penal – CP de aquí en adelante)
2. Violación de secretos y de la privacidad (nuevo título que abarca desde el art. 153 del CP al art. 157bis, Titulo V: libertad, capítulo 3)
    - Apertura o acceso indebido a una comunicación electrónica (CE de acá en más) que no le esté dirigido (Art.153)
    - Apoderamiento indebido de una CE (Art.153)
    - Desvío o supresión indebida de una CE (Art. 153)
    - Interceptación o captación indebida de una CE (Art. 153)
    - Comunicación o publicación ilegítima del contenido de una CE, luego de su apertura o apoderamiento (Art. 153)
    - Acceso sin autorización a un sistema o dato informático (Art. 153 bis)
    - Publicación indebida de comunicaciones electrónicas no destinadas a la publicidad (Art. 155)
    - Revelación de secretos o datos (Art. 157)
    - Delitos relacionados con la protección de datos personales (art. 157 bis):
        - acceso no autorizado a banco de datos personales
        - proporcionar o revelar información de un banco de datos.

- Inserción ilegítima de datos en un banco de datos personales.

3. Estafa informática (art. 173 inc.16) y Carding (Ley 25.930 del 21/09/2004).
4. Daño informático (Arts. 183 y 184).
5. Interrupción de comunicaciones electrónicas (Art. 197)
6. Alteración de prueba(Art.255)
7. Grooming (art.131 CP incorporado por la ley 26.904 sancionada el 13 de noviembre de 2013.
8. Aclaración respecto de robo y hurto.

II.1. Delito de Pedofilia.

> *"Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores. Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización. Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años."* (CP art 128)

Las acciones típicas se pueden clasificar en:

Actos concretos de divulgación: Ofrecer, Comerciar, Publicar, Divulgar, Distribuir por cualquier medio, gratuito u oneroso, en formato físico o digital.

Acciones secundarios que ayuden a cometer el delito: producir (concepto amplio: crear, hacer, organizar, elegir personas), financiar, facilitar, tener con fines inequívocos de distribuir o comercialización, facilitar el acceso a espectáculos pornográficos, suministrar material pornográfico a menores de 14 años.

Ofrecer, facilitar, distribuir y comerciar alcanza toda forma de distribución como emails, archivos adjuntos, streaming o video en vivo, chat, msn, etc.

La definición legal de pornografía infantil dada en el texto del artículo, contempla "toda representación de un menor de 18 años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales". La palabra *representación* involucra toda imagen, fotografía, dibujo, video sin necesidad de que la representación sea entera ya que dice

“partes”. El término *representación* comprende toda figura, imagen o idea que sustituye la realidad, “con fines predominantemente sexuales”. Las manifestaciones artísticas y los relatos eróticos no completan los elementos del tipo. La persona representada debe ser menor de 18. No sería delito si el actor aparenta ser menor de 18. Pero sí a la inversa, si el actor es menor y parece mayor. No se hace mención a actividades sexuales simuladas.

Según la doctrina “es exigible al autor el conocimiento de que se trata de una representación de un menor de 18 años de edad dedicado…”. Por ello es una figura dolosa, sin posibilidad de realizarse con dolo eventual. Se delimitarán varios conceptos afines al dolo tomando como guía el libro de Eugenio Zaffaroni, Estructura Básica del Derecho Penal.

Se entiende por *dolo* a la voluntad realizadora del tipo guiada por el conocimiento de los elementos del tipo objetivo sistemático (como se dijo anteriormente). En el dolo directo de primer grado el resultado se quiere como fin en sí mismo. En el dolo directo de segundo grado el resultado se lo ve como una consecuencia inevitable. En el dolo eventual (indirecto o condicionado) el agente se representa la posibilidad de producción del resultado, pero encubre su voluntad realizadora acudiendo a una infundada esperanza de que no se produzca.

Supuestos: Los usuarios de redes P2P que bajan un archivo sin conocer que el mismo contiene representaciones de pedofilia no completan el elemento *dolo* del tipo penal. El usuario de redes P2P comparte lo que baja, por definición del protocolo de comunicaciones, por lo tanto está mínimamente *facilitando* la comisión del delito previsto por este artículo, con lo cual se verifica la realización de uno de los verbos típicos. La opinión del Instituto de Derecho Penal del Colegio de Abogados de La Plata, vertida en una conferencia y debate dado por el autor, se afirmó que el que usa Ares para descargar representaciones de pedofilia tiene dolo de distribuir dichas imágenes. Otra posición al respecto afirma que el usuario de redes P2P que descarga representaciones de pedofilia es partícipe necesario del delito que comete el/los que le envía/n los datos (esta es una postura innovadora del actual Secretario de Política Criminal de la Procuración General de la Suprema Corte de Justicia de la Provincia de Buenos Aires, Dr. Pon Berges).

Las Empresas que funcionan como intermediarios (telecomunicaciones, ISPs, hosting) no tienen conocimiento de la posible ilicitud de los contenidos ni tienen la posibilidad de monitorearlos. Se presupone que tienen conocimiento si reciben una notificación o comunicación fehaciente del damnificado u otra persona, (Fallo Rodríguez María belén c/ Google Inc s/ daños y perjuicios, CSJN R. 522.XLIX del 28 de octubre de 2014). Si no se erradica el contenido denunciado, podría considerarse que estarían facilitando la difusión de los contenidos prohibidos por el art. 128. Palazzi indica que los proveedores de conexión o de hosting, 1) no tienen conocimiento efectivo de los contenidos y de su ilicitud, 2) no podría existir tal conocimiento por la garantía de inviolabilidad de las comunicaciones que impide monitorearlas salvo que exista una orden de juez competente, 3) no existe un deber de vigilancia o supervisión de contenidos en la Web.

No obstante en Argentina se investigan penalmente representaciones pedófilas interceptadas en subidas a Internet en sitios específicos. Ello se debe a que en EEUU rige el código U.S. Code, Title 18, Part I, Chapter 110, § 2258A que dice textualmente:

> *"Reporting requirements of electronic communication service providers and remote computing service providers: (http://www.missingkids.com/LegalResources/Exploitation/FederalLaw,* 17/03/2018*) que dice textualmente:*
>
> *(1)In general.—Whoever, while engaged in providing an electronic communication service or a remote computing service to the public through a facility or means of interstate or foreign commerce, obtains actual knowledge of any factsor circumstances described in paragraph (2) shall, as soon as reasonably possible—*
>
> *(A)provide to theCyberTipline of the National Center for Missing and Exploited Children, or any successor to the CyberTipline*
>
> *[…] (e)Failure To Report.—An electronic communication service provider or remote computing service provider that knowingly and willfully fails to make a report required under subsection (a)(1) shall be fined—"*

Los párrafos anteriores, traducidos y resumidos por el autor, expresan cuáles son los requisitos de información de los proveedores de servicios de comunicaciones electrónicas y de los proveedores de servicios informáticos remotos. Quien quiera que esté dedicado a proveer un servicio electrónico de comunicación […] y obtiene conocimiento actual de algún acto descripto en el parágrafo 2 (explotación sexual de menores, representación visual de menores en conductas sexuales, producción de representaciones de menores envueltos en escenas sexuales) debe lo antes posible enviar un reporte a NCMEC. Un proveedor de servicios de comunicaciones electrónicas o un proveedor de servicios de computación remota que, a sabiendas y voluntariamente, no presente un informe requerido bajo la subsección (a) (1), será multado.

A fin de salvaguardar la intimidad de las personas que suben fotos de cualquier índole, los sitios que alojan imágenes consumen un servicio web a fin de comparar mediante un mecanismo de hash (matchear por hash) las representaciones de pedofilia almacenadas en una base de datos y realizar el informe CyberTypeline.

NCMEC (National Center of *Missing* and Exploited *Children*) es una organización sin fines de lucro con sede en los Estados Unidos de América que recibe el apoyo del Congreso de dicho país, con el fin de construir una respuesta internacional coordinada e intercambiar información respecto de la problemática de los niños desaparecidos y explotados sexualmente. Para intercambiar información se usa un programa llamado Griffeye que maneja estructuras de hashes almacenadas en formato JSON y se comunican por ODATA. Esta organización, debido a la proliferación de hechos delictuosos contra menores de edad existentes en internet, estableció un mecanismo centralizado donde los proveedores de servicios de internet, reportan actividades sospechosas relacionadas a la explotación sexual de los niños. Dicho mecanismo se denomina CyberTipline.

CyberTipline recibe las denuncias efectuadas por los proveedores de los diversos servicios de internet, inmediatamente envía un reporte al FBI con los datos necesarios para que se dé inicio a una investigación (fecha y hora del hecho, identificación del usuario sospechado y determinación geográfica de la IP utilizada para cometer el hecho). Luego el FBI da intervención a Interpol quien se encarga de transmitir la denuncia a la oficina del país que corresponda, en nuestro caso resulta ser Interpol Buenos Aires.

Mediante el Convenio entre NCMEC y el Ministerio Público Fiscal de CABA, el Cuerpo de Investigaciones Judiciales de esa Ciudad, tiene acceso virtual directo al servidor donde funciona la CyberTipline –previa autorización de NCMEC mediante un correo electrónico a las personas designadas-, a los fines de que se descargue la información de la denuncia de un hecho sospechoso cometido contra menores de edad por parte de usuarios de Argentina. (cfr. https://www.fiscalias.gob.ar/pedofilia/, 17/03/2018).

