Material Imprimible

Curso Ciberdelitos y Derecho Informático

Módulo 3

Contenidos:

- Tipologías y aspectos generales del ciberdelito
- Derecho a la intimidad virtual y protección de los datos personales
- Legislación Argentina en materia de los ciberdelitos: leyes 26388 y 26904

Tipologías y aspectos legales de los ciberdelitos

Podemos entender a la ciberdelincuencia como una forma de adaptación de ciertos delitos tradicionales a la actualidad a partir de medios informáticos. Si bien su naturaleza es cibernética, lo que permite el actuar en cualquier momento y lugar, sus consecuencias tienen la misma magnitud que muchos delitos considerados tradicionales.

El uso del internet y de los dispositivos electrónicos se acentúa día a día exponencialmente, y se emplean en una gran cantidad de actividades que, realizadas todos los días, aumenta las posibilidades de ser víctima de los delitos informáticos que operan todo el tiempo en la web.

Basándonos en el Convenio de Ciberdelincuencia del Consejo de Europa, podemos definir a esta clase de delitos como "los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos".

Las principales dos modalidades de llevar a cabo delitos informáticos son:

- Los delitos periódicos, que son ilícitos que se efectúan de manera rutinaria, como puede ser el fraude a partir de, por ejemplo, el phishing, o el ciberacoso
- La segunda modalidad es la de delitos únicos, la cual se trata de un delito en particular realizado a partir de un solo acto. Un ejemplo sería la instalación de un programa malicioso para obtener las claves bancarias del usuario de la computadora.

El uso de dispositivos electrónicos con acceso a la red cada vez empieza a una edad más temprana, lo que hace que muchos menores se hallen vulnerables a efectuar un mal uso de los correos electrónicos y las demás redes sociales. Por dicho motivo, es fundamental, a partir de la prevención, hacer hincapié en modificar la carencia en la sociedad de la sensibilización de los riesgos y educación que estas herramientas virtuales significan. A su vez, es necesario comprender que no solo es posible recibir un ataque, sino que como

ciudadanos podemos llagar a efectuar algún delito contra el derecho a la intimidad, la moral o a la propia imagen.

Actualmente sigue habiendo bastante ignorancia respecto a los delitos en internet, y esto se da por la falta de información para el común de la población. Por ende, es importante poder saber a qué nos enfrentamos para adquirir los conocimientos básicos que se requieran y así poder prevenirlo.

Se considera que hay cuatro tipos principales de delitos informáticos:

- Los que involucran en acceso ilícito a sistemas informáticos
- Los que obstaculizan el funcionamiento de sistemas cibernéticos
- Los que interrumpen de manera ilícita datos informáticos
- Y los que involucran el uso de dispositivos que faciliten llevar a cabo un crimen

En materia de derecho penal, el despliegue de una conducta delictiva va a suponer la existencia de dos sujetos: un sujeto pasivo y un sujeto activo. Estos, al mismo tiempo, pueden tratarse de una o varias personas jurídicas o naturales.

De esta manera, se considera que el bien jurídico protegido va a ser, en definitiva, el elemento que va a permitir localizar a estos sujetos, así como su posición respecto al delito. Por ello, el titular del bien jurídico vulnerado va a ser el sujeto pasivo, quien puede ser distinto al sujeto perjudicado, el cual dado el caso, de forma eventual, puede ser un tercero. Por otra parte, quien vulnere el bien protegido, a partir de la ejecución del tipo penal, va a ser el sujeto activo.

El sujeto pasivo va a ser el titular del bien jurídico protegido por el legislador y sobre el cual va a recaer la acción típica del sujeto activo.

En primer lugar hay que diferenciar al sujeto pasivo de la víctima del delito. Esta última es el ente sobre el cual recae la conducta de omisión o acción que efectúa el sujeto activo, y en el caso particular de los delitos informáticos, las víctimas pueden ser, además de individuos, gobiernos, entidades bancarias, empresas privadas, entre otros, que utilizan sistemas automatizados de información.

