UNCUYO
UNIVERSIDAD
NACIONAL DE CUYO

FACULTAD DE DERECHO

TESIS DE MAESTRÍA

"LOS DELITOS INFORMATICOS EN ARGENTINA A PARTIR DE LA ADHESION AL CONVENIO DE BUDAPEST"

MAESTRIA EN DERECHO PENAL Y CIENCIAS PENALES

Alumno: CARLA V. CRUZADO **Director: JUAN PABLO CHALES**

MENDOZA, Marzo, 01 de 2021

ÍNDICE

INTRODUCCION:

En la actualidad, las computadoras se utilizan no solo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino como medio eficaz para obtener y conseguir información.

La informática está hoy presente en casi todos los campos de la vida moderna.

El progreso de los sistemas computacionales permite procesar y poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza.

Las más diversas esferas del conocimiento humano están siendo incorporadas a sistemas informáticos que en la práctica cotidiana, entregan con facilidad, a quien lo desea, un conjunto de datos que, hasta hace unos años, solo podían ubicarse luego de largas búsquedas y selecciones en los que el hombre jugaba un papel preponderante y las máquinas existentes tenían el rango de auxiliares para plasmar los resultados. Hoy, la situación se ha invertido, y éste enorme caudal de conocimientos puede obtenerse en segundos o minutos, transmitirse y llegar al receptor mediante sistemas sencillos de operar.

Podemos sostener que en la actualidad las perspectivas de desarrollo de la informática no tienen límites previsibles y que aumenta en forma constante, y que estamos en presencia de un fenómeno científico tecnológico.

Es precisamente el progreso de las computadoras, el creciente aumento de las capacidades de almacenamiento y procesamiento, la fusión del proceso de la información con las nuevas tecnologías de comunicación, ejemplifican el desarrollo actual definido como la “era de la información”.

Esta evolución de la informática, trae aparejado distintos problemas de significativa importancia para el funcionamiento y la seguridad de los sistemas informáticos en los negocios, en la administración, la defensa y la sociedad.

La creciente incorporación de los sistemas informáticos, en la organización y administración de empresas, en la administración pública, en el Poder Judicial, trae aparejada como contrapartida lo que se conoce como “criminalidad informática”.

Nuevas formas de delincuencia antes impensables, han surgido de este desarrollo informático. Así, podemos mencionar la manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos, la utilización indebida de la información que puede afectar el derecho a la intimidad, etc. Es a través de estos procedimientos, que se pueden obtener grandes beneficios económicos o causar importantes daños.

Pero no solo la cuantía de los perjuicios así ocasionados es superior a la que es usual en la delincuencia tradicional, sino que también son mucho más elevadas las posibilidades de que no lleguen a descubrirse. Se trata de una delincuencia de especialistas.

En este sentido la informática puede ser el objeto del ataque o el medio para cometer otros delitos. La informática reúne las características que la convierten en un medio para cometer otros atentados, en especial de carácter patrimonial. La idoneidad proviene, básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente facilidad de acceso a ellos y la relativamente fácil manipulación de esos datos.

Para poder adentrarnos al estudio de los delitos informáticos y los relacionados con las redes sociales, en necesario introducirnos brevemente en el conocimiento y manejo de lo que es la computadora a nivel operacional y estructural, ya que ésta puede ser objeto o utilizarse como medio comisivo para dichas conductas delictivas, así como la noción de diferentes conceptos relacionados con computadoras e Internet[1].

De manera elemental, diremos que las computadoras son máquinas automatizadas de propósito general, integrada por los elementos de entrada, un

[1] CATALA, Gabriel H. Tobares, CASTRO ARGÜELLO, Maximiliano J., “Delitos Informáticos”, Córdoba, Advocatus, 2009, p. 19.

procesador central, dispositivo de almacenamiento y elementos de salida, ello nos da la pauta para considerar sus componentes fundamentales a nivel operacional, a saber:

- Dispositivo de entrada: representado por la forma de alimentación de la información de la computadora, por medio de datos e instrucciones (pantalla, lectoras de soporte magnéticos, discos, disquetes, etc.). Si los datos son nuevos para el sistema en su conjunto se toma de dispositivos de entrada, si ya se encontraban en dispositivos se toma de dispositivo de almacenamiento.

- Dispositivo de salida: son los equipos por medio de los cuales, datos contenidos en los sistemas de cómputos son representados para su disposición.

- Procesador Central: comúnmente conocido como CPU, es donde se llevan a cabo las transformaciones indicadas por los programas aplicados, ya sea de obtener los datos a considerar, la decisión de ejecutarlos, el sentido de elaboración y la forma de guardar y/o exponer la información elaborada.

- Dispositivo de almacenamiento: el cual almacena la información, permite guardar grandes volúmenes de información para su utilización por el sistema de computación, se entiende "soporte" de almacenamiento medio físico que contiene los datos, y como "dispositivo" de almacenamiento a la unidad que puede leer y/o grabar esos datos.

- *Hardware*: constituido por las partes mecánicas, electromecánicas y electrónica, como estructura física, encargada de la captación, almacenamiento y procesamiento de información, así como de la obtención de resultados.

-*Software*: es el conjunto de instrucciones que controlan el funcionamiento del sistema de computación, está compuesto por programas que se cargan en la unidad central del proceso para su ejecución.

Por otro lado, la noción de "informática" es un neologismo derivado de la palabra información y automatización, sugerido por Phillipe Dreyfus en 1962. En sentido general, la "informática" es un conjunto de técnicas destinadas al tratamiento lógico y automático de la información para una mejor toma de decisiones.

Sumado a las anteriores concepciones, nos encontramos con el término "Telemática", utilizado para englobar todo lo que abarca la revolución

tecnológica acelerada, en los campos afines de telecomunicaciones, computadores, microinformática y banco de datos. Y, para ello, al trabajar con comunicaciones de datos, encontramos dos grandes modalidades conocidas como “trabajo en línea”. Se dice que un equipo está en línea cuando está vinculado al sistema de computación y puede ser accedida desde él y “trabajo en tiempo real” tiene como condición necesaria el trabajo en línea[2].

La definición que podemos dar de “Internet”, es que no es un cuerpo físico o tangible, sino una red gigante que interconecta una innumerable cantidad de redes locales de computadoras. Es la red de redes. Es un sistema internacional de intercambio de información que une personas, instituciones, compañías y gobiernos alrededor del mundo, de manera que casi instantánea, a través del cual es posible comunicarse con un solo individuo, con un grupo amplio de personas interesadas en un tema específico o con el mundo en general. En términos generales, Internet se ha convertido en un polémico escenario de contrastes en donde todo es posible: desde encontrar información de contenido invaluable de alcances insospechables en el ámbito de la cultura, la ciencia y el desarrollo personal, hasta caer en el terreno del engaño, la estafa, la corrupción de menores[3].

Internet surgió de un desarrollo realizado a instancia del Departamento de Defensa de los EE. UU. A principio de la década de los ´70, en plena “Guerra Fría” entre Occidente y Europa del Este, el Departamento de Defensa advirtió la dependencia de EE.UU. con respecto a su sistema de comunicaciones, centralizado, donde una serie de computadoras tenía el “control del sistema”, el resto dependían de ellas. Así, las autoridades del departamento de defensa concibieron la idea de una red en la cual todos los nodos fueran jerárquicamente equivalentes, de manera tal que si una fuera destruida el resto pudiera continuar su trabajo. Fue entonces cuando, bajo el auspicio de la Agencia de Programas Avanzados de Investigación (ARPA), en un programa dirigido por Robert Kahn, Vincent Cerf desarrollo en 1973, los protocolos TPC/IP (protocolo de control de la transmisión/protocolo entre redes), base de la actual Internet, se estableció una red denominada ARPAnet, vinculando primeramente unidades militares y laboratorios de

[2] Por ejemplo, al autorizar una compra con tarjeta de crédito nos encontramos con el dispositivo terminal POS, está comunicado con el sistema de computación (está en “línea”) y, adicionalmente se da respuesta “en tiempo real” al evento de compra, verificando la disponibilidad de saldo, actualizando y dando respuesta de “transacción aprobada”. (FREIJEDO, Claudio F. y CORTAGERENA, Alicia, Tecnología de la Información y las comunicaciones, Bs. As., 2000, p.63)

[3] Biblioteca-artículo electrónico del Supremo Tribunal de Justicia del Estado de Michoacán (México). Disponible en http://www.tribunalmmm.gob.mx/biblioteca/aldemadelia/indice.htm.

investigación, para luego convertirse en una red abierta en la década pasada para fines comerciales[4].

Actualmente, cualquier persona puede ofrecer su propia página, un lugar virtual o abrir su propio foro de discusión. En ellos, se aborda temas muy interesantes hasta muy deleznables, incluyendo comportamientos criminales. Dando origen a las famosas “Redes Sociales” siendo las más importantes “Facebook” y “Twitter” compuestas por millones de usuarios.