Con fecha 23 de octubre de 2014 el Consejo Federal de Política Criminal de manera conjunta con el Consejo de Procuradores, Fiscales, Defensores y Asesores Generales de la República Argentina, suscribió el Protocolo de Intervención urgente y colaboración recíproca en casos de detección de uso de pornografía infantil en internet, promoviendo la creación de la red de puntos de contacto (Red 24/7) requerida como modificación en el derecho procesal por el Convenio sobre Cybercriminalidad de Budapest.

II.2. Violación de secretos y de la privacidad

La Reforma más importante que introdujo la ley 26.388 es la que se refiere a este punto, dado que al agregarse la palabra *privacidad* la reforma atiende más a la intimidad y privacidad que al secreto. Ello debido a que hoy en día existen cientos de bases de datos, bancos de datos almacenando datos personales, por otro lado nuestros rastros quedan en numerosos sitios web, videocámaras, correos electrónicos, etc. Las normas ponen límites al uso que se hagan de nuestros datos. A continuación se enumeran los artículos de la ley que hacen referencia:

> *"ARTICULO 153. - Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida. En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido. La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica. Si el hecho lo cometiere un funcionario público que abusare de sus funciones,*

sufrirá además, inhabilitación especial por el doble del tiempo de la condena".

ARTICULO 153 BIS. –"Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido. La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros"

ARTICULO 155. - Será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil ($ 100.000), el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros. Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público.

ARTICULO 157. - Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos.

ARTICULO 157 bis. -Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años.

El art. 153 no crea un nuevo tipo, sino que le agrega a los tipos existentes la locución "comunicación electrónica" que se define como todo mensaje enviado por un individuo a otra persona por medio de un sistema electrónico ya sea por email, fax, chat, VoIP o SMS. Resuelve el problema de la atipicidad[12] de la violación de comunicación electrónica. (caso Brugo, Jorge Ángel c/ Lanata Jorge y otros. CSJN 2522; L. XLI)

A continuación se enumeran las acciones punibles sobre las conductas referenciadas en los artículos antes citados:

[12] Una acción es atípica cuando no está contemplada como delito en el Código Penal.

1. Apertura o acceso a una CE o correspondencia que no le esté dirigida, excepto si existe una orden judicial. En el caso de mails o chats se interpreta como Acceso a la comunicación que no le está dirigida.

    – No abarca la revisión que el administrador de una red hace de los correos a fin de mantener la seguridad.

2. Apoderamiento indebido de una comunicación electrónica: El delito consiste en abrir y conocer el contenido de una CE. Al realizar una copia de un mail o de un archivo adjunto también se configura este delito. Al no existir el tipo penal hurto informático, este tipo penal es el más semejante. Si se lo imprime y se destruye el original este delito concurre con el delito de daño informático.

3. Desvío o supresión de comunicación electrónica: consiste en sacar una CE de su camino o desviarla. Se entiende que la CE se encuentra *en curso* mientras el destinatario no la haya bajado del servidor y no la haya abierto. Serían los casos de spoofing y Man In The Middle.

4. Interceptación o captación de una C.E.: consiste en realizar los verbos tipos mencionados por ejemplo en una *escucha* telefónica de forma ilegal, sin autorización judicial.

5. Comunicación o publicación ilegítima: consiste en apoderarse indebidamente de una CE y además comunicarla a otro o publicarla. La diferencia con el delito del Art. 155 es que en este último artículo el delito consiste en publicar una CE no destinada a publicación o publicarla indebidamente causando perjuicios a terceros.

6. Acceso ilegítimo a un sistema o dato informático. La acción punible consiste en acceder por cualquier medio a un sistema informático de ingreso restringido. En esta categoría entra el spyware.

7. Publicación indebida de una CE, art.155: se da cuando la CE no está destinada a publicidad y su publicación cause daño a terceros.

8. Revelación de secretos, que por ley deben ser tales. Este tipo está vinculado con la Ley 25.326 (Protección de Datos Personales), art 10. Deber de confidencialidad.

9. Delitos relacionados a la protección de datos personales: (son delitos de acción privada[13])

    – Acceso no autorizado a un banco de datos personales.

    – Proporcionar o revelar información registrada en un banco de datos personales.

    – Inserción de datos en un banco de datos.

13 Requieren en consentimiento de la víctima para ser investigados

Se pone de manifiesto que son tres los accesos vedados: acceso indebido a una CE, acceso por cualquier medio a un sistema o dato informático de acceso restringido y el acceso violando sistemas de seguridad a un banco de datos personales.

Es necesario citar como antecedente a estas modificaciones del CP, la Ley Protección De Los Datos Personales N° 25.326, que establece como Objeto de dicha Ley (art 1, CN art. 43):

> *"La protección integral de los datos personales asentados en archivos, registros, bancos de datos, (públicos o privados) destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre".* (Ley de Protección de datos Personales N° 25.326)

Esta Ley establece, en su art. 2 las siguientes definiciones que se detallan a continuación:

> *"— Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.*
>
> *— Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.*
>
> *— Archivo, registro, base o banco de datos: Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.*
>
> *— Es lícito el tratamiento de datos aun sin el consentimiento del titular cuando este se limite a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; (art. 5). La dirección IP no está en la enumeración de datos de acceso público disponibles sin consentimiento por ello los ISPs la revelan a pedido del juez".* (Ley de Protección de datos Personales N° 25.326)

II.3. Estafa Informática

La estafa es un ataque a la propiedad cometido mediante fraude (cfr. Fontán Balestra, *Derecho Penal Parte Especial*) y por lo tanto requiere un engaño y un desplazamiento patrimonial.

En el ámbito informático es posible cometer tres tipos de defraudaciones:

1. La definida en el art. 172 CP, definición genérica de estafa, que se realiza en el phishing por el cual se engaña a una persona para producir el desplazamiento patrimonial.
2. El cardin, o uso no autorizado de tarjetas o sus datos, que se halla legislado como delito en el siguiente artículo del CP

" El que defraudare mediante el uso de una tarjeta de compra, crédito o débito, cuando la misma hubiere sido falsificada, adulterada, hurtada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos, aunque lo hiciere por medio de una operación automática". (CP art. 173, inc. 15 incorporado por la Ley N° 25.930 B.O. 21/9/2004)"

3. La estafa informática propiamente dicha que se encuentra legislada en el art. 173 inc.16 que dice textualmente:

"Se considerarán casos especiales de defraudación: 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". (CP art. 173 inc. 16)

Este tipo penal fue creado debido a la imposibilidad jurídica de estafar a una máquina, ya que el engaño debe ser padecido por una persona. La acción típica, defraudar mediante una manipulación en la PC, tiene dos requisitos: alterar el normal funcionamiento del sistema o la transmisión de datos. Este tipo penal es *abierto* ya que dice "que altere" sin especificar cómo será la alteración. Puede recaer sobre la transmisión de datos, por ejemplo en ataques a Web Sites, Spoofing, man in the middle, falsificación de cookies, modificación de parámetros de URL, ataques a la autenticidad, fuerza bruta o diccionarios para romper una contraseña o ataques en el control de acceso. También se considera estafa informática el falso montaje en cajeros automáticos con dispositivos disimulados con el fin de copiar datos.

II.4. Daño Informático

El Art. 183 2do párr. Establece que:

"En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños".

Antes de la sanción de este tipo penal, la destrucción de datos o programas era una conducta atípica. Las acciones típicas son alterar (verbo agregado en la nueva redacción), destruir o inutilizar datos, documentos, programas o sistemas informáticos. Se entiende por documento a toda representación de actos o hechos con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión (art.77 CP). Este tipo penal requiere para su consumación como elemento subjetivo el dolo.

Supuestos: Malware: Virus o código malicioso, Ransomware. No penaliza la existencia de virus, sino su distribución o introducción en dispositivos informáticos. El programa distribuido tiene que ser un programa destinado a causar daño, el format.exe por ejemplo no cumple los elementos del tipo. Este tipo penal no alcanza a los fabricantes de "tecnología de doble uso" por ejemplo fotocopiadora, programas P2P.

Daño informático agravado: el Art. 184 CP establece que la pena será mayor, si mediare cualquiera de las circunstancias siguientes:[…]

"5. Ejecutarlo en archivos o registros de uso público, o en datos, documentos, programas o sistemas informáticos públicos; 6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público." (CP art 184)

II.5. Interrupción de las comunicaciones electrónicas:

Dentro del Título 7, Capítulo 2 "Delitos contra la seguridad del tránsito y de los **medios** de transporte y de **comunicación"** se legisla el art.197 que dice textualmente

"Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida". (CP art. 197, modificado por la Ley 26.388)

La frese Comunicación Electrónica (CE) se refiere tanto al sistema de envío como al objeto enviado. La Ley Nacional de Telecomunicaciones N° 19.798 en su art 2 define la Telecomunicación como

"toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza, por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos". (Ley 19.798 art 2)

La Ley de Inteligencia Nacional N° 25.520 en el Art 5, enuncia ejemplos de este concepto:

"Las comunicaciones telefónicas, postales, de telégrafo o facsímil o cualquier otro sistema de envío de objetos o transmisión de imágenes, voces o paquetes de datos, así como cualquier tipo de información, archivos, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público, son inviolables en todo el ámbito de la República Argentina, excepto cuando mediare orden o dispensa judicial en sentido contrario." (Ley 25.520 art 5)

Esta modificación al CP introducida por la ley de Delitos Informáticos, se encuentra vinculada la Ley 27.126 BO 5/3/2015 (AFI) que modificó la Ley de Inteligencia 25.520. El artículo 42 establece una pena para el que:

"…participando en forma permanente o transitoria de las tareas reguladas en la presente ley, indebidamente interceptare, captare o desviare comunicaciones telefónicas, postales, de telégrafo o facsímil, o cualquier otro sistema de envío de objetos o transmisión de imágenes, voces o paquetes de datos, así como cualquier otro tipo de información, archivo, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público que no le estuvieren dirigidos". (Ley 25.520, art. 42)

Este tipo penal ampara las comunicaciones públicas y privadas como: email, programas que usen el protocolo VoIP, mensajes de chat o de texto por celulares, etc.