El sujeto pasivo del delito va a ser muy relevante para el estudio de los delitos informáticos, ya que a partir de él vamos a poder indagar respecto a los distintos ilícitos que cometen los autores, con el objetivo de prever las acciones anteriormente mencionadas, debido a que muchos de los crímenes son descubiertos casuísticamente por la ignorancia de la metodología delictiva de los sujetos activos.

Los individuos que efectúan delitos informáticos son aquellos que mantienen ciertas características que no muestran la mayoría de los autores de delitos tradicionales. Estos son los sujetos activos, los cuales tienen conocimientos y habilidades para el uso de los sistemas informáticos.

Estos, a su vez, habitualmente por su situación de trabajo, se hallan en lugares considerados estratégicos, donde se emplea información de carácter sensible, o también son idóneos en la utilización de los sistemas informatizados, aunque, en muchos casos, no desplieguen actividades laborales que ayuden a la comisión de esta clase de delitos.

El bien jurídico protegido se refiere al bien vulnerado o lesionado por el accionar del sujeto activo. Este nunca debe dejar de existir, y a veces resulta difícil que estén expresamente tipificados en el Código Penal de la República Argentina.

Generalmente, el bien jurídico protegido va a ser la información, pero está contemplada en distintas maneras, por ejemplo, como un valor económico, como un valor propio del individuo, por su tráfico jurídico y su fluidez, y por último, por los sistemas que la automatizan o procesan; los mismos que se igualan a los bienes jurídicos de carácter tradicional,

- La fiabilidad y la seguridad del tráfico probatorio y jurídico va a ser el caso, por ejemplo, de falsificaciones documentos probatorios o datos relevantes a partir de medios informáticos
- La intimidad, reserva y confidencialidad de información va a verse en las agresiones informáticas dentro de los valores de la intimidad, particularmente en el caso de los bancos de datos

- El derecho a la propiedad es una circunstancia que se da respecto a la información o respecto a los elementos físicos, materiales de un sistema informático.
- Por último, el patrimonio involucra una gran variedad de fraudes informáticos y las manipulaciones de información que se desarrollan bajo este aspecto.

Dentro de la delincuencia informática es posible clasificar los ilícitos en distintos grupos:

- Las vulneraciones al derecho de la intimidad son ilícitos que se fundamentan en la difusión sin consentimiento o el hurto, de datos privados de las personas
- Los timos son, principalmente, sustentados en estafas por hurto o en falsificaciones de tarjetas de crédito. También, otra modalidad es llevarlos a cabo a partir de la posesión o creación de programas informáticos maliciosos encargados de falsificar
- Los delitos contra los derechos de autor se llevan a cabo cuando se vulnera la propiedad efectuando copias o distribuciones falsas de sistemas electrónicos y de distintos programas.
- Por su parte, los daños informáticos se sustentan en la modificación o destrucción de programas informáticos y de documentos electrónicos obtenidos en sistemas informáticos, y se suele llevar a cabo mediante el uso de programas maliciosos
- También los insultos y falacias, siempre y cuando se lleven a cabo mediante cualquier tipo de comunicación por medios electrónicos.
- Las intimidaciones se refieren a actos amenazantes de cualquier índole o con motivos de extorsión que se efectúen por medio de cualquier medio de comunicación.
- Y por último, la pederastia, es decir, la pornografía infantil, que es un delito contra la integridad sexual

Derecho a la intimidad virtual y la protección de datos personales

Con el término "datos personales" nos referimos a toda información que se relaciona con los individuos y permiten identificarnos, como por ejemplo, domicilio, nombre completo, DNI, teléfono, situación crediticia, etc.

A partir de la década de 1970 comenzaron a aparecer gran cantidad de archivos con información de índole personal, con una agrupación mínima de datos, como fecha y lugar de nacimiento, filiación, estado civil, domicilio, etc., hasta otra clase de datos con características aún más específicas, como religión, inclinaciones políticas, raza, ingresos, historia clínica, historial bancario, etc. Estos datos suelen ser recopilados en distintas instituciones, como los registros, civiles, censales, bancarios, médicos, académicos, culturales, deportivos, laborales, administrativos, fiscales, etc., a partir del auxilio de medios automatizados, lo que genera una gran sistematización, concentración y disposición instantánea de esa clase de información con distintos objetivos.