El espíritu de la información que se maneja en Internet es que sea pública, libre y accesible a quien tenga la oportunidad de entrar en la red, lo cual marca un principio universalmente aceptado por los usuarios y que ha dado lugar a una normativa sin fronteras y de lo cual podemos deducir, en términos jurídicos, cuál sería la ratio iuris o razón de ser de ésta especial normatividad. Se intenta que Internet sea un medio interactivo viable para la libre elección, la educación y el comercio.

Los individuos tienen una amplia gama de formas de introducirse a Internet, a través de los proveedores de acceso a Internet, conocidos en el medio de las telecomunicaciones. En términos de acceso físico, se puede usar una computadora personal, conectada directamente -por cable coaxial o fibra óptica- a una red -un proveedor de servicios de Internet, por ejemplo- que esté, a su vez, conectada a Internet; o puede hacerse desde una computadora personal con un modem conectado a una línea telefónica a fin de enlazarse a través de ésta a una computadora más grande o a una red, que esté directamente conectada a Internet. Ambas formas de conexión son accesibles a las personas en una amplia variedad de instituciones académicas, gubernamentales o comerciales. Lo cierto es que hoy en día el acceso a Internet es cada vez más sencillo en Universidades, bibliotecas y los llamados “cibercafés”.

Tan importante se ha convertido el acceso a Internet, sobre todo en un contexto en el que la pandemia obliga a buena parte de los argentinos a trabajar desde los hogares, que el Gobierno Nacional, dictó el DNU N° 69/20, el cual se publicó en la edición del 22 de agosto del Boletín Oficial el Decreto de Necesidad y Urgencia denominado "Argentina Digital" DNU N° 690/20, mediante el cual en su artículo 15 dispone: “Carácter de servicio público en competencia. Se establece que los Servicios de las

[4] FREIJEDO, Claudio F. y CORTAGERENA Alicia B., ob. Cit., p.3)

Tecnologías de la Información y las Comunicaciones (TIC) y el acceso a las redes de telecomunicaciones para y entre licenciatarios y licenciatarias de servicios TIC son servicios públicos esenciales y estratégicos en competencia. La autoridad de aplicación garantizará su efectiva disponibilidad". En el mismo se establece "Que el derecho de acceso a internet es, en la actualidad, uno de los derechos digitales que posee toda persona con el propósito de ejercer y gozar del derecho a la libertad de expresión. La ONU ha expresado en diversos documentos la relevancia de las Tecnologías de la Información y las Comunicaciones (TIC) para el desarrollo de una sociedad más igualitaria y la importancia de que a todas las personas les sea garantizado su acceso a las mismas…".[5]

En Internet encontramos diferentes servicios, que requieren el software apropiado en la computadora que hace uso de ellos. Los servicios más importantes, en general, son los siguientes:

a) Correo electrónico, siendo el servicio de mayo uso, de mayor tráfico, por lo tanto de mayor importancia en el surgimiento, en la actualidad de diversas relaciones contractuales.
b) Transferencia de Archivos, que permite transferir archivos, los cuales pueden ser de texto, gráficas, hojas de cálculo, programas, sonido y video.
c) Acceso remoto a recursos de cómputo por interconexión, es una herramienta interactiva que permite introducirse, desde una computadora en casa o en la oficina, a sistema, programas y aplicaciones disponibles en otra computadora, generalmente ubicada a gran distancia y con gran capacidad.
d) Word Wide Web, por medio del cual se pueden transmitirse textos gráficos, imágenes y sonido. Es un conjunto de sistemas de archivos, denominados "paginas" o "sitios" que incluyen información multimedia y vínculos a otros sitios.
e) Grupos de discusión.
f) Comunicación en tiempo real (Chat), es la posibilidad de establecer diálogos inmediatos en tiempo real, a través de Internet, permitiendo a dos o más personas "dialogar" simultáneamente por escrito, sin importar distancia geográfica. Esta forma de comunicación es análoga a la línea de teléfono, sólo que emplea el teclado o monitor en lugar de auricular.

[5] DECNU-2020-690-APN-PTE - Ley N° 27.078. Modificación

Ahora bien, al intentar conceptualizar nuestra temática de estudio es importante, previo a delimitar el ámbito de aplicación de las leyes, doctrina y jurisprudencia sobre el tema[6], determinar, en primer término, de qué estamos hablando cuando nos referimos a los delitos informáticos, o de alta tecnología y relacionados con redes informáticas, debido a que la doctrina no se ha mantenido pacífica frente al tema, ni mucho menos direccionada a un punto común. En el ámbito internacional se considera que no existe una definición propia del delito informático, sin embargo, muchos han sido los esfuerzos de expertos que se han ocupado del tema, y aún no existe una de carácter universal[7].

Acercarnos al concepto de delito informático implica afirmar que éste abarca, por una parte, la amenaza a la esfera privada del ciudadano mediante la acumulación, archivo, asociación y divulgación de datos obtenidos mediante computadoras y, por otra parte, delitos patrimoniales, por el abuso de datos procesados automáticamente, que es el sector que en mayor medida se ha dedicado a estudiar la doctrina[8].

Es decir, que puede comprender aquellas conductas que recaen sobre herramientas informáticas propiamente tales, llámense programas, ordenadores, etc., como aquellas que valiéndose de estos medios lesionan otros intereses jurídicamente tutelados como la intimidad, el patrimonio económico, la fe pública, entre otros[9].

Por ello, surgían diversas consideraciones con relación a que los delitos informáticos, como tales, no existían, o no podían ser verificados, se afirmaba que solamente eran delitos comunes que lo único en que se podían diferenciar de otro delito cualquiera, era en cuanto a las herramientas utilizadas o en los objetos que vulneraban. Sin embargo, esa era una visión muy limitada de la realidad, que sólo se podía sostener si se

[6] Se puede definir a los delitos informáticos como “aquellas acciones típicas, antijurídicas y culpables, que recaen sobre la información, atentando contra su integridad, confidencialidad o disponibilidad como bien jurídico de naturaleza colectiva o macrosocial (abarcativo de otros intereses, v.gr., propiedad común, intimidad, propiedad intelectual, seguridad pública, confianza en el correcto funcionamiento de los sistemas informáticos, etc.) en cualquiera de las fases que tienen vinculación con su flujo o intercambio (ingreso, almacenamiento, proceso, transmisión y/o egreso), contenida en sistemas informáticos de cualquier índole, sobre los que operan las maniobras dolosas” (HOCSMAN, Heriberto Simon, “Delitos Informáticos”, Simposio Argentino de Informática y Derecho 2003).
[7] http.//personales.ciudad.com.ar/roble/thaisdelitosinformaticos.htm
[8] SAEZ CAPEL, José, Informática y Delito, 1° Ed., Proa XXI Editores, Bs. As. 1999, p. 27.
[9] http.www.delitosinformaticos.com/delitos/colombia

pensaba tan solo en el tipo de apunte informático falso en un banco o del robo de una cantidad de dinero gracias a la utilización de una tarjeta de crédito. Pero existían muchas otras conductas que difícilmente se podían tipificar con las leyes existentes con anterioridad a la 26.388, por lo que resultaba de imperiosa necesidad la adopción de un nuevo régimen legal conforme a la nueva realidad que imponía el uso de las tecnologías de la información[10].

Es cierto, de todas formas, que un delito informático podía ser simplemente un delito "clásico" en un nuevo envoltorio. Lo que ocurre es que no es sólo eso; además, el avance que está sufriendo Internet en número de usuarios, que parece colapsarse en cualquier momento, hace que haya que actuar rápidamente ante los posibles delitos que puedan cometerse a través de ella.

Es así que algunos definen al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas"; otros como "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de acción criminógena". Por su parte el Departamento de Justicia de Estados Unidos de América definió al delito informático como "cualquier acto ilegal que requiera el conocimiento de tecnología informática para su perpetración, investigación o persecución." [11]

Tales definiciones son suficientemente ilustrativas, por lo que tan sólo agregaríamos la categoría denominada "delincuencia informática".

De manera tal que, al momento de conceptualizar este nuevo fenómeno delictivo, podemos decir que los delitos informáticos son aquellas conductas ilícitas, susceptibles de reproche y pasibles de sanción por el derecho penal, en las cuales se utilizan de manera indebida cualquier medio, mecanismo y/o sistemas informáticos, ya sea como fin en sí mismo o como medio para la comisión de otro delito.

Previo a la sanción de la ley 26.388, existían acciones u omisiones informáticas reprochables que reunían características para ser catalogadas como futuros delitos informáticos, ya sea llevadas a cabo utilizando un elemento tecnológico

[10] http./www.derechotecnológico.com/delitos.html
[11] RUDI, Jorge Adrian, "Las Actas de 1984 y 1986 sobre delitos informáticos en Estados Unidos de América", E. D., t. 159-1994-2,ps. 1055/1061, citado por Riquert, ps. 35 y 36.

o vulnerando los derechos del titular de un soporte informático (hardware o de software); contexto que fue advertido por nuestro legislador, dado el vacío legal imperante en la época y que se tradujo, luego de muchos proyectos legislativos y discusiones doctrinarias, en nuestra normativa en la materia[12].