Es una figura dolosa. Supuestos: Incluye ataques DoS (denegación de servicio): Saturación del servidor, que se torna inaccesible. Jackeo.

II.6. Alteración de prueba

El Artículo 255 del CP expresa textualmente:

> *Será reprimido el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo. Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($ 750) a pesos doce mil quinientos ($ 12.500).* (CP art. 255)

II.7. Grooming

A partir del impulso dado por distintas ONG que trabajan en la temática se propulsó la sanción de una ley que penalice la conducta del ciberhostigamiento o ciberacoso. La conducta del grooming la llevan adelante aquellos sujetos adultos que emprenden acciones deliberadas con el objetivo de ganarse la amistad de un menor de edad, buscando crear una conexión emocional con éste, con el fin de disminuir las inhibiciones del niño y, eventualmente, poder abusar sexualmente de él. La palabra inglesa “groom”, que alude a conductas de preparación o acercamiento para un fin determinado.

El art.131 CP, incorporado por la ley 26.904 sancionada el 13 de noviembre de 2013 establece que

> *“…será penado el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma.”* (CP art 131)

Este delito conlleva un recorrido de distintas conductas: 1) contacto y acercamiento, en la cual el abusador se vale de herramientas para engañar sobre su verdadera edad, esto implica la creación de perfiles falsos, con fotos o videos ajenos o adulterados a través de programas informáticos. Se busca generar confianza y empatía. 2) el abusador consigue que el menor le envíe alguna fotografía o video con componentes íntimos. 3) La fase final es la del ciberacoso o sextorsion, en tanto si el menor no accede a sus pretensiones sexuales (le requiere envío de más material, más videos o fotografías, o peticiona un encuentro personal), el ciberacosador amenaza con difundir la imagen con mayor carga sexual que haya logrado de la víctima (o una creada a partir de otras imágenes) para su divulgación a través de Internet (plataformas de intercambio de videos, redes sociales, foros u otros) o enviarlas a los contactos personales del menor. (cfr. Sabrina B. Lamperti, “*El rastro digital del delito*”, InFo-Lab Universidad Fasta Ediciones, marzo 2017)

Rovira del Canto señala las siguientes fases del acoso sexual infantil o child grooming, a saber: a) fase de amistad; b) toma de contacto, gustos, preferencias, confianza; c) fase de relación; d) confesiones personales e íntimas, consolidación; e) componente sexual; f) participación de actos de naturaleza sexual, fotografías, webcam; g) extorsión; h) escalada de peticiones; i) agresión (Cfr Rovira del Canto, E. (2010) *Trabajo para la Primer Jornada TIC sobre Ciberdelincuencia*; http://www.iaitg.eu/mediapool/67/671026/data/Ciberdelincuencia_intr usiva_hacking_y_grooming_Enrique_Rovira.pdf, 17/03/2018)

II.8. Robo – Hurto de datos

Cabe aclarar que los tipos penales de robo y hurto implican el apoderamiento ilegítimo de una cosa mueble, total o parcialmente ajena. La jurisprudencia[14] ha entendido que la información no encuadra en el concepto de cosa mueble, y por otro lado cuando el supuesto robo consiste en copiar datos no se produce el desapoderamiento de la víctima. Por ello los tipos penales de robo y hurto no son aplicables a los incidentes de STICs en general. Por el contrario, en el caso de que el ladrón de datos también destruyera la fuente desde donde los copió o robara los discos donde los datos se encuentren se podría configurar el delito de robo o hurto.

Por ello en todos los casos en que se refiera a *robo* de información (en especial en el informe de OWASP al que se referirá más adelante) se deben considerar los siguientes tipos penales a fin de evaluar en qué prevenciones encuadra la conducta:

1. estafa informática, si concurren el desplazamiento patrimonial y la manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos. (Art. 173 inc 16 CP) y se da un desplazamiento patrimonial a consecuencia de un engaño (art. 172 CP).

2. “almacenamiento de copias ilícitas” que consiste en realizar copias no autorizadas (Ley 11.723 de Propiedad Intelectual, art. 72bis). En su art. 1 establece que el derecho de autor comprende además los programas de computación fuente y objeto; las compilaciones de datos o de otros materiales.

3. “acceso ilegitimo” a una base de datos (art. 153bis). En caso de que la base de datos sea un banco de datos personales se aplicaría el 157bis CP al que acceda a esos datos, o los revele o inserte.

4. Si se da un apoderamiento de una comunicación electrónica, se aplicaría el art. 153 CP.

De todos modos, se usará la locución robo de datos, entendida en sentido amplio y no técnico jurídico.

III. Mapeo de los incidentes de STICs en el Derecho Penal

En este trabajo se tiene en consideración no solo la ley de Delitos Informáticos N° 26.338 que modifica el CP, sino también leyes previas, posteriores y

[14] Conjunto de sentencias que marcan una tendencia conceptual.

complementarias a fin de poder calificar los incidentes de STICs y sus correspondientes conductas punibles.

A continuación, se individualizan los activos informáticos tutelados por el derecho penal, posteriormente se realiza una enumeración no taxativa de incidentes de STICs que constituyen conductas delictivas y a modo de conclusión se sintetiza el listado de delitos informáticos clasificándolos por el atributo de la Información que comprometen. Esto atributos constituyen el esquema axiológico de la informática, o escala de valores con los que se puede explicar, a nivel de principios generales los elementos normativos[15] de los tipos penales.

Los llamados delitos informáticos en algunos casos, son nuevos medios comisivos de figuras típicas anteriores a la Ley 26.388, pero cuando se dañan activos informáticos, la informática deja de ser un medio para delinquir y se convierte en el fin u objeto del delito.

III.1. Los activos tutelados

Se entiende por activo informático a toda cosa que tiene valor para una organización ya sea la información (archivos o bases de datos), aplicaciones, equipos y la infraestructura de comunicaciones. (Inciso 6 de la norma ISO 27001). El concepto de activo tutelado o activo informático tutelado abarca la noción informática de víctimas de los incidentes de STICs.

Los activos informáticos mencionados como elementos normativos de los delitos son: 1) los archivos, 2) los datos (incluyendo los de acceso restringido), 3) las comunicaciones electrónicas (entendidas tanto como sistema de envío y como objeto enviado), 4) el contenido de los archivos (pedofilia), 5) las bases de datos y/o los bancos de datos, 6) los sistemas informáticos, 7) el hardware y las personas que son la razón de ser del derecho penal.

1. Los **archivos** son los conjuntos de bytes que pueden conforman un documento de texto, una planilla de cálculos, una representación gráfica, un contenidos de audio, una base de datos o un programa ejecutable, etc. Son tutelados en el tipo penal de daño, en los artículos referidos a la Violación de Secretos y de la Privacidad (arts. 3, 4, 5, 6, 7, y 8 de la Ley de Delitos informáticos que modificaron los artículos 153, 153 bis, 155, 157 y 157 bis). El concepto de archivo incluye el concepto de documento.

2. Los **Datos** pueden estar en tránsito o almacenados, en cambio el concepto de archivo se refiere a datos almacenados. Son tutelados por los delitos de daño, por el fraude informático, por el acceso ilegitimo, por la prohibición de revelación de datos en cabeza de un funcionario público, por el proporcionar o revelar datos personales, o por la inserción ilegítima de datos.

La ley tutela el **dato informático de acceso restringido,** siendo estos los datos que están protegidos con algún grado de seguridad informática, ya sea por algo

[15] Elementos que se deben verificar para que se complete el tipo penal

que sé (un contraseña), por algo que tengo (una tarjeta de débito) o por algo que soy (la huella dactilar o el iris del ojo). La misma contraseña de acceso es un dato restringido.

3. Las **comunicaciones electrónicas y su infraestructura** que son entendidas en dos sentidos a saber:

a) **objeto enviado** como los emails, los mensajes instantáneos de los programas de chateo como Skype, WhatsApp, etc. Se hallan protegidos por el tipo penal del art 153.

b) **como medio de comunicación** siendo estas las que se dan entre computadoras dentro de una red LAN de una oficina o en Internet, que utiliza comunicaciones telegráficas, telefónicas o de otra naturaleza. Dicha tutela se halla en los artículos 153 2do párrafo 173 inc. 16 (transmisión de datos) y 197 del CP.