Esta clase de datos no son vulnerables de por sí, sino que esto dependerá del destino para el cual van a ser utilizados, que pueden ser muy variados. De esta manera, estas informaciones pueden utilizarse con fines comerciales, publicitarios, fiscales, policiales, etc., y transformarse, de esta forma, en un instrumento de mercantilismo.

La diversidad de las posibles situaciones de indefensión respecto al problema genera que las personas estén a la merced de una gran variedad de situaciones que vulneren sus derechos fundamentales en una sociedad incitada por manipulaciones, discriminaciones, persecuciones, asedios, presiones, entre otros, todo ello dejando de lado un control jurídico propicio.

El 4 de octubre del año 2000 se sancionó la ley nacional de la República Argentina número 25326 de Protección de datos personales.

Esta ley tiene como fin la protección integral de los datos personales que se encuentren en archivos, bancos de datos, registros u otros medios en donde se efectúe tratamiento de datos, ya sean de carácter público o privado, con el fin de brindar informes para garantizar la intimidad de los individuos y el derecho al honor, así como además el acceso a la información que se registre sobre los ciudadanos.

Dicha Ley fue reglamentada por el Decreto 1558/2001, y confiere que cualquier individuo pueda acceder a los datos personales que alguien más mantiene sobre él, y en caso de falsedad, error o desactualización, ordenar la actualización, modificación, supresión, o inclusive reclamar que determinados datos se encuentren bajo confidencialidad.

Las siguientes definiciones fueron extraídas de la ley Protección de datos personales:

- Los datos personales es información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables
- Los datos sensibles son 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 designan, indistintamente, 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
- Por último, el tratamiento de datos tiene que ver con las operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción y, en general, el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias

El artículo 6 de la Ley de Protección de datos personales manifiesta lo siguiente: "Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara:

- La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios;

- La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable;
- El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente;
- Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos;
- La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos."

Por su parte, el artículo 7 hacer referencia a la categoría de datos. El mismo expresa que:

- Ninguna persona puede ser obligada a proporcionar datos sensibles.
- Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.
- Asimismo, queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros.
- Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas.

Por último, el artículo 13 hace hincapié en el derecho a la información, y plantea que "Toda persona puede solicitar información al organismo de control relativa a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables. El registro que se lleve al efecto será de consulta pública y gratuita".

Para poder comprender el derecho a la intimidad, es menester diferenciar la vida del ser humano en su doble espacio: privado y público. Así, la intimidad se comprende como la referencia a un ámbito privado y propio, externo a la injerencia de terceros.

La intimidad respecto a la información abarca aquellas cuestiones de la vida privada de los individuos, cuya comprensión debe ser tutelada desde un punto de vista objetivo. Esta se refiere a la noción de carácter social de aquellas cuestiones de la personalidad que conciernen a la facultad de autodeterminación y a la información protegida desde el enfoque subjetivo, que supone la capacidad de decisión por parte de su titular de la información respecto a cuál pertenece a su ámbito privado.

El derecho a la intimidad consta en la defensa del individuo en su totalidad a partir de una línea que prohíbe dar a conocer o publicar datos respecto a determinados temas, como la política, la religión o la vida íntima. Toda persona va a tener derecho absoluto de mantener su vida en la esfera privada, y bajo ninguna cuestión esto puede ser revelado, aunque se trate de personas muy cercanas.

Conforme al investigador Julio Téllez Valdés, el derecho a la información comprende tres acciones: difundir, investigar y recibir la información. Estas acciones están reflejadas en el derecho a ser informado, así como el deber de informar.

El contenido pasivo se hace consistir en la obligación que tiene el estado de no interferir en la difusión de la información por parte de los particulares. De esta forma, el derecho a la información se encuentra estrechamente relacionado con la libertad de expresión. Desde un punto de vista activo, el derecho a la información se observa desde la obligación que tiene el estado de aportar información.