En ese orden de ideas, resulta adecuada, la clasificación efectuada por Julio Téllez Valdez:

- Como instrumento o medio: en esta categoría se encuentra las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:
    - Falsificación de documentos vía computarizada (tarjeta de crédito, cheques, etc.);
    - Variación de los activos y pasivos en la situación contable de las empresas;
    - Planeamiento y simulación de los delitos convencionales (robo, homicidio, fraude);
    - Lectura, sustracción o copiado de información confidencial;
    - Modificación de datos tanto en la entrada como en la salida;
    - Aprovechamiento indebido o violación de un código para penetrar un sistema, introduciendo instrucciones inapropiadas;
    - Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa;
    - Uso no autorizado de programas de cómputo;
    - Introducción de instrucciones que provocan interrupciones en lógica interna de los programas;
    - Alteración en el funcionamiento de los sistemas, a través los virus informáticos;
    - Obtención de la información residual impresa en papel luego de la ejecución del trabajo;
    - Acceso a áreas informatizadas en forma no autorizadas;
    - Intervención en las líneas de comunicación de datos o teleproceso.

[12] TOBARES CATALA, Gabriel H., CASTRO ARGÜELLO, Maximiliano J., ob. Cit. P. 3

- Como fin u objeto: en esta categoría se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como, por ejemplo:
    - Programación de instrucciones que producen un bloqueo total al sistema;
    - Daño a los dispositivos de almacenamiento;
    - Atentado físico contra la máquina o sus accesorios;
    - Sabotaje político o terrorismo en que se destruye o surja un apoderamiento de los centros neurálgicos computarizados.
    - -Secuestro de soportes magnético en lo que figure información valiosa con fines de chantaje (pago de rescate, etc.)[13].

Por otra parte, el autor Moisés Barrio André, en su obra "Ciberdelitos 2.0", señala "…en la actualidad si resulta evidente la existencia de una ulterior generación de delincuencia. La apertura del ciberespacio[14] no solo ha traído beneficios y progreso en la comunidad, sino que también ha sido una herramienta para generar nuevas formas delictivas antes desconocidas tales como el Malware[15], Ransomware[16] , Pharming[17], entre otros.

Asimismo, ha permitido la comisión de delitos clásicos como la suplantación de identidad, el fraude y acoso, a través de la red, logrando un mayor alcance y extensión a la vez que el medio dificulta su persecución *(Hackers, Cracker, Virucker, Phisher,* etc), vinculada a las TIC y la sociedad digital: "el cibercrimen" o "ciberdelincuencia", caracterizado por la utilización de internet, bien como entorno en el que

[13] www.universidadabierta.edu.mx/Biblio/E/Estrada%20MiguelDelitos%20informaticos.htm

[14]El ciberespacio se ha definido como un espacio virtual de interacción que surge directamente como un lugar relacional, es decir su existencia solo será efectiva cuando haya intercambio de información, siendo por tanto espacio y medio. (AGUIRRE Romero, Joaquín. Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo XXI. Biblioteca virtual universal, Universidad Complutense de Madrid. Pág. 1. [en línea] [consulta: 01 de junio de 2020]

[15] Es un "software malicioso" que se inserta en los sistemas operativos o discos duros de computadores y smartphones para recolectar la información que genera el usuario. Por lo general su descarga es automática y sin previo conocimiento del usuario como archivo adjunto desde emails publicitarios falsos, páginas web, o aplicaciones.

[16] Este ciberdelito hizo su debut mundial en 2017 con "Wannacry", programa informático malintencionado que impidió el acceso a la información de determinados archivos o todo el disco duro de computadores de empresas en todo el mundo. Su valor está en que cifra los datos para hacerlos imposibles de acceder excepto por un sistema de descifrado específico que los hackers desarrollan para ese fin, previo pago de una cuantiosa suma de dinero o bitcoins

[17] Es la explotación de una vulnerabilidad en el software de los servidores que permite al atacante redirigir un nombre de dominio a otra computadora distinta, de esta forma cuando el usuario ingrese un nombre de dominio será redirigido al que el atacante haya especificado.

son atacados los propios sistemas electrónicos o sus archivos y programas, bien como medio comisivo de múltiples actividades ilícitas."[18]

En el ámbito de organismos internacionales también se han enfocado esfuerzos destinados a enmarcar las conductas que hoy analizamos, intentando de alguna manera ordenarlas y categorizarlas. Así es que esta nueva categoría dogmática de la "ciberdelincuencia" ya cuenta con el apoyo de la propia legislación internacional en el Convenio de Budapest.

De allí, que podemos concluir que los ciberdelitos, conforman una nueva generación de infracciones penales, que se cometen en el ámbito de Internet, entre los cuales podemos mencionar; interceptación de las comunicaciones *(hacking*), la protección de la intimidad, la privacidad y la imagen, el ciberacoso (*cyberbullying*), los daños y sabotajes *(cracking*), el ciberterrorismo, el abuso de sistemas informáticos (*phreaking*), los fraudes y estafas a través de internet, la publicación ilegitima de imágenes íntimas o porno venganza (*sexting y revenge porn*), el *grooming* y los delitos contra la propiedad intelectual.

Todo ello, acarrea el desafío de contar con un derecho penal moderno, con herramientas prácticas, que se adecue a la realidad social y recurriendo a distintos modelos de intervención como, por ejemplo, adelantamiento de la intervención punitiva a momentos previos a la lesión, delito de peligro abstracto, bienes jurídicos colectivos o supraindividuales, sin abandonar los criterios tradicionales de imputación y las garantías básicas del Estado constitucional de derecho.

En este marco, aparece una nueva disciplina -la computación forense- como respuesta al reto de encontrar la verdad en el análisis de la información almacenada en los componentes tecnológicos, de tal forma que pueda dar claridad mediante los hechos electrónicos identificados.

Ahora bien, es necesario aclarar que la protección de los sistemas informáticos y de los datos debe ser abordada desde los distintos ordenamientos

[18] BARRIO ANDRES, Moisés. "Ciberdelito 2.0. Amenazas criminales del ciberespacio", Astrea, Buenos Aires, 2020, pág. 8.

jurídicos. Sólo a través de una protección global es posible alcanzar una cierta eficacia en la defensa de los ataques que aquellos sufren.

En la actualidad, el fenómeno de la cibercriminalidad no solo es abordado por los diferentes organismos gubernamentales y fuerzas de seguridad sino también por organismos internacionales, con el objetivo de fortalecer la cooperación entre países y la armonización penal de los delitos informáticos.

El Convenio sobre la Cibercriminalidad del Consejo de Europa se presenta como la única solución internacional existente para el tratamiento de la cuestión ciberdelictual. Se convierte en una adecuada herramienta para la armonización legislativa interestatal y la lucha contra el ciberdelito.

Como resultado de esta problemática, en noviembre del año 2001 se firmó el Convenio sobre ciberdelincuencia en la ciudad de Budapest por los miembros del Consejo de Europa (C.O.E.- Council of Europe) con el objeto de llevar a cabo una política penal común destinada a prevenir la criminalidad en el ciberespacio y, en particular, mediante la adopción de una legislación apropiada, es decir, acorde al derecho interno de cada Estado, y la mejora de la cooperación internacional. Dicho Convenio constituye el piso mínimo a fin de estar al día en materia de delitos informáticos y de armonización legislativa al respecto.[19]

El mencionado Convenio se presenta como una solución internacional para el tratamiento de la cuestión ciberdelictual, convirtiéndose en un adecuado instrumento para la adecuación legislativa interestatal y de lucha contra el ciberdelito.

Este convenio, a más de establecer las pautas de definición de los ciberdelitos, constituye una herramienta eficaz, tal como surge de su propio Preámbulo, "…para prevenir los actos atentatorios de la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos, así como su uso fraudulento de tales sistemas, redes y datos, asegurando la incriminación de dichos comportamientos, como los descritos en el presente Convenio, y la atribución de poderes

[19] CHALES, Juan Pablo, "Las técnicas de investigación penal a la luz del Convenio sobre Ciberdelitos y su aplicación en Argentina". Tesis de Maestría. UNCUYO, 2018, pág. 10.

suficientes para permitir una lucha eficaz contra estas infracciones penales, facilitando la detección, la investigación y la persecución, tanto a nivel nacional. Como internacional, y previendo algunas disposiciones materiales al objeto de una cooperación internacional rápida y fiables".

Es de soslayar que el objeto del mismo lo constituye la necesidad lograr la unión más estrecha entre sus miembros y de llevar a cabo una política penal destinada a prevenir el delito en el ciberespacio y, en particular, de hacerlo mediante la adopción de una legislación apropiada y la mejora de la cooperación internacional.

A la fecha, Budapest ha sido ratificado por 60 estados, junto a los Estados miembros de la Unión Europea, el Convenio ha sido ratificado por países no europeos, entre ellos Estados Unidos, Canadá, Australia, japón, Israel, República Dominicana, Chile, Argentina, Colombia, entre otros.