4. El **contenidos de los archivos** es tutelados, prohibiendo ciertas conductas referidas a la producción (creación de un archivo) y distribución (utilización de medios de comunicación) de representaciones de pedofilia. Ello se encuentra en el art. 128 del CP modificado por el art 2 de la Ley 26.388.

5. Las **bases de datos** son un conjunto ordenado y estructurados de información que es almacenada para su posterior uso por un sistema o frontend con el cual se cargan los datos y se obtienen respuestas a las consultas. Se encuentran tutelados por el artículo 153 bis que pena el acceso a un sistema o dato informático de acceso restringido. Al tutelar los sistemas informáticos se protegen las bases de datos que forman parte de los mismos. Si bien banco de datos en informática es sinónimo de base de datos, el art. 157 bis tutela los datos personales almacenados en bancos de datos. En el ámbito jurídico se prefiere el uso del nombre banco de datos asociándolo a datos sensibles, privados o relacionados con la salud. En este sentido la locución base de datos sería el género y banco de datos una especie.

6. También se tutelan los **sistemas informáticos** que son el conjunto de hardware y software destinados a cumplir una función específica. Se protegen los sistemas operativos, los programas de aplicación y las aplicaciones web. Los riesgos en las aplicaciones se encuentran analizados, clasificados y rankeados gracias a la labor de dos organizaciones estadounidenses denominadas OWASP (Open Web Application Security Proyect) y MITRE cuyo objetivo es colaborar con la confiabilidad de las aplicaciones web. OWASP genera periódicamente un listado de diez riesgos de las aplicaciones denominado Top Ten. (cfr. https://www. owasp.org /index.php/ Top_10_2017-Top_10, 17/03/2018).

Son tutelados en el art 153bis, por el tipo penal de daño y el delito de defraudación.

7. El **hardware** se protege en el concepto de *sistema informático* mencionado por el tipo del artículo 183.

8. Las **personas.** La falta de capacitación constituye una vulnerabilidad de una organización. Por otro lado las personas son víctimas de incidentes de STICs a través de la ingeniería social, phishing, spam, hoax o falsos mensajes de alerta, etc.

III.2. Incidentes de STICs y su mapeo en el Sistema Penal.

A continuación se analizarán los incidentes de STICs indicando qué delito se puede cometer con dichas conductas:

III.2.1. Ingeniería social: es un conjunto de trucos, engaños o artimañas que pueden producir confusión en las personas con la finalidad de que entregue información confidencial. Kevin D. Mitnick, uno de los ingenieros sociales más conocidos y escritor del libro "El Arte Del Engaño" (cfr. http://www.seaceptanideas.com/biblio/El_Arte_del_Enga%C3%B1o.pdf, 17/03/2018), afirma que la ingeniería social se basa en cuatro principios: 1) todos queremos ayudar, 2) el primer movimiento es siempre de confianza hacia el otro, 3) no nos gusta decir no y 4) a todos nos gusta que nos alaben.

Existen cuatro categorías de ataque por Ingeniería Social, categorizadas por OWASP (cfr. https://www.owasp.org/images/2/27/02_INGENIER%C3%8DA_SOCIAL.Pdf, 17/03/2018), a saber:

1) ataques técnicos: en los que el atacante no se contacta directamente con las víctimas, utilizan emails o páginas web, y simulan ser una entidad reconocida y de confianza. Está orientado a obtener información sensible de los usuarios. Es altamente exitoso.
2) ataques al ego: la víctima trata de probar su inteligencia y eficacia. Se busca que la víctima sienta que está ayudando en un tema relevante y que posiblemente reciba reconocimiento. Usualmente la víctima no se da cuenta del ataque.
3) ataques de simpatía: se simula un escenario donde es urgente completar una tarea o actividad. Se apela a la empatía de la víctima. El atacante pide ayuda hasta que encuentra alguien que le pueda proporcionar lo que necesita, se muestra desesperado.
4) ataques de intimidación: el atacante simula ser alguien importante en la organización y usa su autoridad para pedir colaboración de la víctima

Legalmente, son ardides o engaños que buscan confundir a las personas para que entreguen información confidencial. El delito de estafa admite la existencia de etapas en su proceso de ejecución llamados actos preparatorios. Por ello la ingeniería social se podría encuadrar en estas conductas preparatorias de la estafa o en la tentativa de estafa que comienza en el momento en que se despliegan los medios engañosos dirigidos a inducir a error al sujeto pasivo.

III.2.2. El phishing es una combinación de ingeniería social y elementos técnicos que persigue engañar a un usuario con el fin de que éste entregue información confidencial a otros usuarios malintencionados.

El phishing es una tergiversación en la que el criminal usa la ingeniería social para aparecer como una identidad confiable. Aprovecha la confianza para obtener información valiosa; generalmente detalles de cuentas, o información suficiente para abrir cuentas, obtener préstamos o comprar bienes a través de sitios de comercio electrónico. (cfr. https://www.owasp.org/index.php/Phishing, 17/03/2018)

Los ataques de phishing siguen alguno de los siguientes patrones (ibídem)

- La entrega a través de un sitio web, correo electrónico o mensaje instantáneo, el ataque pide a los usuarios hacer clic en un enlace para "volver a validar" o "reactivar" su cuenta.
- El enlace muestra un facsímil creíble de su sitio y de su marca para provocar que los usuarios ingresen detalles privados.
- Envíar un correo electrónico amenazante a los usuarios diciéndoles que el usuario ha atacado al remitente. Hay un enlace en el correo electrónico que solicita a los usuarios que proporcionen datos personales.
- Instalar spyware que busca que se tipeen ciertas URL bancarias, y cuando se escribe, aparece una forma creíble que les pide a los usuarios sus detalles privados.
- Instalar spyware (como Berbew) que busca datos POST, como nombres de usuario y contraseñas, que luego se envían a un sistema de terceros.
- Instalar spyware (como AgoBot) que draga la PC host para obtener información de cachés y cookies.
- Mensajes "urgentes" de que la cuenta del usuario se ha visto comprometida, y necesitan tomar algún tipo de acción para "aclararla".
- Mensajes de la sección "Seguridad" que solicitan a la víctima que revise su cuenta como alguien que accedió ilegalmente en esta fecha. Simplemente haga clic en este enlace de confianza.

El phishing encuadra en el art. 172 del CP, estafa genérica, debido a que no implica manipulación del sistema como requiere el nuevo tipo del art. 173 inc. 16 que es un tipo específico de defraudación.

III.2.3. El Pharming: consiste en reenviar el navegador a una página web que no es la original cambiando una entrada de un DNS. Se realiza alterando la asociación de una URL (www.mibanco.com) con la dirección real IP para dirigir a un usuario a una dirección que no es la verdadera.

El pharming redirige a los usuarios a sitios web fraudulentos sin interrupciones, sin actividad sospechosa, sin correo no deseado que solicita a un usuario que inicie sesión en un sitio web. Todo funciona perfectamente normal y los usuarios se sienten cómodos, ya que han visitado los mismos sitios web hace unos días sin ningún problema y ahora están repitiendo la misma actividad. Pero esta vez, se les redirige a un sitio web fraudulento, debido a envenenamiento de DNS u otros ataques como la escalada de rango de página (page rank scalation) y el ataque de hombre en el medio (Man in the Middle).

En la página de OWASP se halla un paper realizado por Cheong Kai Wee, titulado “Threat modelling of pharming” que resumen los vectores de ataques pharming en la siguiente enumeración: (cfr. https://www.owasp.org/index.php/File: Threat_modelling_of_pharming.doc, 17/03/2018)

3.1) Ataques a la conexión de red local

- Servidor DHCP rogue: Al configurar un servidor DHCP fraudulento, un pharmer puede enviar información falsa de configuración de red y asignar un servidor DNS bajo el control de pharmer a todos los clientes DHCP.

- Punto de acceso rouge / acceso libre: Un ataque típico a la red inalámbrica con Access Point AP deshonesto (punto de acceso) es enviar un mensaje de desautentificación al cliente inalámbrico y luego establecer un punto de acceso malicioso con la misma dirección ESSID y MAC pero diferente canal con el AP legítimo

- Instrucciones falsas sobre la configuración de la red: los pharmers pueden llevar a cabo un ataque de ingeniería social, enviando un correo con el encabezado del ISP a los usuarios e instruirlos para que introduzcan alguna configuración de red falsa en sus computadoras, por ejemplo un DNS controlado por pharmers.

- Hombre en el medio ataque con envenenamiento ARP u otros métodos. Se verá más adelante.

3.2) Ataques en navegadores

- Navegador Trojanizado: compartir para descargar navegadores con un Troyano dentro.

3.3) Ataque a la memoria caché local del host

- Envenenar la memoria caché DNS local: El router domiciliario funciona como un servidor DNS, que almacena información de los servidores DNS del ISP que provee servicios. La PC tiene una memoria caché de DNS local, por lo que puede hacer referencia rápidamente a las búsquedas de DNS que han sido realizadas con anterioridad, en lugar de realizar una búsqueda de DNS varias veces. Las tablas de estos DNSs pueden ser falsificadas por atacantes.