El derecho a la intimidad y el derecho de información son nociones jurídicas que se hallan en conflicto constante, lo que nos hace distinguir la protección jurídica de datos personales, a partir de la comprensión inicial de los motivos que justifican esta protección. De allí la necesidad de comprender la regulación y la noción del derecho a la intimidad.

Sobre los derechos en internet se puede manifestar que los datos personales de los usuarios de la web circulan muy fácilmente por la red, lo que genera muchos desafíos

que, ni las legislaciones de hoy en día, ni la comunidad de la información, ha sabido hacerles frente.

La incursión de internet en la vida diaria de los individuos ha generado un fenómeno que avanza continuamente y que supone la digitalización de la información personal. Asimismo, los derechos que va a reconocer la Ley de Protección de Datos pueden practicarse en el ámbito de la web.

Lo que en muchos casos se hace complejo respecto a su ejercicio es el lugar inicial de los sitios web, a los cuales les brindamos nuestros datos, como así también la dificultad de identificar al propietario de una página de internet, las diferentes legislaciones que hay en el mundo respecto al tema, y la aceptación de las conocidas "Políticas de Privacidad" de algunos sitios web que inclusive pretenden aplicar otras normativas o implican jurisdicciones extranjeras para implementar los derechos.

La mayoría de las adquisiciones respecto a estas cuestiones se despliegan en las redes sociales. Estas representan, más que cualquier otra plataforma, el conjunto de datos personales e interacciones, por lo que se vuelve el lugar más adecuado para que las empresas muestren sus iniciativas comerciales con bastante ventaja.

Las empresas saben utilizar a su favor las redes sociales y sacan provecho de ese entorno para poder identificar los perfiles de los consumidores, ya que, además, la información personal que mantienen las redes sociales respecto a nosotros suele ser actualizada y precisa.

Asimismo, es importante recordar que las creaciones intelectuales que se publiquen en la web mantienen la misma protección que fuera de la misma. Sin embargo, la simplicidad con la que se puede utilizar y reproducir un objeto ordena que seamos prudentes a la hora de subir fotografías íntimas, ya que estas permiten reconocer a menores de edad, que puedan resultar perjudiciales para alguien, o que afecten derechos otras personas.

Sobre las fotos que son publicadas en un sitio, el autor va a tener derecho a que se distinga su autoría e inclusive, que estas no se usen comercialmente o sin su consentimiento. Por esto, hay que ser muy preciso incorporando los avisos en relación al copyright, y si se considera prudente, incorporando marcas de agua.

Es importante saber cómo podemos hacer como usuarios para proteger nuestros datos personales en lo que implica la web. Por eso, el gobierno argentino publicó en su web oficial algunos consejos para preservar nuestra identidad.

En la web y en las redes sociales:

- Usa contraseñas seguras con mayúsculas, minúsculas, números y símbolos, y cámbialas cada 30, 60 o 90 días
- Usa el modo incógnito para que no se guarden tus contraseñas y tu historial de navegación
- No uses la misma contraseña para los sitios a los que accedes y para las redes sociales
- No ingreses datos personales en sitios desconocidos
- No respondas mails donde te solicitan que completes tus datos personales
- Lee las condiciones de uso de tus datos personales que te proponen las redes sociales o aplicaciones antes de aceptarlas
- No guardes contraseñas en lugares públicos
- En sitios web que requieren el ingreso de usuario y contraseña verifica siempre que la dirección de la página sea auténtica
- Usa sitios seguros si tenés que ingresar datos personales o hacer alguna compra con tarjeta de crédito
- Mira la barra del navegador y fíjate si en la barra de direcciones aparece el "candadito gris o verde" y las letras "https" para estar seguro de que nadie verá tus datos
- Consulta los datos personales que tienen las redes sociales

Por su parte, en los dispositivos:

- Protege tus dispositivos con una contraseña
- Cifra la información de tus dispositivos

- Hace una copia de toda la información una vez por semana
- Activa "Encontrar mi dispositivo" en dispositivos Android o "FindMyPhone" en dispositivos Iphone.
- Usa un antivirus y un antimalware
- Si vas a usar una red pública, usa una Red Privada Virtual o Virtual Private Network, ya que este servicio impide que la información sea vista por otras personas.