Es de destacar que, en Argentina, el Código Penal data de comienzos del siglo XX, cuando esta era de la información no se iniciaba aún. Sin embargo, a partir de la década del ´90, se sancionaron leyes que ya incluían figuras penales informáticas. Tal es el caso de la Ley 24.766 de secretos comerciales (1996), la Ley 24.769 Régimen penal Tributario (1997), la Ley 25.036 de Derechos de Autor (1998), la Ley 25.326 de Protección de Datos, la Ley 25.506 de Firma digital (2001), la Ley 25.520 de Inteligencia (2001), la Ley 25.930 que reformó el concepto tradicional de defraudación (2004), la Ley 25.891 de celulares (2005).

Sin embargo, y a más de ello, el Convenio de Budapest, ha tenido incidencia en la legislación argentina, motivando la sanción de la Ley de Delitos Informáticos (Ley N°26.388), y posteriores reformas, que incorporaron distintos tipos penales y actualizaron algunos conceptos jurídicos, en consonancia con el primero.

Esta reforma significó no solo una actualización de nuestra legislación penal, sino que implica un cambio de concepción en muchos conceptos legales que el avance tecnológico había dejado obsoletos, así como también la incorporación de nuevos tipos penales y la actualización de algunos ya existentes.

Es de destacar, que nuestro país adhirió al Convenio de Budapest en el año 2017, mediante la Ley N° 27.441. Tal adhesión responde a la necesidad

de articular una política penal común, a prevenir 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.[20]

Es importante, tener en cuenta que Argentina, al momento de la adhesión al Convenio, realizó importantes Reservas, basadas en nuestra tradición legislativa clásica en materia jurídico penal.

Asimismo, y con posterioridad, se sancionaron importantes leyes nacionales, a los fines de cumplir con el compromiso internacional asumido al adherirnos al Convenio de Budapest, a saber: la Ley N° 26.904 (2013), por la cual se incorpora la figura del "*Grooming*" o "ciberacoso" sexual al art. 131 del Código Penal y la ley N° 27.436, que castiga la simple tenencia de material pornográfico infantil.

Ahora bien partiendo de la base de la hipótesis oportunamente propuesta de que "la escasa previsión normativa de la legislación nacional se ha solucionado con la adhesión al Convenio de Budapest", el objeto del presente trabajo será analizar la normativa penal y las respectivas figuras delictivas, que ofrece la legislación argentina referida a los delitos informáticos, tomando como punto de partida, los delitos previstos en el Convenio de Cibercriminalidad, celebrado en la ciudad de Budapest, al que -como adelantamos- Argentina adhirió mediante ley 27.411, a fin de determinar la incidencia positiva del mencionado instrumento en nuestra legislación penal de fondo.

Así, luego de señalar el rol de los organismos internacionales, procederemos a analizar los nuevos paradigmas surgen en el Derecho Penal y las formas de colaboración internacional a la luz de la mencionada Convención.

Se dividirá el trabajo en cinco capítulos.

En el primer capítulo, evaluaremos el rol de los organismos internacionales, los nuevos paradigmas en el derecho penal, las formas de colaboración, del cual se distingue el Convenio de Budapest como la principal herramienta legal de colaboración para prevenir el ciberdelito. Se estudiará su estructura.

[20] BARRIO ANDRES, Moisés., Obra citada, pág. 29.

En el capítulo II, analizaremos los antecedentes nacionales referidos a nuevas tecnologías de la información y con un breve detalle lo de los legislado por las distintas leyes.

En el capítulo III, desarrollaremos la incidencia del Convenio de Budapest, para que se sancionara la “Ley de Delito Informáticos” (Ley 26.388), mediante la cual se actualizó la legislación nacional a la nueva era digital, introduciendo conceptos y figuras penales al Código Penal. La Ley 27.411 de Adhesión al Convenio, donde por medio de la cual, Argentina, efectuó importantes reservas, basadas en su tradición penal clásica.

En el capítulo IV, describiremos los sujetos que intervienen en los delitos informáticos, según nuestra Legislación Penal y las conductas relacionadas con los delitos informáticos.

Por último, en el capítulo V, estudiaremos las figuras penales contempladas en la legislación nacional, las cuales guardan relación con las descriptas por el Convenio de Budapest, al regular en sus apartados las conductas penales reprimidas.

Para concluir en las figuras penales no contempladas en la reforma.

CAPITULO I

EL ROL DE LOS ORGANISMOS INTERNACIONALES. CONVENIO DE BUDAPEST

A.- El rol de los organismos internacionales:

Frente a situaciones de carácter económico, social, cultural, financiero y desarrollo constante, los Estados se ven inmersos en la evolución misma de las relaciones de carácter internacional, con el fin de que dichas relaciones se involucren en la participación de cada uno de ellos frente a las oportunidades surgidas constantemente en un mundo cambiante. Es de ésta manera que surgen desde la antigüedad fenómenos de agrupación y cooperación entre diferentes pueblos y naciones del mundo, a fin de crear la organización, evolucionando hasta nuestros días en organismos internacionales de diferente índole y con el abordaje de innumerables funciones que centran la finalidad de unión, ligadas con el fin común; de ésta manera se conforman como asociaciones voluntarias de Estados establecidas por acuerdo internacional, dotadas de órganos permanentes, propios e independientes, encargados de gestionar unos intereses colectivos y capaces de expresar una voluntad jurídicamente distinta de la de sus miembros[21].

Así, cuando las relaciones internacionales adquieren cierto grado de permanencia, surge la necesidad de su organización, precisamente para mantener esa permanencia. Cuando se organizan las relaciones permanentes de una sociedad- en nuestro caso la sociedad internacional-resultan imprescindible dos cosas: a) determinar lo más específicamente posible los fines de la sociedad; b) crear los órganos de expresión de su voluntad.

Tal como venimos sosteniendo, las nuevas tecnologías de la información y comunicaciones no poseen normas de carácter legal en forma acabada, debido a la constante y gran dinámica que la materia representa, lo cual notamos tanto en legislaciones de regulación plena de un derecho unificado como así también en lo referido a características aisladas de las diversas ramas del derecho. En lo que se refiere a nuestro análisis de estudio, específicamente sólo podemos mencionar dentro del contexto

[21] DIEZ DE VELAZCO, Manuel, Las organizaciones internacionales, Madrid, 9° ed. Tecnos, 1996, p. 37.

internacional, pocos países que cuentan con una legislación apropiada para el tratamiento de los delitos informáticos. Esto es el fruto de la aplicación y utilización ilícitas de las nuevas tecnologías de la información, como por ejemplo la utilización de la web para el acceso a vínculos propios y necesarios para la transmisión de datos, voz, etc., a través de Internet y todas sus aplicaciones, comunicaciones electrónicas, transacciones e intercambio, protegidos de los accesos ilegales a sistemas de cómputo, la difusión de virus o la intercepción de mensajes informáticos entre otros, incluyéndolos dentro de una ley capaz de encuadrar estas conductas punibles penalmente[22].

En 1986 la OCDE público un informe titulado de Delitos de informática: análisis de la normativa jurídica**,** donde se reseñaban las normas legislativas vigentes y las propuestas de reforma en diversos Estados miembros y se recomendaba una lista mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales.

En 1992 elaboró un conjunto de normas para la seguridad de los sistemas de información, con intención de ofrecer las bases para que los Estados y el sector privado pudieran erigir un marco de seguridad para los sistemas informáticos.

En 1990 la Organización de las Naciones Unidas (ONU) en el Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en La Habana, Cuba, se dijo que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos.

La ONU ha publicado una descripción de "Tipos de Delitos Informáticos", que se transcribe al final de esta sección.

En 1992 la Asociación Internacional de Derecho Penal durante el coloquio celebrado en Wurzburgo en 1992, adoptó diversas recomendaciones respecto a los *delitos informáticos*, entre ellas que, en la medida que el derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el "principio de subsidiariedad".

[22] TOBARES CATALA, Gabriel H., CASTRO ARGÜELLO, Maximiliano J., ob. Cit. p. 53 y 54.

B.-Nuevos paradigmas surgen en el Derecho Penal:

El mundo actual, es el mundo de las tecnologías, estamos viviendo en lo que se denomina la "era de la informática", en una "sociedad digital". Las redes sociales han invadido en todas las sociedades y han provocado una verdadera revolución en el campo de las comunicaciones. La masificación de las tecnologías de la información y la globalización han producido una brecha generacional difícil de dimensionar y de controlar mediante limitadas herramientas que nos proporciona el derecho y otras disciplinas sociales.

El Mundo se ha contraído, todo se puede lograr en tiempo real, viajando en forma virtual en el espacio infinito de internet.

Por su parte, internet presenta la peculiaridad adicional, dado su carácter descentralizado, de que no es posible que un organismo dirija y gestione la red. Su funcionamiento es consecuencia del empleo, por una gran cantidad de operadores de sistemas informáticos y de redes de telecomunicaciones -o de comunicaciones electrónicas, como ahora las denomina el derecho de la Unión Europea-, de unos protocolos y arquitecturas comunes; esto es, de un mismo conjunto de convenciones relativas a la transmisión de datos e interoperabilidad de los sistemas.[23]

Es precisamente, por estas características propias de Internet, que se generan nuevos paradigmas y una pregunta a debatir: ¿Por qué un derecho internacional de los Ciberdelitos?, teniendo en cuenta que tanto en derecho penal y el procesal clásico, así como los principios garantistas inherentes a ambos, han sido construidos, en esencia, sobre la base de un modelo de delincuencia física, marginal e individual.