3.4) Ataques en el archivo host

- Modificación en el archivo de host: La mayoría de los sistemas operativos realizan la búsqueda de archivos de hosts para resolver un nombre de dominio antes de enviar consultas al servidor DNS. Al comprometer el archivo de hosts para agregar entradas adicionales, los pharmers pueden redirigir a los usuarios a sitios web fraudulentos.

3.5) Ataques a la resolución de nombres de dominio

- Secuestro de nombre de dominio: consiste en robar un dominio a su legítimo propietario. El objetivo es establecer un servidor DNS autorizado para ese dominio bajo control de los pharmers. El pharmer puede utilizar este servidor DNS para redirigir el tráfico de los usuarios a un sitio web fraudulento que se ve idéntico al sitio original.

- Registro de nombre de dominio similar: En este ataque, los pharmers aprovechan el nombre de dominio ligeramente mal escrito para engañar a los usuarios a visitar el sitio web de pharmers. Otras variaciones incluyen registrar un nombre con un dominio de nivel superior diferente. Este ataque explota el error de tipeo de los usuarios y su incapacidad para memorizar todo el nombre de dominio.

- DNS spoofing: Consiste en introducir datos falsos en un servidor DNS, lo que hace que el servidor de nombres devuelva una dirección IP incorrecta. Esto provoca que el tráfico se desvíe a la computadora del atacante (o a cualquier otra computadora). Spoofing significa redireccionar o falsificar algo. Se aclara este término ya que se volverá a usar en el párrafo de ataques por sniffing.

3.6) Ataques en servidores proxy

- Servidores proxy gratuitos: Un Pharmer puede configurar sus propios servidores proxy libres / anónimos y publicitarlos a los usuarios de Internet. Al actuar como servidor proxy, los pharmers pueden realizar un ataque man-in-the-middle para redirigir a los usuarios a sitios fraudulentos.

- Servicios Rogue WPAD: WPAD (Web Proxy Auto-Discovery Protocol) es un protocolo que permite a los clientes web buscar y cargar información de configuración de proxy desde un solo servidor. Los usuarios pueden aprovechar el algoritmo de búsqueda para instalar un servidor WPAD deshonesto en el nivel inferior de un dominio.

- Compromiso del servidor proxy: los pharmers también pueden comprometer el servidor proxy para redirigir el tráfico de los usuarios.

3.7) Ataques en los servidores web / páginas web

- Comprometer el servidor web: los pharmers pueden atacar el servidor web páginas web del dominio de destino y modificar su código para redirigir el tráfico de los usuarios.

- Cross site scripting: Las secuencias de comandos cruzadas del sitio ocurren cuando los atacantes incrustan scripts maliciosos en una página web dinámica generada y ejecutan el script en la máquina de los usuarios que ven esa página web. Hay 2 tipos de XSS: activo y pasivo. Los ataques XSS activos requieren la interacción de la víctima, en la que los atacantes construyen una URL malformada con una cadena de inyección y la envían a las víctimas mediante un correo electrónico o un programa de mensajería, lo que atrae a la víctima a hacer clic en el enlace. Los ataques pasivos XSS no requieren la interacción del usuario y pueden llevarse a cabo de forma automática y silenciosa. Los ataques pasivos son particularmente peligrosos y generalmente suceden en el foro, el tablón de anuncios y los libros de visitas, donde un script de ataque puede ejecutarse automáticamente cuando el usuario ve las páginas web.

3.8) Ataques a los motores de búsqueda

- Escalado de rango de página: busca que el sitio fraudulento esté en la parte superior del resultado de búsqueda de Google o Msn y así poder usarlo en la función autocompletar del cuador de dirección URL de los navegadores.

Tipificación Penal: El pharming sí implica manipulación del sistema por lo que se podría calificar como defraudación informática, art. 173 inc. 16 (nuevo tipo penal de la Ley 26.388) siempre que concurra un desplazamiento patrimonial.

III.2.4. Spam: es el correo electrónico no deseado, mensajes no solicitados, de remitente desconocido, enviados en cantidades masivas, de carácter publicitario, político, de propaganda, solicitando ayuda, etc. Se puede usar para realizar phishing o distribuir malware. El Spam genera una carga adicional a los servidores de correo y puede causar pérdidas de la información deseada.

La nueva conducta típica de daño informático contempla el "*hacer circular*" programas destinados a causar daños y esto es exactamente el propósito del spam.

III.2.5. Malware: Malware es la abreviatura de "*Malicious software",* término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento. Dentro de este género de programas podemos encontrar: Virus, Troyanos (Trojans), Gusanos (Worm), Botnets, Ransomwares, Spyware, Adware, Hijackers, Keyloggers, Rootkits, Rogues.

El tipo penal de daño informático, art. 183 2do párr., utiliza una descripción muy amplia en la frase "programas destinados a causar daños", en la que se engloban los distintos tipos de malware enunciados.

Una clasificación más amplia es la que hace Kaspersky y https://www.infospyware.com/articulos/que-son-los-malwares/ (17/03/2018) en su sitio web que se copia a continuación:

5.1) Virus clásicos. Programas que infectan a otros programas por añadir su código para tomar el control después de ejecución de los archivos infectados. La velocidad de propagación de los virus es algo menor que la de los gusanos.

5.2) Gusanos de red (o Worm). Este tipo de malware usa los recursos de red para distribuirse. Su nombre implica que pueden penetrar de un equipo a otro. Lo hacen por medio de correo electrónico, sistemas de mensajes instantáneos, redes de archivos compartidos (P2P), canales IRC, redes locales, redes globales, etc. Su velocidad de propagación es muy alta.

Al penetrar un equipo, el gusano intenta obtener las direcciones de otros equipos en la red para empezar enviarles sus copias. También suelen usar los datos del libro de contactos del cliente de correo electrónico. La mayoría de los gusanos se propagan en forma de archivos pero existe una pequeña cantidad de gusanos que se propagan en forma de paquetes de red y penetran directamente la memoria RAM del equipo víctima, donde a continuación ejecutan su código.

5.3) Troyanos. Los troyanos no pueden penetrar a los equipos por si mismo, sino se propagan simulando ser un software "deseable" disfrazándose de un programa legítimo. Esta clase de programas maliciosos incluye una gran variedad de programas que efectúan acciones sin que el usuario se dé cuenta y sin su consentimiento: recolectan datos y los envían a los criminales; destruyen o alteran datos con intenciones delictivas, causando desperfectos en el funcionamiento del ordenador o usan los recursos del ordenador para fines criminales, como hacer envíos masivos de correo no solicitado. No son virus clásicos porque no infecta otros programas o datos.. Son capaces de causar mucho más daño que los virus clásicos.

5.4) Spyware. Software que permite colectar la información sobre un usuario/organización de forma no autorizada. Su presencia puede ser completamente invisible para el usuario.

Pueden colectar los datos sobre las acciones del usuario, el contenido del disco duro, software instalado, calidad y velocidad de la conexión, etc.

5.5) Adware. Muestran publicidad al usuario. La mayoría de programas adware son instalados a software distribuido gratis. La publicidad aparece en la interfaz. A veces pueden colectar y enviar los datos personales del usuario.

5.6) Rootkits. Un rootkit es una colección de programas usados por un hacker para evitar ser detectado mientras busca obtener acceso no autorizado a un ordenador y tomar el control del sistema. Esto se logra de dos formas: reemplazando archivos o bibliotecas del sistema; o instalando un módulo de kernel. El hacker instala el rootkit obteniendo un acceso similar al del usuario: por lo general, craqueando una contraseña o explotando una vulnerabilidad, lo que permite usar otras credenciales hasta conseguir el acceso de root o administrador.

5.7) Backdoors. Estos programas son diseñados para abrir una *"puerta trasera"* en nuestro sistema de modo tal de permitir al creador de esta aplicación tener acceso al sistema y hacer lo que desee con él. El objetivo es lograr una gran cantidad de computadoras infectadas para disponer de ellos libremente hasta el punto de formas redes botnets.

5.8) Hoax. Un hoax (en español: farsa) es un correo electrónico distribuido en formato de cadena, cuyo objetivo es hacer creer a los lectores, que algo falso es real. A diferencia de otras amenazas, como el phishing; los hoax no poseen fines lucrativos, por lo menos como fin principal.

5.9) Keyloggers. Aplicaciones programadas con el fin de almacenar en un archivo todo lo que el usuario ingrese por el teclado (Capturadores de Teclado). Son ingresados por muchos troyanos para robar contraseñas e información de los equipos en los que están instalados.

5.10) Rouge. Un rogue software es básicamente un programa falso que dice ser o hacer algo que no es. Con la proliferación del spyware, aquellos comenzaron a surgir como un importante negocio para los ciberdelincuentes en formato de "Falso Antispyware". Con el tiempo fueron evolucionando creando desde "Falsos Optimizadores" de Windows, y en los más extendidos "**Falsos Antivirus**".

5.11) Ransomware ó Secuestradores. Es un código malicioso que cifra la información del ordenador e ingresa en él una serie de instrucciones para que el usuario pueda recuperar sus archivos. La víctima, para obtener la contraseña que libera la información, debe pagar al atacante una suma de dinero, según las instrucciones que este disponga.