Por último, en las aplicaciones:

- Lee los permisos que das cuando instalas aplicaciones
- Si vas a instalar una aplicación para una persona menor de edad, lee la clasificación del juego y el tratamiento de los datos que realizan
- Descarga las aplicaciones sólo de sitios oficiales
- Evita aplicaciones crackeadas, ya que pueden estar infectadas con malware o software espía.

Aunque en muchos Estados se desarrollaron legislaciones estrictas al respecto, al momento de aplicarlas se choca con una realidad más difícil. Algunas complejidades denotan en función a cómo controlar el cumplimiento de leyes locales en un entorno como internet. Si tenemos en cuenta que la actividad de una empresa puede extenderse a todo el mundo gracias a los medios informáticos, ese negocio podría estar exento de la aplicación de la regulación de un determinado Estado, por lo que tendría que someterse a las leyes del estado donde se encuentre dicha actividad.

A partir de la obtención de la información de una persona, una persona puede abrir nuevas cuentas en nombre del titular de la información, obtener fondos de préstamo a su nombre, o retirar fondos desde una cuenta propia de la víctima, como podría ser su línea de crédito hipotecario o su cuenta de cheques. Aunque los delitos de carácter financieros son los más habituales, no van a ser los únicos que se emplean en el robo de identidad de las personas.

Al robo de identidad lo podemos ver de varias formas, pero habitualmente incluye la adquisición de información personal, como la fecha de nacimiento, el nombre de los progenitores, números de cuenta, DNI, dirección, etc., los cuales son utilizados para actividades delictivas, como el empleo no autorizado de tarjetas de crédito o de cuentas bancarias.

Las modalidades más habituales en lo que respecta al robo de identidad:

- Skimming se refiere al hurto de números de tarjetas de crédito y/o débito utilizando un dispositivo específico de almacenamiento al utilizar su tarjeta
- En el Dumpster Diving se intenta identificar dentro de la basura facturas u otros papeles que mantengan información personal
- Changing your address tiene que ver con desvíos de los estados de cuenta hacia otro domicilio para terminar la forma del cambio de dirección
- Por su parte, Phishing se basa en el engaño, en donde se hacen pasar por instituciones o entidades financieras y envían spam, es decir, correo no deseado, para que, de esta manera, revelen la información personal.
- Por último, "Old-fashioned" stealing se refiere al tradicional robo de mochilas y carteras y que de la información obtenida se utilicen estados de tarjetas de crédito, información fiscal, ofertas de crédito aprobadas y cheques nuevos. También bajo esta modalidad se hurtan registros personales de los empleadores para sobornan a los empleados que tienen el correspondiente acceso.

Por lo expuesto, debemos tomar a consideración que el robo de identidad, en sus muchas maneras de efectuarse, es un problemática cada vez más grande y con muchas manifestaciones posibles, teniendo en cuenta principalmente la gravedad de los abusos en los procesadores de tarjetas de crédito de terceros y el robo de cheques impresos.
Recordemos de muchos de estos ilícitos son llevados a cabo a partir de engaños por medio del correo electrónico. Asimismo, los hackers, a partir de las instrucciones en

sistemas informáticos, pueden ayudar significativamente al alcance y al impacto en lo que respecta al robo de identidad.

Legislación Argentina en materia de los ciberdelitos

En la República Argentina, el ordenamiento jurídico de la constitución consignó, a partir de 1853, un sistema de gobierno federal, basado en la división de poderes: Ejecutivo, Legislativo y Judicial.

Podemos decir entonces que al ordenamiento estructural de la jerarquía de las leyes en la República Argentina se lo grafica a partir de una pirámide estableciendo el orden en el que deben ser respetadas, teniendo en cuenta que la norma con un rango inferior no puede contradecir a la norma con un rango superior.