Ahora bien, siendo que Internet es un espacio y no un territorio, el Dr. Manuel David Masseno, nos enseña que es necesario tener en cuenta los principios de Legalidad y de Territorialidad que dan formas a los Derechos Penales, con la inherente fragmentación de los regímenes nacionales.[24]

[23] BARRIO ANDRES, Moisés. "Ciberdelito 2.0. Amenazas criminales del ciberespacio", Astrea, Buenos Aires, 2020, pág. 2.
[24] https://www.youtube.com/watch?v=EOlIRWF4vSE&t=4835s

Mientras que la criminalidad informática es transnacional, por su naturaleza misma, ya que ésta nueva generación de delitos ya no preocupa por tener como elemento característico el realizarse desde ordenadores, sino por el hecho de que tales sistemas informáticos están conectados en un ámbito de comunicación universal, el ciberespacio, y porque es en este nuevo "lugar" en el que, desde cualquier espacio físico ubicado en cualquier Estado, se cometen infracciones que pueden afectar, en lugares distintos y simultáneamente, a bienes jurídicos tan importantes como el patrimonio, la intimidad, la libertad y la indemnidad sexuales, el honor, la dignidad personal, la seguridad del Estado o la libre competencia, entre otros muchos[25].

Es precisamente de las especiales características de Internet, que resulta muy difícil determinar la autoría, el lugar de comisión del delito y, la competencia para juzgarlos.

Por ello, es necesario superar la dimensión territorial del Derecho, creando reglas comunes y aplicables al ciberespacio. Reglas de derecho material, con referencia comunes para los tipos penales, reglas de derecho adjetivo, sobre todo en lo concerniente a la prueba, reglas de cooperación judicial y policial.

C.- Las formas de colaboración internacional:

Los Estados colaboran entre sí a través de los contratos o acuerdos internacionales, que se rigen por la Convención de Viena.

Una de las respuestas posibles al interrogante planteado, es precisamente el Convenio de Budapest sobre la Ciberdelincuencia, adoptado en Budapest, el día 23 de noviembre de 2001.

Dicho instrumento, surgió a partir de los estudios efectuados por la Organización de Cooperación y Desarrollo Económico (OCDE), con el objeto de luchar contra el problema del uso indebido de los sistemas informáticos, elaborando normas de seguridad con intención de ofrecer bases para que los Estados puedan erigir un marco legal a este tipo de situaciones.

[25] BARRIO ANDRES, Moisés, obra citada, pág., 9.

Este acuerdo se firmó bajo el patrocinio del Consejo de Europa. Aunque no es un instrumento de la Unión Europea, el Convenio recoge efectivamente los intereses de aquella en su ámbito de aplicación. Su negociación coincidió con la creciente importancia del comercio electrónico, la propiedad intelectual y la mayor penetración del acceso de banda ancha a internet y de la telefonía móvil.

Dicho Convenio surge como consecuencia del desarrollo y utilización cada vez mayor de la TIC y de las posibilidades consiguiente que ofrecen tales medios para la comisión de nuevos tipos de delito, así como la necesidad de aplicar una política penal común encaminada a proteger a la sociedad frente a la ciberdelincuencia, a cuyo fin ordena a las partes la adopción de una legislación que dé respuesta adecuada a tales nuevas formas de delincuencia y el establecimiento de una política de colaboración internacional. Se trata de un instrumento internacional pionero en el ámbito de los delitos cometidos por medio de internet u otras redes electrónicas, y pone un acento especial en la lucha contra la pornografía infantil, el fraude informático y las violaciones de seguridad en la red.

Es de destacar, que nuestro país adhirió al Convenio de Budapest en el año 2017, mediante la Ley N° 27.441. Dicho convenio, responde a la necesidad de articular una política penal común, a prevenir 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.[26]

Es un instrumento efectivamente internacional, fue negociado con la participación efectiva de EE. UU, de Canadá, Sudáfrica y Japón. Tiene prevista la adhesión de Estados Terceros, siendo los últimos en hacerlo, en Latinoamérica, Costa Rica y Paraguay en el año 2018. Brasil en la actualidad se encuentra próximo a adherirse.

a.- Cómo se estructura el Convenio de Budapest?

Básicamente, podemos decir que el Convenio consta de tres propósitos que hacen a su estructura, a saber:

[26] BARRIO ANDRES, Moisés., Obra citada, pág. 29.

1.- Armonizar el derecho penal material, definiendo el Derecho penal sustantivo, en su Cap. II. Secc. 1, está destinada a crear una base común de delitos, que incluye los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos (arts. 2° a 6°), los delitos informáticos (arts. 7° a 8°), los delitos relacionados con el contenido (art. 9°) y los delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines (art. 10°).

2.- Establecer medidas procesales (Cap. II, Secc.2): El Convenio en materia procesal, hace referencia a varias medidas de investigación, y obtención de prueba. Diferenciando entre aquellas que adaptan a la investigación informática medidas ya existentes, por ejemplo, el caso de entrada y registro, y aquellas de nueva creación, específicas de la investigación informática (ejemplo, la conservación rápida de datos informáticos almacenados del art. 16, la conservación y revelación parcial rápida de datos sobre tráfico del art. 17, la orden de presentación del art. 18, registro y confiscación de datos informáticos almacenados del art. 19 o la obtención en tiempo real de datos informáticos de los arts. 20 y 21.

3.- Poner en funcionamiento un régimen rápido y eficaz de cooperación internacional (Cap. III): En su art. 23 establece que las partes cooperan entre sí en la mayor medida posible para los fines de investigación o los procedimientos relativos con sistemas y datos informáticos o para la obtención de prueba electrónica de los ciberdelitos. En el art. 24 introduce la posibilidad de extradición de delincuentes. Además, el Convenio crea la “red 24/7” como punto de contacto disponible las 24 horas del día, siete días a la semana, como el objeto de garantizar la prestación de ayuda inmediata a los fines de las investigaciones relacionadas con los delitos tipificados. Las medidas que pueden solicitarse incluyen el asesoramiento técnico, la conservación de datos y la obtención de pruebas, el suministro de información jurídica y la localización de sospechosos.[27]

Es de destacar que, en el año 2003, se aprobó el Primer Protocolo Adicional al Convenio de Budapest, relativo a la penalización de actos de índole racista y xenófobo, cometidos por medio del sistema informático, alcanzado en Estrasburgo.

Además, desde el año 2017, se está negociando un Segundo Protocolo Adicional, reforzando la cooperación para la obtención de prueba

[27] BARRIO ANDRES, Moisés. Obra citada, pág. 30 y 31.

electrónica teniendo en cuenta la protección de datos personales. Sin embargo, debido a la dificultad del proceso de revisión, hace que dicha negociación sea lenta y engorrosa.

b.- Sobre los aspectos de fondo del Convenio de Budapest:

El interés de este trabajo analizar la sección 1 (“Derecho Penal Material) del Capítulo II (“Medidas que deben adoptar los Estados nacionales”) de este Convenio, destinado a las adecuaciones que cada Estado debe realizar respecto de sus propias legislaciones.

Dicho Convenio, establece como delitos, en su Título I, las infracciones contra la confidencialidad, la integridad y disponibilidad de los datos de los sistemas informáticos; así, como en su artículo 2, considera el acceso ilícito, doloso y sin autorización a todo o parte de un sistema informático. En su artículo 3, considera como infracción penal, la interceptación, dolosa y sin autorización, cometida a través, de medios técnicos, de datos informáticos (en transmisiones no públicas) en el destino, origen o en el interior de un sistema informático; artículo 4, Atentados contra la integridad de los datos, reprimiendo la conducta de dañar, borrar, deteriorar, alterar o suprimir dolosamente y sin autorización los datos informáticos; artículo 5, Atentados contra la integridad del sistema, considerando infracción penal la obstaculización grave, cometida de forma dolosa sin autorización, del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos; artículo 6, establece como delito, el abuso de equipos e instrumentos técnico. En el Título II, señala en su artículo 7, de la falsedad informática, considerando infracción la introducción, alteración, borrado o supresión doloso y sin autorización de datos informáticos, con la intención de que sean percibidos o utilizados como auténticos; artículo 8, señala la estafa informática, la cual causa un perjuicio patrimonial; artículo 9, contempla las infracciones relativas a la pornografía infantil; finalmente en el Título 4, artículo 10 , describe las infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines.

En esta sección, más allá de los parámetros que establece para que cada parte modifique su legislación, el Convenio destaca dos cuestiones fundamentales: en cuanto a las sanciones y medidas, señalando, por un lado, que las partes adoptaran las medidas legislativas o de otro tipo que estimen necesarias para permitir que las infracciones penales establecidas en los artículos 2 a 11 sean castigadas con sanciones efectivas, proporcionadas y disuasorias, incluidas las penas privativas de libertad. Por

último, las partes velarán para que las personas jurídicas que hayan sido declaradas responsables según lo dispuesto por el artículo 12 sean objeto de sanciones y disuasorias, incluidas las sanciones pecunarias.