III.2.6. Skimming: es una práctica ilegal orientada hacia la captura no autorizada de los datos confidenciales contenidos en el plástico de una tarjeta de

pago (banda magnética) con el fin de ser empleados para fines fraudulentos (clonación, uso en transacciones no presenciales, etc.). Esta conducta sería un acto previo del tipo penal de defraudación usando tarjeta de crédito, art. 173 inc 15, incorporado al CP por ley 25.930 en el año 2004.

III.2.7. Hacking, cracking: consiste en la explotación de vulnerabilidades de sistemas. En seguridad informática este término concierne principalmente a entradas remotas no autorizadas por medio de redes de comunicación como internet conocidas como sombreros negros (black hats). Pero también incluye a aquellos que depuran y arreglan errores en los sistemas como sombreros blancos (white hats) y a los de moral ambigua como son los sombreros grises (grey hats).

El acceso ilegitimo a un sistema o dato informático de acceso restringido se encuentra penado en el artículo 153bis y 157bis del CP, se realiza violando los sistemas de confidencialidad.

III.2.8. Hijacking: es un concepto muy amplio que se refiere a toda técnica ilegal que lleve consigo a adueñarse o robar algo por parte de un atacante, por ejemplo el secuestro del browser, de una sesión con un servidor o de una página web. Modifican la página de inicio y búsqueda por alguna de su red de afiliados maliciosos, entre otros ajustes que bloquea para impedir sean vueltos a restaurar por parte del usuario. Esta conducta podría encuadrarse en el daño informático.

III.2.9. Sniffing: consiste en inspeccionar el tráfico de una red analizando los protocolos de comunicación. Un ataque de sniffing puede ocasionar que se pierda la confidencialidad en las comunicaciones atacadas o se pierda la integridad de la comunicación si se alteran datos.

Los distintos tipos de sniffing en redes LAN switcheadas son ARP spoofing, DHCP spoofing, ICMP Redirect, siendo ARP, DHCP e ICMP los protocolos falsificados. Son tres técnicas destinadas a interceptar el tráfico de una PC para que el mismo pase por la PC del atacante capturando los datos transmitidos.

ARP Spoofing permite engañar a una PC para que crea que una IP determinada está asociada a la MAC del atacante. DHCP spoofing permite brindar a una PC información de autoconfiguración falsa: GW, DNS. ICMP Redirect utiliza un mensaje ICMP para alterar las rutas de una PC hacia un destino dado.

El atacante se interpone entre el origen y el destino, por eso se llaman genéricamente ataques MITM (Man In The Middle). Se pueden escuchar y modificar datos como así también obtener ilegítimamente contraseñas. Si las comunicaciones están cifradas por el uso de SSL o HTTPS, el sniffing solo accederá al tráfico pero no a su contenido.

Se repite la aclaración de que spoofing significa falsificación de algo. En pharming se usó este concepto de spoofing. Pero el pharming consiste básicamente en redirigir a un sitio falso, y el sniffing en inspeccionar el tráfico de la red. Para ambos ataques es útil la falsificación de los DNSs, pero con distintas finalidades.

Esta conducta se podría subsumir en el tipo penal creado por el artículo 173 inc 16, defraudar a otro "mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de la transmisión de datos" ya que el spoofing (falsificación) involucra la manipulación de los protocolos de comunicación, siempre que concurra un desplazamiento patrimonial.

III.2.10. BotNet: Una botnet es una red de equipos infectados por códigos maliciosos, que son controlados por un atacante, disponiendo de sus recursos para que trabajen de forma conjunta y distribuida. Cuando una computadora ha sido afectado por un malware de este tipo, se dice que es un equipo es un robot o **zombi**.

El secuestro de la capacidad de procesamiento implica un daño informático (art. 183 2do parr), el daño reside en el menoscabo de la capacidad y velocidad de procesamiento de la PC secuestrada.

Tareas comúnmente realizadas por una botnet:

- Usar el poder de la máquina infectada para ayudar en los ataques distribuidos de denegación de servicio (DoS) para cerrar sitios web.
- Envío de correos electrónicos no deseados a millones de usuarios de Internet.
- Generar tráfico de Internet falso en un sitio web de terceros para obtener ganancias financieras.
- Reemplazar anuncios publicitarios en su navegador web específicamente dirigido a usted.
- Anuncios pop-ups diseñados para que pagues por la eliminación de la botnet a través de un paquete falso de software espía.

El ataque DoS podría encuadrarse en el tipo de daño informático o en el art. 173 inc 16 si se da el desplazamiento patrimonial y la manipulación de informática en la transmisión de datos.

III.2.11. Grooming es la conducta descripta en el art 131 del CP, que establece que será penado el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, **contactare a una persona menor de edad**, con el propósito de cometer cualquier delito contra la integridad sexual de la misma. Este tipo penal fue sancionado por el Ley 26.904 el 13 de noviembre de 2013.

III.2.12. Cyberbullying, el bullying es una forma de conducta agresiva habitual que ocasiona daño deliberado. El cyberbullying consiste en acoso físico o psicológico a través de redes sociales, realizando comentarios crueles de otra persona mediante el envío o publicación de material dañino o la implicación en otras formas de agresión social usando Internet u otras tecnologías digitales. (cfr https://www.emagister.com/blog/ciberbullying-definicion-caracteristicas-tipologias/, 16/03/2018).

La Lic. en Psicopedagogía, María Zysman, que dictó en la Facultad de Informática UNLP el día 28/11/2017 una conferencia, y es quien dirige el Equipo Libres de Bullying, define al mismo diciendo que es el acoso escolar a través de e-mails, blogs, mensajería instantánea, redes sociales, mensajes de texto, imágenes digitales enviadas

a través de teléfonos móviles, salas de chat, carteleras web y demás páginas disponibles.

Internet permite sostener el hostigamiento a toda hora y desde cualquier lugar. Repercute en la escuela aunque no se realice dentro de ella. Puede ser **directo** (envío de mensajes, agresiones directas en redes sociales, salas de chat o juegos on line) o **indirecto** (por delegación, supone un desarrollo de mayor capacidad estratégica).

El cyberbullying presenta ciertas características similares al bullying tradicional (conducta agresiva, desequilibrio de fuerzas entre hostigador y hostigado, y reiteración), pero también algunas diferencias. Estas se refieren fundamentalmente al **anonimato** que brindan las nuevas tecnologías y la **accesibilidad permanente**. Por otra parte, los niños y adolescentes temen que, al denunciar el acoso que sufren o pedir ayuda, se le quite la posibilidad de seguir utilizando estos recursos. (cfr. https://libresdebullying.wordpress.com/quienes-somos/, 17/03/2018)

Existen proyectos para crear un tipo penal que lo castigue, por ejemplo el llevado adelante por el Consejo de los Derechos de Niñas, Niños y Adolescentes (cfr. http://www.elsindical.com.ar/notas/proyecto-de-ley-sobre-derecho-al-olvido-contra-el-cyberbullying, 26/03/2018)

III.2.13. Cybervenganza es la publicación de pornografía en Internet, no consentida por la víctima y realizada por un individuo con el que aquella ha tenido relaciones íntimas. Incluye basicamente imágenes sexuales y es ampliamente distribuido a través de redes sociales, blogs, emails y mensajes de texto. La Cyber Civil Rights Initiative es contactada por un promedio de 20 a 30 víctimas por mes (según datos del año 2015, ver CELE - Paula Vargas de Brea, "*La Regulación de la Pornografía no Consentida en Argentina"*, 2015). Según esta organización existen 3.000 sitios donde se puede subir pornografía de este tipo. Dos tercios de las víctimas son mujeres según el informe de la Association for Progressive Communication.

Las categorías de víctima y victimario se redimensionan con internet, el ataque a una ciber-víctima es personalizado y masivo por su difusión y por la cantidad de participantes del mismo. Colocan a la víctima en una mayor indefensión y le profieren un fuerte shock emocional ya que son imprevisibles y difíciles de conjurar.

Se encuentra en proyecto de legislación un tipo penal que castigue esta conducta lesiva de la intimidad de las personas, bajo el número S-2119/16, Penalización De La Publicación Y/O Difusión De Imágenes No Consentidas De Desnudez Total O Parcial Y/O Videos De Contenido Sexual O Erótico De Personas. (cfr. www.senado.gov.ar/parlamentario/parlamentaria/377141/downloadPdf, 26/03/2018).

III.2.14. Scaneo de puertos y de vulnerabilidades: son actividades con las que se busca en un servidor un puerto de comunicación abierto o una ruta de ataque. Si un puerto está abierto indica que hay un proceso atendiendo a los requerimientos que llegan al puerto. Existen distintas técnicas de escaneo de puertos como el Inicio de Conexión (saludo de tres vías), Cierre de Conexión, TCP connect scanning, Half-open, Inverse TCP flag scanning, TCP idel scan y UDP ICMP port unreachable scanning.

Son actos previos para la comisión de un delito o pueden constituir un acceso ilegitimo.

III.3. Delitos Informáticos y el Top 10 de OWASP

Se continúa con el mismo análisis referido a qué delito se puede cometer cuando se produce un incidente de STICs.

III.3.1. Inyección, ocurre cuando un usuario envía datos malintencionados a un intérprete situado en un servidor web, como parte de un comando o consulta. Los datos hostiles enviados por el usuario pueden hacer que el programa manejador de la base de datos ejecute comandos involuntarios o que se acceda a datos sin autorización. Se pueden inyectar comandos o instrucciones SQL. El impacto en los negocios puede ser el robo de la totalidad de los datos, su modificación o borrado y la pérdida de la reputación de la organización.