En la punta de la pirámide se encuentra la Constitución Nacional y los Tratados Internacionales de jerarquía constitucional, y por debajo, respectivamente en este orden, las leyes nacionales, las Constituciones Provinciales, las leyes provinciales y la carta orgánica y ordenanzas. Una particularidad que mantiene el conjunto de normas jurídicas es que es evolutivo, es decir, que a medida que transcurre el tiempo, cambia, como también lo hace la realidad misma.

El artículo 18 de la Constitución Nacional establece que “Ningún habitante de la Nación puede ser penado sin juicio previo fundado en ley anterior al hecho del proceso”. Con esto hacemos foco en que si no está tipificada una acción como delito, la misma no va a considerarse como un acto ilícito.

Asimismo, el principio de irretroactividad de la ley consta de que las leyes se dirigen para el futuro y no podrán aplicarse a hechos que transcurrieron antes de ser sancionadas, es decir, no pueden aplicarse de manera retroactiva. De esta manera, si alguien realiza hoy un hecho que no es un ilícito y en unos días una ley lo sanciona como delito, no se puede establecer una facultad punitiva sobre esta persona por aplicación de esa nueva ley, ya que es posterior al hecho cometido.

Ley 26.388

A partir de junio del año 2008, la República Argentina mantiene el marco legal que sancionará a los delitos informáticos. Esta ley es una respuesta jurídica y política que establece una protección legal que vino a llenar el "vacío legal", ya que la Jurisprudencia o las sentencias judiciales no eran uniformes debido a dicho vacío legal.

El caso disparador para la elaboración de la ley fue en el año 2006, cuando espiaron y robaron correos electrónicos de un juez y de un periodista del diario Clarín. Se trata de Daniel Rafecas y Daniel Santoro, respectivamente. Desconocidos espiaron y robaron correos electrónicos del Juez Federal Daniel Rafecas y del periodista de Clarín Daniel Santoro, en una clara violación al derecho a la correspondencia privada y al secreto profesional periodístico.

De esa intromisión informática sacaron copias de mensajes electrónicos en que el juez responde al periodista preguntas "off the record", es decir, para publicar con reserva de la fuente, sobre la causa en que se investiga a dos serbios millonarios por el intento de contrabando de 171 kilos de cocaína a Europa en un operativo conocido como "Viñas Blancas". Este caso fue impulso legislativo para el tratamiento de los proyectos sobre Delitos Informáticos, y de ahí surge la Ley 26388, publicada en el Boletín Oficial el 25 de junio de 2008.

Delitos informáticos incorporados a las legislaciones

El artículo 183 del Código Penal establece que "Será reprimido con prisión de 15 días a un año, el que destruyere, inutilizare, hiciere desaparecer, o de cualquier modo dañare una cosa mueble o inmueble o un animal, total o parcialmente ajeno, siempre que el hecho no constituya otro delito más severamente penado."

Sin embargo, la nueva incorporación al artículo 183 sobre el daño informático 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".

Por su parte, el artículo 184 expresa que la pena será de 3 meses a 4 años de prisión si mediare cualquiera de las circunstancias siguientes:

- Ejecutarlo en archivos, registros, bibliotecas, museos o en puente, caminos, paseos u otros bienes de uso público; o en datos, documentos, programas o sistemas informáticos públicos
- 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.

El artículo 172 del mismo Código hace referencia al fraude informático, y manifiesta que "Será reprimido con prisión de un mes a seis años, el que defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negociación o valiéndose de cualquier otro ardid o engaño".

Asimismo, el artículo 173 expone que "Sin perjuicio de la disposición general del artículo precedente, se considerarán casos especiales de defraudación y sufrirán la pena que él establece…". Aquí, en este artículo, se incorpora el inciso 16, que plantea que "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."

La alteración de prueba está presente en el artículo 255 de la Ley de Delitos Informáticos, y plantea que "Será reprimido con prisión de un mes a cuatro años, 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 750 a $12.000."

En cuanto a la pornografía infantil, el artículo 128 de la misma ley manifiesta que "Será reprimido con prisión de seis meses a cuatro años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de 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".