CAPITULO II

ANTECEDENTES LEGISLATIVOS EN ARGENTINA

A.- Legislación de nuevas tecnologías de la información y comunicaciones en Argentina, y normativa específica en materia de derecho penal nacional

Podemos concluir que en Argentina se ha legislado en cinco oportunidades sobre la materia incluyendo ciertos delitos relacionado con la informática, ya sea en el Código Penal o en sus leyes complementarias[28], para luego, dar un marco más completo en cuanto al alcance y tipificación a través de la ley 26.388.

En primer lugar, en 1990, se llama a concurso público internacional con base, para la privatización de la prestación del servicio público de telecomunicaciones, mediante el decreto del P. E. N. N° 62/90 en Pliego de Bases y Condiciones para la prestación de servicios telefónicos, en este decreto quedó establecido el doble régimen para el servicio de acceso a Internet; por un lado, la salida al exterior en exclusividad, y por el otro, un régimen de libre competencia para el ámbito nacional.

Luego, fue promulgada la ley 24.766 (20/12/1996), referida a la confidencialidad de la información y producción, que estén legítimamente bajo el control de una persona y se divulgue indebidamente de manera contraria a los usos comerciales honestos. La ley, establece la posibilidad de impedir que solo aquella información que sea secreta, con un valor comercial y que haya sido objeto de medidas razonables para mantenerla como tal, se divulgue a terceros, sea adquirida o utilizadas por ellos de manera contraria a los usos comerciales honestos. Dejando al margen aquella información que no sea de carácter comercial, o que siéndolo y que a pesar de su necesaria protección no es posible encuadrar estrictamente en el tipo descripto, delatando de esta manera “una parcial impunidad”. Incluso en el art. 9 de la ley, deja expresado que no estará protegida la información que hubiera caído en el dominio público en cualquier país, por la publicación

[28] CABANELLAS DE LAS CUEVAS, Guillermo, MONTES DE OCA, Ángel, Derecho de Internet, Bs. As., Heliasta, 2004, p.58.

de cualquiera de los datos protegidos, la presentación de todos o partes de éstos en medios científicos o académicos, o por cualquier otro medio de divulgación. Es importante destacar que, en este cuerpo legal, se hace expresa mención del lugar o soporte donde se halla contenida o resguardada la información protegida por la ley. El art. 2 expresa que se resguarda “la información que conste en documentos, medios electrónicos o magnéticos, discos ópticos, microfilmes, películas u otros elementos similares”. Se demuestra de esta manera un avance de relevancia en nuestra legislación nacional.

En lo que se refiere a la libertad de contenido, el Decreto 1279/1997 declara que el servicio de Internet, se considera comprendido dentro de la garantía constitucional que ampara la libertad de expresión, correspondiéndole en tal sentido las mismas consideraciones que a los demás medios de comunicación social, la ley 26.032. Establece que la búsqueda, recepción y difusión de información e ideas de toda índole, a través del servicio de Internet, se considera comprendida dentro de la garantía constitucional que ampara la libertad de expresión.

La ley 24.769 sobre el régimen penal tributaria, promulgada el 13 de enero de 1997, relativa a los delitos tributarios, y a los recursos de la seguridad social, que deroga la ley 23.771, en el art. 12 hace referencia a la alteración dolosa de registros, teniendo como objeto de protección al registro o soporte informático, penalizando ciertos actos que tengan como fin el propósito de disimular la real situación fiscal de un obligado. Es evidente y notorio que la acción típica a la que hacer referencia es “el que de cualquier modo sustrajere, suprimiere, ocultare, adulterare, modificare o inutilizare los registros o soportes documentales o informáticos del fiscal nacional…”, relativos sólo a un área determinada como la tributación, al expresar en su articulado las obligaciones tributarias o de recursos de la seguridad social.

Podemos afirmar, conforme a la fórmula legal, que nos encontramos en presencia de un delito de carácter doloso, requiriendo por lo tanto el simple conocimiento (y por ende la intención) por parte del sujeto activo de que la sustracción, supresión, ocultación, adulteración, modificación o la utilización de aquellos registros antes mencionados, son exclusivamente con el propósito de disimular la real situación fiscal de un obligado tributariamente hablando. Deduciendo de ello que dicho accionar puede ser cometido tanto por el obligado o contribuyente como por parte de un tercero, sin requerir (necesariamente) la producción de algún daño, ya que éste es un tipo de delito de peligro

abstracto siendo suficiente para su consumación la realización de las conductas enumeradas taxativamente en el art. 12 de la ley, aunque el propósito de disimular aquella situación llegue a su plenitud.

En lo que se refiere específicamente a la participación de los proveedores del servicio, a través de la resolución S. C. N° 1235/98 se determina como obligación de los ISP (Internet Service Provider), la inclusión de una leyenda aclarando que el Estado no controla ni regula la información disponible en la red. En ella se recomienda a los padres ejercer un razonable control por los contenidos que consumen sus hijos. Es aconsejable la consulta a su proveedor de servicio de acceso a fin de obtener el correspondiente asesoramiento sobre programas de bloqueo se sitios que consideren inconvenientes. Por su parte la ley 25.690, establece la obligación de los ISP de proporcionar software adicional a sus usuarios a efectos de facilitar el bloqueo del acceso a determinadas páginas o sitios de Internet.

La ley 25.036, (promulgada en noviembre de 1998) modificó los art. 1°, 4°, 9° y 57° e incorpora el art. 55° bis a la ley 11.723 referida a la propiedad intelectual ha venido a procurar una protección más eficiente a los trabajos personales de los autores, creadores de software, programas de computación, como un aporte a los avances que llevan al desarrollo social, reconociéndoles paternidad y originalidad requerida por la ley. Regula la explotación de la propiedad intelectual sobre los programas señalados, adoptando entre otras las formas los contratos de licencia para uso y reproducción, incluyendo el depósito de los elementos y documentos que determine la reglamentación cuando de la anotación en el Registro Nacional de Propiedad Intelectual se alude a la ley 11.723. Como consecuencia de la reforma de la ley sobre propiedad intelectual es que hoy se puede hablar de una protección penal del software, teniendo presente la posibilidad de amparar los programas de computación.

La ley 25.326 (promulgada el día 30/10/2000) sobre protección de los datos personales, viene a reglamentar la disposición establecida en el art. 43 de la C. N., referida entre otras a la acción de habeas data. Esta ley se propone otorgar protección integral de los datos personales asentados en los registros; garantizar el derecho al honor a la intimidad de las personas y el acceso a la información que sobre estas se registre, realizando una tutela más amplia sobre los datos personales, ya que no sólo se refiere a lo de las personas físicas sino también a lo de las personas jurídicas, que se

encuentren en archivos, registros y banco de datos, entre otros medios de técnicos de tratamiento destinados a dar informes. También en ella se ha de tener en cuenta que su protección no se limita tampoco a lo referente al área garantizada, tratando en su regulación tanto a los bancos de datos de carácter público como privado. En su art. 32 se hace referencia a las sanciones penales incorporando los arts. 117 bis y 157 bis, en el Código Penal Argentino, las conductas que actualmente se tipifican se limitan en el art. 117 bis:"al que insertare o hiciere insertar datos falsos en un archivo de datos personales, y al que proporcionare a un tercero información falsa contenida en un archivo de datos personales…"

En ambos casos se requiere un conocimiento sobre la falsedad del dato. Elevándose la escala penal por la existencia de un perjuicio o por el sujeto que lo comete haciendo referencia al funcionario público. Así también la pena en el art. 157 bis: "el acceso doloso e ilegítimo a un banco de datos personales y al que revelare la información secreta registrada en un banco de datos…"

Elevándose también en este caso la escala penal en el caso de que dicho ilícito sea cometido por un funcionario público.

Otro de los temas legislados es el de los dominios de Internet (Resolución 2226/2000).

La ley 25.596 (promulgada el día 11/12/2001), tiene como objeto el reconocimiento del empleo de la firma electrónica; de la firma digital y su eficacia jurídica, regulando la relación entre el certificador licenciado que emite un certificado digital y el titular de ese certificado. Entendiéndose por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. Esa ley penaliza las falsedades de "documentos, instrumentos privados y certificados "pero no de instrumentos públicos digitales en el art. 78 bis del C. P.: "los términos firman y suscripción comprenden la firma digital o firmar digitalmente. Los términos documento, instrumento privado o certificado, comprenden el documento digital firmado digitalmente*".*

Se trata de esta manera de brindar un resguardo efectivo, asegurando la confiabilidad, confidencialidad y un correcto funcionamiento.

La ley 25.520 (Ley de Inteligencia Nacional), específicamente está destinada al tratamiento en lo que se refiere la interceptación, captación de comunicaciones. En los art. 42 y 43 de dicho cuerpo, se regula la interceptación, captación y derivación de las comunicaciones que utilice cualquier otro tipo de transmisión de imágenes, voces o paquetes de datos, así como cualquier otro tipo de información archivos, registros y/o documentos privados, o de entrada o lectura no autorizada o no accesible al público.