El documento de OWASP califica a estas conductas como robo en un sentido amplio y no jurídico del término, según lo dicho en el punto II.8.-

III.3.2. Pérdida de autenticación y gestión de sesiones: las funciones de las aplicaciones relacionadas con la autenticación y control de sesión se encuentran frecuentemente implementadas de manera incorrecta. Esto permite a los atacantes comprometer las contraseñas, claves, token de sesión o explotar otro defecto de implementación para asumir la identidad de otro usuario, ya sea de manera temporaria o permanente. Su impacto consiste en que todas las cuentas de usuarios pueden ser atacadas y el atacante puede hacer en el sistema todo lo que la víctima puede hacer, resultando una suplantación de un usuario autorizado.

La realización de este ataque encuadraría en la figura básica de estafa, “el que defraudare a otro con nombre supuesto o calidad simulada”. También se podría evaluar la aplicación del art. 153bis CP, acceso ilegitimo sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

III.3.3. Secuencia de comandos en sitios cruzados: conocidos por su sigla XSS. Este defecto ocurre cuando una aplicación incluye datos no confiables en una nueva página web sin validarlos adecuadamente siendo que los mismos provienen de un usuario. XSS permite a los atacantes ejecutar programas en el navegador de la víctima con el fin de secuestrar la sesión de usuario, modificar sitios web, o redirigir al usuario a sitios maliciosos. Estos ataques modifican las páginas web, ya sea de forma permanente o temporaria para generar otros perjuicios.

Podría subsumirse esta conducta en el daño informático siempre que concurran *la alteración, destrucción o inutilización de datos, documentos, programas o sistemas informáticos* o en la estafa informática, en caso de que se verifique un desplazamiento patrimonial.

III.3.4. Controles de acceso deficientes: ocurre cuando las restricciones sobre qué pueden hacer los usuarios autenticados no se encuentran adecuadamente configuradas. Los atacantes pueden explotar estos defectos para acceder a funcionalidades o datos no autorizados, como cuentas de usuario, ver archivos

sensibles, modificar los datos de otro usuario o cambiar derechos de acceso. Los datos pueden ser robados o modificados. Se aplican las mismas previsiones enunciadas en el punto II.8.

III.3.5. Configuración de seguridad incorrecta: la buena seguridad requiere tener una configuración segura definida para la aplicación, los servidores y bases de datos. Se deben definir patrones de seguridad, implementarlos y mantenerlos. Estos deben reemplazar los patrones de seguridad por defecto, que suelen ser inseguros. Adicionalmente, el software debe ser actualizado. El impacto de un ataque a través de esta ruta podría implicar que todos los datos sean robados o modificados. Se aplica lo dicho para robo informático.

III.3.6. Exposición de datos sensibles: muchas aplicaciones no protegen adecuadamente los datos sensibles como tarjetas de crédito o datos de salud. Los atacantes pueden robar o modificar estos datos protegidos débilmente para realizar fraudes con tarjetas de crédito, robo de identidad, u otros delitos. Los datos sensibles merecen protección extra, como encriptación en su almacenamiento o tránsito, como también precauciones especiales cuando son intercambiados por el navegador. Se repiten los mismos supuestos anteriores referidos al robo.

III.3.7. Protección insuficiente ante ataques: la mayoría de las aplicaciones carecen de las habilidades básicas para detectar, prevenir y responder a los ataques manuales o automatizados. La protección de los ataques va más allá de la simple validación de ingreso de datos y requiere detección automática, registro, respuesta e inclusive bloqueo de intentos de ataque. Los propietarios de las aplicaciones deben ser capaces de implementar parches rápidamente para proteger las aplicaciones de los ataques. Tener datos desprotegidos no constituye en sí mismo un delito.

III.3.8. Falsificación de peticiones en sitios cruzados: este ataque fuerza al navegador de una víctima autenticado en un sitio, a enviar requerimientos falsos, incluyendo las cookies de sesión e información de autenticación hacia una aplicación web vulnerable. Este ataque hace que la víctima envíe requerimientos legítimos aunque le sean probablemente desfavorables. Dicha conducta encuadraría en el tipo penal de defraudación informática.

III.3.9. Utilización de componentes con vulnerabilidades conocidas: Componentes como librerías o módulos de software corren con los mismos privilegios que la aplicación. Si un componente vulnerable es explotado se puede perder mucha información o tomar el control del servidor. Las aplicaciones que usan componentes con vulnerabilidades pueden socavar las defensas de la aplicación y permitir ataques e impactos severos. Se puede tomar el control de un servidor y robar la información. Vale lo dicho en el punto II.8 referido a robo para el caso de que se concrete un ataque por esta ruta. Obviamente la utilización de componentes con vulnerabilidades conocidas no implica la comisión de un delito.

III.3.10. APIs desprotegidas: las aplicaciones modernas, como por ejemplo buscadores de hoteles recogen datos de los sitios que los ofrezcan a través de estas APIs. Las APIs por lo general se encuentran desprotegidas y contienen vulnerabilidades.

Esto permite el robo de datos, corrupción, destrucción o acceso no autorizado. Se repiten lo dicho sobre robo informático.

III.4. Atributos de la información:

En el ámbito de la seguridad informática se busca garantizar tres atributos de la información, que vendrían a desempeñar un rol semejante a los bienes jurídicos tutelados en el derecho penal[16]. Los delitos informáticos atentan contra estos valores informáticos. Los atributos de la información y los delitos opuestos a los mismos son:

La **confidencialidad**, que garantiza que la información sólo sea accesible por las personas autorizadas. Este atributo se ve comprometido con los delitos en los que se abre o accede indebidamente a correspondencia que no le esté dirigida, o alguien se apodera o intercepta indebidamente una comunicación electrónica de carácter privado o de acceso restringido, o cuando se produce un acceso ilegitimo a un sistema o dato informático sin la debida autorización o excediendo la que posee, cuando se publica indebidamente comunicaciones electrónicas, por el acceso no autorizado violando la seguridad a un banco de datos personales, por proporcionar o revelar información registrada en un banco de datos personales.

La **Integridad** que garantiza que la información sólo pueda ser modificada por quien está autorizado a hacerlo. Este atributo se ve comprometido con los delitos en los que indebidamente se suprime o desvía de su destino una comunicación electrónica que no le esté dirigida, se insertan ilegítimamente datos en un banco de datos o en un archivo de datos personales, o por interrumpir o entorpecer una comunicaciones electrónicas.

La **disponibilidad**, que garantiza que los usuarios autorizados tienen acceso a la información y a los recursos relacionados cuando lo necesiten. Este atributo se ve comprometido cuando se cometen los delitos que alteren registros informáticos para defraudar a otro, por el uso no autorizado de tarjetas y claves falsas o sustraídas, por el daño informático (alterar, destruir o inutilizar datos y/o sistemas o por la introducción de un programa destinado a causar daños), o por la alteración o destrucción de pruebas.

Otros atributos de segundo orden son:

La **autenticidad** que garantiza que la persona que origina o recibe un mensaje es quien dice ser. Este atributo se ve comprometido por el phishing o robo de identidad.

El **no repudio**, garantiza que la persona que recibió o envió un mensaje no pueda negar haberlo hecho. Esto se ve claro en la firma digital y su legislación vigente (Ley 25.506 art. 7).

Estas acciones enunciadas precedentemente, que comprometen los atributos informáticos constituyen delitos informáticos. Por ello no sería errado entender que **estos objetivos técnicos constituyen un esquema axiológico del quehacer**

[16] Los bienes jurídicos protegidos por el derecho penal, como la vida, la propiedad, etc, estructuran el Código Penal.

informático y como tal están vinculados con la estructura de los bienes jurídicos protegidos por el Código Penal.

IV. Guía de intervención urgente ante casos de grooming y cyberbullying.

Se deben tener en cuenta las recomendaciones generales de seguridad como ser utilizar contraseñas seguras, conocer a los amigos de las redes sociales, no aceptar solicitudes de amistad de desconocidos, ser precavido cuando se usa una PC pública, ser cuidadoso con el contenido que se publica, configurar correctamente la privacidad, ubicación de la computadora (a la vista de los padres), evitar la instalación de webcams, evitar usar sobrenombres que revelen sexo o edad, poner horario para ir a la cama. (cfr. http://www.internet-grooming.net/consejos-8.html, 17/03/2018)

Más allá de los cuidados que los padres, hermanos mayores y tíos realicen de los menores en su vida digital, una vez detectado un contacto o chat inapropiado, con contenidos sexuales probablemente dañinos para el desarrollo natural de la persona se debe **realizar la denuncia pertinente en una fiscalía**.

El objetivo de la investigación penal preparatoria del Juicio (IPP) es **llegar desde una URL atacante hasta el domicilio real de la persona que realizó el ataque** a fin de poder, con la orden del Juez de Garantías, allanar el domicilio y secuestrar los elementos informáticos para realizar pericial con los mismo y constatar o no la comisión del delito.