Posteriormente, el artículo continúa: "Será reprimido con prisión de cuatro meses a dos años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización. Y será reprimido con prisión de un mes a tres años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce años."

En cuanto a los delitos contra la privacidad, el artículo 153 sostiene que "Será reprimido con prisión de 15 días a seis 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."

Asimismo, el artículo prosigue manifestando que "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 mes a un 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."

Por su parte, el artículo 153 bis expresa que "Será reprimido con prisión de quince días a seis 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 mes a un 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."

El artículo 155 manifiesta que "Será reprimido con multa de $1.500 a $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…"

En cuanto al artículo 157, este expone lo siguiente: "Será reprimido con prisión de un mes a dos años e inhabilitación especial de uno a cuatro años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos."

El artículo 157 Bis dictamina que "Será reprimido con la pena de prisión de un mes a dos años el que:

- A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;
- 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.
- 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 uno a cuatro años."

Por último, sobre los delitos contra la seguridad pública se puede expresar que el artículo 197 anuncia que "Será reprimido con prisión de seis meses a dos años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida".

Podemos decir que la Ley 26.388 ha sido una solución reclamada por diversos sectores académicos, instituciones, y los sectores privados y estatales. Los grandes cambios de la informática que se dan de manera continua nos obligan a estar alertas de manera constante para solicitar los cambios que la realidad imponga.

Grooming.

El verbo "to groom" tiene como significado la preparación a alguien para un rol específico, es decir, con finalidad determinada. Este involucra diversas caracterizaciones que ponen enfoque en la noción de la seducción, otras dirigen el concepto de grooming en base de la idea de pedofilia y, por último, la idea más aceptada, que expone el fenómeno a partir de la idea de una sucesión de acciones para ganar la confianza de la víctima.

A partir de esto podemos afirmar que los conceptos que mantienen más aceptación en la comunidad científica alrededor del mundo son los que derivan la definición del grooming a la noción de proceso que conduce a ganarse la confianza de la víctima, que en la mayoría de legislaciones, como en la de Argentina, va a tratarse de menores.

Definimos entonces al grooming como al acoso sexual a través de internet de niños, niñas y adolescentes.

En tal sentido, Rachel O'Connell, directora de la unidad de investigación del ciberespacio en la Universidad Central de Lancashire, identificó en el año 2003 las cinco fases que ocurren en el Grooming:

- En primer lugar, la fase de establecimiento de amistad, que implica que el victimario conoce al niño.

- Luego llega la fase de establecimiento de la relación, que es una continuación de la primera fase, en la cual el adulto puede iniciar conversaciones sobre cuestiones vinculadas con la vida del menor, como por ejemplo, el colegio, su casa y su familia, generando habitualmente una relación de amistad con él.
- Después sigue la fase de valoración del riesgo, en donde el abusador pasa a preguntar para obtener información respecto de las posibilidades de detección de su conducta por parte de los padres, es decir, respecto a cuestiones como en qué lugar de la casa mantiene su computadora y cuáles son los otros usuarios del mismo.
- En la fase de exclusividad la conversación se vuelve más personal o privada y el menor es incitado a revelar secretos y problemas personales.
- Por último está la fase sexual, que empieza cuando el adulto lleva la conversación hacia un lugar en que la confianza entre ambos parece ya asentada. Habitualmente en esta fase es cuando se produce la mayor parte de intercambios, propios de estas modalidades. Acá es cuando el abusador, quien ya dispone de toda la información, tiene el objetivo de establecer esa relación sexual con el menor a través del chantaje.

La Ley 26904 es la Ley de Grooming en Argentina. Al momento en el que fue aprobada la ley por parte del Senado, se encontraba ya instaurada una Comisión con el objeto de llevar adelante una reforma del Código Penal actual, denominada "Comisión para la Elaboración del Proyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación". Sin embargo, no se mantuvo una comunicación entre el Congreso y dicha Comisión a fin de arribar a un texto consensuado.