Por su parte, en el ámbito de la Secretaría de Comunicaciones de la Presidencia de la Nación se creó el "Programa Nacional para la Sociedad de la Información", que tiene como misión fundamental programar, desplegar y ejecutar iniciativas proyectos y programas dirigidos a reducir la "brecha digital" entre quienes tienen acceso a las tecnologías de la información y comunicación. Tiene competencia en aquellas actividades y cuestiones vinculadas al diseño e implementación de políticas públicas destinadas a promover:

- La universalización de Internet, la apropiación social de las tecnologías de la información.
- La formación de recursos humanos especializados en su gestión.
- El desarrollo de servicios y redes de alta complejidad computacional.
- El fomento de las inversiones, la electrónica, el software y demás tecnologías afines[29].

Además, en 2013 se sancionó la Ley de grooming 26.904 con penas de cárcel para el que contacte por medio de cualquier tecnología de transmisión de datos a una persona menor de edad con el propósito de cometer cualquier delito contra su integridad sexual[30].

[29] Htpp://psi.gov.ar/queeselpsi.htm

[30] servicios.infoleg.gob.ar/infolegInternet/anexos/220000-224999/223586/norma.htm
Ley 26.904 'Artículo 131: Será penado con prisión de seis (6) meses a cuatro (4) 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. 'ARTICULO 2° — Comuníquese al Poder Ejecutivo.

Por último, ley N° 27.436, que castiga la simple tenencia de material pornográfico infantil, la Argentina cumple con su compromiso internacional de adecuar su ley interna al Convenio de Budapest. [31]

B. Panorama general de la reforma de la ley 26.388

En nuestro país, y luego de numerosos proyectos legislativos que se sucedieron en la última década[32], se sancionó la ley 26.388 de Reforma al Código Penal en materia de "Delitos Informáticos", sumándose así a un grupo de países que intentan brindar protección jurídica a situaciones que emergen del uso creciente de las tecnologías de la información e internet. Es importante poner relieve que no se regulo con la mencionada reforma un cuerpo legal autónomo del Código Penal, con figuras determinadas, clasificaciones y definiciones propias, sino que se enfocó el esfuerzo en incorporar, sustituir, modificar y agregar a las figuras típicas existentes, incorporando nuevos conceptos y ensanchándose de este modo el tipo penal, en los diversos artículos del Código Penal vigente, por lo que si bien es valiosos el aporte, la sistemática del Código se ha visto forzada[33].

El Dr. Gustavo Arocena[34] sostiene, que hubiera sido conveniente el tratamiento de la temática que analizamos en la presente obra en una ley específica, por tratarse de un bien jurídico novedoso, que aumenta el especial tratamiento

---

[31] http://servicios.infoleg.gob.ar/infolegInternet/anexos/305000-309999/309201/norma.htm. ARTÍCULO 1°.- Sustitúyese el artículo 128 del Código Penal por el siguiente ARTICULO 128.- Será reprimido con prisión de tres (3) a seis (6) 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 un (1) año el que a sabiendas tuviere en su poder representaciones de las descriptas en el párrafo anterior. Será reprimido con prisión de seis (6) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el primer párrafo 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. Todas las escalas penales previstas en este artículo se elevarán en un tercio en su mínimo y en su máximo cuando la víctima fuere menor de trece (13) años. ARTÍCULO 2°.- Comuníquese al Poder Ejecutivo nacional.

[32] Desde 1996 al 31 de diciembre de 2007 se verificaron en el Congreso de la Nación Argentina un total de treinta expedientes que responden a proyectos legislativos con relación a delitos informáticos.

[33] TOBARES CATALA, Gabriel H., CASTRO ARGÜELLO, Maximiliano J., ob. Cit. p. 37

[34] En su disertación en las Terceras Jornadas Argentinas de Derecho Informático que se llevaron a cabo el 13/08/2008, en la Facultad de Derecho y Ciencias Sociales de la Universidad Nacional de Córdoba.

y permite la incorporación de figuras en su texto, sin la necesidad de romper con la sistemática del Código Penal. Pero no obstante ello, considera muy positivo y de vital transcendencia, contar con una regulación normativa en la materia, puesto que la nueva Ley de Reforma al Código Penal 26.388 hace frente a una nueva realidad informática llenando el vacío legal imperante en el tema y que brinda amparo a diversas situaciones de hecho, contra conductas que quedaban en impunidad colocando a la toda la sociedad en un estado de indefensión y de inseguridad jurídica. “Si bien esta ley, y sus respectivas modificaciones al Código Penal, dan pie a mucha controversia, lo cierto en que establece las bases legales para comenzar actuar en casos en donde hasta este momento era imposible incursionar o se debía “dibujar” los casos para que los mismos encuadraran en un delito tipificado”[35].

Asimismo, incorporó cierta terminología a nuestra normativa de fondo que permite adecuar el mismo a los avances de las tecnologías de la información y comunicaciones; términos que se agregan como último párrafo del art. 77 del mencionado cuerpo legal y que se definen de la siguiente manera:

- “Documento” comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.
- “Firma” y “suscripción” comprende la firma digital, la creación de una firma digital o firmar digitalmente.
- “Instrumento Privado” y “certificado” comprende el documento digital firmado digitalmente.

Por otro lado, es importante poner de relieve que, con anterioridad a la sanción de la ley, se verificaron algunas normas que intentaban regular nuevos fenómenos comunicacional, tratando de acordar protección contra estas conductas disvaliosas, reprochables y antisociales, individualizándose normas que se vinculan al área de la administración pública y que se remontan a la década de los noventa juntamente con el proceso de privatización en materia de telecomunicaciones.

[35] Http://www.segu-info.com.ar/boletín-113-080607.htm

CAPITULO III

LA LEY 26.388 Y EL CONVENIO DE CIBERDELICUENCIA

A.- El Convenio de Budapest y la Legislación Argentina

El Convenio de Budapest, tal como lo adelanté, ha tenido incidencia en la legislación argentina, motivando la sanción de la ley 26.388[36], y posteriores

[36] http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm. ARTICULO 1º — Incorpóranse como últimos párrafos del artículo 77 del Código Penal, los siguientes: El término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente. ARTICULO 2º — Sustitúyese el artículo 128 del Código Penal, por el siguiente:Artículo 128: 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. ARTICULO 3º — Sustitúyese el epígrafe del Capítulo III, del Título V, del Libro II del Código Penal, por el siguiente:*"Violación de Secretos y de la Privacidad"* ARTICULO 4º — Sustitúyese el artículo 153 del Código Penal, por el siguiente:Artículo 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 5º — Incorpórase como artículo 153 bis del Código Penal, el siguiente: Artículo 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 6º — Sustitúyese el artículo 155 del Código Penal, por el siguiente: Artículo 155: Será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil ($ 100.000), el que

reformas, que incorporaron distintos tipos penales y actualizaron algunos conceptos jurídicos, en consonancia con el primero.

Argentina fue invitada a adherirse al Convenio en septiembre de 2010. En marzo de 2017 se ingresa el proyecto de ley para ratificar el Convenio y el

---

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 7º — Sustitúyese el artículo 157 del Código Penal, por el siguiente:Artículo 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 8º — Sustitúyese el artículo 157 bis del Código Penal, por el siguiente: Artículo 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. ARTICULO 9º — Incorpórase como inciso 16 del artículo 173 del Código Penal, el siguiente: Inciso 16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos. ARTICULO 10**.** — Incorpórase como segundo párrafo del artículo 183 del Código Penal, el siguiente: 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. ARTICULO 11. — Sustitúyese el artículo 184 del Código Penal, por el siguiente: Artículo 184: La pena será de tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes:1. Ejecutar el hecho con el fin de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones;2. Producir infección o contagio en aves u otros animales domésticos;3. Emplear substancias venenosas o corrosivas;4. Cometer el delito en despoblado y en banda;5. Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; 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. ARTICULO 12. — Sustitúyese el artículo 197 del Código Penal, por el siguiente: Artículo 197: 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. ARTICULO 13. — Sustitúyese el artículo 255 del Código Penal, por el siguiente: Artículo 255: Será reprimido con prisión de un (1) mes a cuatro (4) 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 funcionar público 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). ARTICULO 14. — Deróganse el artículo 78 bis y el inciso 1º del artículo 117 bis del Código Penal. ARTICULO 15. — Comuníquese al Poder Ejecutivo.

poder legislativo de la República Argentina lo aprobó el 22 de noviembre del año 2017, convirtiéndose en la Ley 27.411.

Es a partir del año 2017, al adherirse Argentina al Convenio de Budapest, se comprometió, con algunas reservas a adecuar su Derecho Penal y Procesal a una política penal común a nivel internacional.