Para ello se debe presentar como prueba o el agente judicial debe solicitar los siguientes datos informáticos:

1. La URL desde donde se realizó el ataque. El denunciante debe en el momento del ataque, o posteriormente si es posible, registrar la URL desde donde se produjo el ataque. Para ello se podrá realizar capturas de pantallas o fotos donde se vean especialmente la URL atacante. Luego deberá facilitar los dispositivos informáticos pertenecientes a la víctima a fin de poder obtener y agregar a las actuaciones judiciales fotos como las que se muestran a continuación en las que se pone de relieve el camino para llegar a la URL:

Se aclara que las fotos son memes que usó el imputado para evitar exponer su verdadero rostro. En la URL aparece el ID de Facebook del *contactador* en este caso de Grooming: este ID debe ser copiado en un Oficio firmado por el Juez de Garantías solicitando a Facebook el registro de conexiones de ese usuario, la fecha y hora y la IP de creación del perfil.

2. También resulta conveniente bridar y/o solicitar, para el caso de que el menor y la familia estén de acuerdo, el usuario y contraseña de Facebook o de la red social implicada. Estos datos se ingresan al expediente por escrito, dejando constancia de los consentimientos prestados por los padres, tutores o víctimas. Con estos datos se puede acceder a los chats con los cuales se cometió el delito de grooming y también se puede descargar el perfil completo de la víctima para obtener más prueba. Para ello se debe

navegar hasta el panel de Facebook denominado “Configuración General de la cuenta”, y hacer clic en el link “Descarga una copia de tu información”. Es necesario tener en cuenta a qué mail se enviará dicha descarga y tener acceso a esa casilla de mail.

3. El oficio del Juez de Garantías se sube al Panel de Facebook denominado “Law Enforcement Online Requests”. Este panel chequea que el mail requirente pertenezca a un agente judicial o policial a través del envío de un tocken de acceso al mail oficial del requirente de la información. Para acceder a este panel se debe escribir en el navegador la URL del agente seguido de /records o www.facebook.com/records.

4. Una vez que se cuenta con la IP del atacante se debe determinar cuál es el Proveedor de dicha IP usando el servicio Whois en la página, por ejemplo de sitio www.Lacnic.net.

5. Enviar un Oficio al proveedor para que remita el domicilio real donde una IP prestó servicios en un día y hora determinado. Se debe tener en cuenta el uso horario, por ejemplo Facebook responde la hora en formato UTC 0 y los proveedores locales registran los datos de navegación en formato UTC -3 por lo cual se debe realizar la conversión de la fecha respondida por Facebook a la fecha con formato UTC -3.

V. Conclusiones:

En toda sociedad éticamente pluralista coexisten distintos niveles de moralidad, no obstante el derecho penal protege una ética de mínimos obligatoria para todos (ver G. Jellinek, *Teoría General del Estado*, Buenos Aires, Editorial Albatros, 1954), en la que se insertaron, a través de los tipos penales descriptos, los valores de confidencialidad, integridad y disponibilidad de la información.

El conocimiento cabal de estos tipos penales implica la comprehensión del contexto tecnológico en el que se despliega la conducta punible. Para lograr este conocimiento por parte de los jueces, fiscales y defensores que deben entender y aplicar la ley, el derecho prevé la figura del **Perito Informático** que puede asesorar a las partes del proceso. El Código Procesal Penal de la Provincia de Buenos Aires entiende por Perito en su artículo 244, a personas con "conocimientos especiales en alguna ciencia, técnica o arte" que podrán redactar o explicar algún hecho o circunstancia pertinentes a la causa que requiera este conocimiento especial. Los peritos deberán tener títulos habilitantes en la materia a la cual pertenezca el punto sobre el que han de expedirse. Si no estuviera reglamentada la profesión, no hubiere peritos diplomados o inscriptos, deberá designarse a una persona de conocimiento o de práctica reconocidas.

Como es sabido en la Provincia de Buenos Aires existe el Consejo Profesional de Ciencias Informáticas que fuera creado por la Ley Provincial 13.016 y regula el ejercicio de la profesión. El artículo 7 de este cuerpo legal establece que los habilitados en las profesiones comprendidas en esta ley, podrán hacer ejercicio profesional al realizar […] arbitrajes, pericias y tasaciones relacionados con los Sistemas Informáticos y todo el equipamiento para el Procesamiento de Datos, dictaminar e informar a las Administraciones e Intervenciones Judiciales como perito en su materia, en todos los fueros.

Estos Peritos Informáticos deberán tener en claro en claro que **cuando los incidentes de STICs se realizan con voluntad y conocimiento de que se está produciendo un perjuicio, los mismos pueden ser delitos perseguidos penalmente**. Deberán conocer la lista de los delitos previstos en el ordenamiento penal y, por otro lado entender si los activos comprometidos en un incidente de STICs forman parte de los elementos normativos de los tipos penales a fin de poder asesorar en la evaluación de la conducta analizada.

Este es el aporte realizado en este trabajo y deberá continuarse ampliando a medida que se sancionen y promulguen nuevas tipos penales, como por ejemplo la simple tenencia de pornografía infantil, que recientemente se promulgó en la ley Ley N° 27.436 B.O. 23/4/2018, que modificó el Código Penal.

VI. BIBLIOGRAFIA

1) Borda, G, 1987, *Tratado de derecho Civil - Parte general,* Buenos Aires, Abeledo Perrot Tomo I.
2) Kelsen, H, 1986, *Teoría Pura del derecho*, Buenos Aires, Eudeba.
3) Iglesias,G, Aspectos Legales y Profesionales de la informática.
4) Cossio, C, 1964, *La teoría egológica del derecho y el concepto jurídico de libertad, Buenos Aires,* Abeledo Perrot
5) Zaffaroni, E, 2006, *Manual de Derecho Penal*, Buenos Aires, Ediar.
6) Ferrajoli, L, 1995, *Derecho y Razón*, Trotta, Madrid.
7) Enciclopedia Jurídica, http://www.enciclopedia-juridica.biz14.com, 17/03/2018
8) SGSI, http://www.pmg-ssi.com/2014/12/iso-27001-que-diferencia-existe-entre-la-seguridad-informatica-y-la-seguridad-de-la-informacion/, 11/09/2017
9) RFC 2828, titulada Internet Security Glossary, May 2000
10) https://www.owasp.org/index.php/Glossary, 17/03/2018
11) Ley 27.078 – Ley Argentina Digital (18/12/2014)
12) Código de Procedimiento Penal de la Provincia de Buenos Aires en su ARTÍCULO 60.- (Texto según Ley 13943)
13) Ley Provincial N° 13.016
14) Zaffaroni, Eugenio, “Estructura básica del Derecho Penal”, Ed. Ediar, Buenos Aires, 2009.
15) Fallo Rodríguez María belén c/ Google Inc s/ daños y perjuicios, CSJN R. 522.XLIX del 28 de octubre de 2014
16) https://www.fiscalias.gob.ar/pedofilia, 17/03/2018
17) Brugo, Jorge Ángel c/ Lanata Jorge y otros. CSJN 2522; L. XLI
18) Ley 25.326 (Protección de Datos Personales)
19) Fontán Balestra, Derecho Penal Parte Especial, Abeledo Perrot, Buenos Aires, 1998.
20) Ley de Inteligencia Nacional N° 25.520
21) Sabrina B. Lamperti, “El rastro digital del delito”, InFo-Lab Universidad Fasta Ediciones, marzo 2017)
22) Rovira del Canto, E. (2010) Trabajo para la Primer Jornada TIC sobre Ciberdelincuencia; http://www.iaitg.eu/mediapool/67/671026/data/Ciberdelincuencia_intr usiva_hacking_y_grooming_Enrique_Rovira.pdf, 17/03/2018.
23) Ley 11.723 de Propiedad Intelectual
24) Norma ISO 27001
25) https://www. owasp.org /index.php/ Top_10_2017-Top_10 OWASP, 17/03/2018
26) Kevin D. Mitnick, “El Arte Del Engaño” http://www.seaceptanideas.com/biblio/El_Arte_del_Enga%C3%B1o.pdf, 17/03/2018
27) https://www.owasp.org/images/2/27/02_INGENIER%C3%8DA_SOCIAL. Pdf, 17/03/2018.
28) https://www.owasp.org/index.php/Phishing, 17/03/2018.
29) Cheong Kai Wee, “Threat modelling of pharming” en https://www.owasp.org/index.php/File: Threat_modelling_of_pharming.doc, 17/03/2018.
30) https://www.infospyware.com/articulos/que-son-los-malwares, 17/03/2018.

31) María Zysman, Conferencia dictada en la Facultad de Informática UNLP el día 28/11/2017.
32) https://libresdebullying.wordpress.com/quienes-somos/, 17/03/2018.
33) https://www.emagister.com/blog/ciberbullying-definicion-caracteristicas-tipologias/, 16/03/2018
34) http://www.elsindical.com.ar/notas/proyecto-de-ley-sobre-derecho-al-olvido-contra-el-cyberbullying, 26/03/2018
35) CELE- Paula Vargas de Brea, “La Regulación de la Pornografía no Consentida en Argentina”, 2015, 17/03/2018.
36) www.senado.gov.ar/parlamentario/parlamentaria/377141/downloadPdf, 26/03/2018
37) http://www.internet-grooming.net/consejos-8.html
38) G. Jellinek, Teoría General del Estado, Buenos Aires, Editorial Albatros, 1954

Indice