Además, el texto aprobado también ha estado sujeto a críticas por parte de distintos sectores. Como ejemplo de esto citamos a la Licenciada en Comunicación Social y Presidenta de la organización civil sin fines de lucro llamada Fundación Vía Libre, Beatriz Busaniche, que informa que el proyecto aprobado en Senadores "(…) no sirve para proteger y tutelar el bien jurídico que se supone debe defender, es decir: la integridad de los menores."

En el año 2012, el Poder Ejecutivo de la Nación Argentina llevó a cabo, a partir del Decreto 678/1225, una "Comisión para la Elaboración del Proyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación". El presidente de la comisión fue el Dr. Eugenio Zaffaroni, y estaba integrada por representantes de varios sectores políticos.

Finalmente, la Cámara de Senadores aprobó en Noviembre del 2013 la Ley número 26.904, en la cual se incluyó bajo el título de "Delitos contra la integridad sexual" un artículo en el Código Penal que tipifica el grooming como delito.

El texto aprobado dispone en su artículo 131 lo siguiente: "Será penado con prisión de seis meses a cuatro años 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."

A su vez, el Decreto 349/2018 promulgó la Ley 27436, que castiga la simple tenencia de material pornográfico infantil. Esto es "toda representación de un menor de 18 años dedicado a actividades sexuales explícitas o de sus partes genitales con fines predominantemente sexuales".

Esta ley, que modifica el artículo 128 del Código Penal, establece que será sancionado con penas de prisión de tres a seis años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio pornografía infantil. La escala penal anterior era de seis meses a cuatro años.

Además, se reprime con prisión de entre seis meses a dos años para quien tenga material "con fines inequívocos de distribución o comercialización". En este caso, la sanción también aumentó, pero solo en el mínimo, ya que en el pasado era de cuatro meses a dos años.

En el último párrafo del artículo se establecen penas de prisión de un mes a tres años para quien facilite el ingreso a espectáculos pornográficos o entregue pornografía de menores de 14 años.

Grooming Argentina es una organización no gubernamental que fue creada con el fin de trabajar fundamentalmente sobre tres ejes, basados en la concientización, prevención y erradicación del grooming en el país.

La ONG está formada por un grupo de profesionales interdisciplinarios con el fin a tratar este tema que avanza de manera prominente con el advenimiento de las redes sociales y las nuevas tecnologías. A su vez, dicha organización trabaja junto a distintas organizaciones privadas, públicas y organismos de cooperación internacional para implementar iniciativas para la promoción y el cumplimiento de los derechos de los menores en el tratamiento de este delito.

Recomendaciones de cómo proceder con la evidencia de los delitos informáticos para poder denunciar.

- Es muy importante no destruir o modificar la información que mantiene en su computadora, celular, u otro dispositivo electrónico, vinculada al hecho. Es necesario recordar que siempre la integridad de la información es fundamental para poder proceder con las causas penales que se inicien
- Asimismo, no se deben reenviar los mensajes que constituyen el delito
- Y también es importante guardar, con el fin de resguardar la prueba correctamente. Una vez efectuada la denuncia, hay que proceder de la forma en que indique el investigador.

Ante hechos de delitos informáticos, es importante denunciar inmediatamente. Existen distintas alternativas en toda la Argentina para realizar una denuncia o solicitar asesoramiento de equipos especializados. Asimismo, es posible presentarse ante una fiscalía o hacer la denuncia ante una dependencia policial.

El grooming, así como cualquier otro delito informático, puede ser denunciado en la Ciudad de Buenos Aires en la Fiscalía de la Ciudad Autónoma de Buenos Aires, en la Unidad Fiscal Especializada en Ciberdelincuencia, en la Dirección Nacional de Protección

de Datos Personales, y en el Instituto Nacional contra la Discriminación, la Xenofobia y el Racismo, más conocido como INADI. También existe un teléfono gratuito, que es el 137. En esta línea directa se puede denunciar casos de grooming, además de abuso y trata.

Ante todos los casos expuestos, las autoridades policiales y fiscalías tienen siempre la obligación de tomar tu denuncia.