Si bien, en forma paulatina el derecho fondo ha sido adecuado a través de las leyes nacionales, una cuenta pendiente son las legislaciones provinciales, quienes tienen el desafío de adecuar sus códigos de procedimiento, al mencionado instrumento internacional, donde la investigación de un alto número hechos, requieren de cierta prueba, la cual, debe recolectarse en o a través de medios digitales, sin violentar garantías constitucionales.

Argentina no ha adoptado ni tiene en tramitación actualmente algún proyecto de ley de adecuación unificada de la normativa del Convenio de Budapest.

Sin embargo, a la fecha se encuentran en tramitación proyectos relacionados en el Senado tales como el N°230/19 que modifica el Código Penal tipificando la publicación por medios informáticos de imágenes de personas en actividades sexuales y el robo de identidad, además del proyecto N°109/16 sobre utilización de programas informáticos de formato libre y el proyecto N°3918/14 sobre daño a un sistema informático. Por su parte, la Cámara de Diputados tiene en tramitación el proyecto de Ley 4199-D-2019 mediante el cual se establecería un agravante para los delitos cometidos a través de internet o por medios electrónicos.

Además, Argentina se encuentra tramitando el proyecto de Ley 2714-D-2017 que regula el agente encubierto informático[37], incorporándolo a las disposiciones de la Ley 27.319 sobre Delitos Complejos, definiendo agente informático online, en el artículo 2 del Proyecto como: “Será considerado agente encubierto informático todo aquel funcionario de las fuerzas de seguridad autorizado, altamente calificado, que presta su consentimiento y ocultando su 130 “La REPÚBLICA ARGENTINA hace reserva del artículo 29.4 del CONVENIO SOBRE CIBERDELITO y manifiesta que no regirá en su jurisdicción por entender que el requisito de la doble incriminación es una de las bases

[37] DIPUTADOS ARGENTINA. Proyecto de Ley. 2017. [En línea] [Consulta: 01 de julio de 2020]

fundamentales de la LEY DE COOPERACIÓN INTERNACIONAL EN MATERIA PENAL Nº24.767 para el tipo de medidas de cooperación previstas en artículo y numeral citados." 131 DIPUTADOS ARGENTINA. Proyecto de Ley. 2017. [En línea] [Consulta: 01 de julio de 2020] 110 identidad interactúe, se relacione o participe, a través de una identidad supuesta en grupos de internet, redes sociales y plataformas de intercomunicación on-line, con el fin de identificar o detener a los autores, partícipes o encubridores, de impedir la consumación de un delito, o para reunir información y elementos de prueba necesarios para la investigación, con autorización judicial".

El proyecto además contempla, la responsabilidad del agente policial, cómo deberá operar y forma de ejercer su encomienda; así, en el mensaje de fundamentos del Proyecto de Ley, se señala: "Es por ello que el recurso de la tecnología por parte del Estado cumple en la actualidad un doble papel en relación con el proceso penal: por un lado permite el perfeccionamiento de los medios de análisis para investigación y prueba ofreciendo resultados más fiables, y por otro, permite la persecución de aquellos delitos conectados directamente con la tecnología, cada vez más numerosos."

El proyecto impulsado por la Asociación Argentina de Lucha Contra el Cibercrimen (AALCC), reconoce la masificación de los delitos vinculados a medios tecnológicos, y la utilización de ésta para la facilitación de su comisión, y como almacenamiento de evidencia esencial para el procesamiento de estos delitos.

a.- Breve reseña de lo normado por la Ley 26.388 y la Ley 27.411:

La ley 26.388, promulgada en junio de 2008, incorporó distintos delitos informáticos en el Código Penal Argentino, adecuando la ley penal argentina a las normas previstas en la Convención sobre Cibercriminalidad, firmada en la ciudad de Budapest en 2001. Esta reforma significó no solo una actualización de nuestra legislación penal, sino que implica un cambio de concepción en muchos conceptos legales que el avance tecnológico había dejado obsoletos, así como también la incorporación de nuevos tipos penales y la actualización de algunos ya existentes.

En noviembre de 2017 se sancionó la ley 27.411, que dispuso la adhesión de la Argentina al Convenio sobre Ciberdelincuencia celebrado por el Consejo de Europa en la ciudad de Budapest, en el año 2001. Dicho convenio, si bien celebrado inicialmente en el marco europeo, está destinado desde un inicio a uniformar la legislación

aplicable en cada estado parte respecto a la lucha contra la ciberdelincuencia, previendo no solo su aplicación por los estados europeos, sino también por todo aquel que así lo pretenda, previo los pasos de ingreso a este, que el propio convenio prevé.

En la actualidad, es el único convenio multilateral y el de mayor alcance en cuanto a países suscriptos a nivel mundial, que incluye no solo los países del Consejo de Europa, sino también países como Estados Unidos, Canadá, Australia, Japón, Chile, Paraguay, y otros, siendo 61 países quienes a la actualidad han adherido al Convenio. Este convenio, más allá de establecer las pautas de definición de los ciberdelitos, resultó de gran relevancia a los fines de uniformar la legislación de cada Estado parte.

La recepción de este Convenio en Argentina ha sido en mayor medida en los aspectos sustanciales, esto es la definición de aquellas conductas disvaliosas como delitos, siendo la base por la que se sancionó la reforma del Código Penal dispuesta por ley 26.388.

Sin embargo, en lo procesal la adecuación de las reglamentaciones no ha tenido el mismo auge, manteniéndose aún, la aplicación analógica de ciertos institutos tradicionales, como el registro y allanamiento o la interceptación postal o de comunicaciones telefónicas.

Así, algunos códigos procesales, como el nuevo Código Procesal Penal de la Nación, sancionado por ley 27.063 (cuya entrada en vigencia se encuentra suspendida), o los ordenamientos neuquino o mendocino han incorporado ciertas adaptaciones a las nuevas tecnologías de la información y la comunicación que permiten la adopción de medidas necesarias para la obtención de evidencia digital.

Cabe reiterar que el avance de la cibernética ha permitido mayores injerencias en distintos ámbitos de privacidad e intimidad de las personas, quedando estas mucho más expuestas frente a accesos arbitrarios por parte de las autoridades. Ello implica que se deba analizar las distintas medidas a la luz de las garantías constitucionales, que marcan un límite a las posibilidades de intrusión del investigador.

La gran cantidad de información que puede almacenarse o desprenderse de la prueba digital, al accederse a ámbitos de privacidad e intimidad que la misma investigación puede no tener interés inicial, requiere que las reglas procesales

impongan a los operadores judiciales una mayor rigurosidad de los controles a fin de autorizar el acceso y/o registro y/o secuestro de las evidencias digitales.

En este sentido, los proveedores de servicio de internet adquieren un rol vital en razón de la información que manejan y que pueden o no guardar, atento que no se encuentran obligados a hacerlo. Téngase en cuenta que muchas veces una investigación se inicia con el conocimiento simplemente de una dirección IP desde la cual se produjo una conexión y, por tanto, las posibilidades de referenciar dicha dirección con una persona, depende en gran medida de la colaboración de la empresa que proveyó la misma, a fin que aporte los datos relativos al abonado como también aquellos de tráfico, o quizás de contenido, que permitan identificar al usuario o la ruta de tráfico utilizada. La preservación de dicha información, por demás útil en una investigación, depende en consecuencia de la colaboración de dicha empresa, por lo que es necesario la regulación de canales de comunicación entre investigador y sector privado que permitan alcanzar y acceder a estos datos. Asimismo, el registro y conservación de datos informáticos puede implicar la colaboración de proveedores de servicios, que pueden ser públicos o privados, y que pueden tener asiento en el lugar donde transcurre la investigación o, en otro país, lo que implica la necesidad de aplicar mecanismos de cooperación expeditos, en razón de la volatilidad de la evidencia digital.[38]

Finalmente, cada vez más las organizaciones criminales utilizan herramientas tecnológicas que brindan grandes niveles de anonimato, usando conexiones a través de TOR y generación de espacios de intercambio en el Deep Web. Estos casos suelen ser los de mayor dificultad de investigación, toda vez que las conexiones suelen cambiar cada poco minuto, conectándose desde distintos proxys anónimos ubicados en distintos lugares del mundo, de difícil cooperación judicial.

Particularmente en estos casos es donde se justificaría la utilización del agente encubierto digital, toda vez que a través de la misma sería posible que los investigadores ingresaran en el ámbito de confianza de las bandas de ciberdelincuentes, pudiendo obtener información útil para identificar a los autores por un lado y para probar los delitos por otro.

[38] SAIN, Gustavo Raúl, “Delito y nuevas tecnologías: fraude, narcotráfico y lavado de dinero por internet”, CABA, Editores del Puerto, 1ª Ed, 2012.

b- Alcance de la Reforma:

Es de destacar que la reforma no actualiza solamente el Código Penal en relación con las lagunas legislativas señaladas por la jurisprudencia. Ella implica un cambio de concepción en muchos conceptos que el avance tecnológico había dejado obsoleto[39].

Así, en materia de protección de delitos contra la seguridad de los medios de transporte y comunicación se amplía el concepto de comunicaciones protegidas por el art. 197 del C. P. En la época de la redacción del Código Penal, estos servicios se prestaban en forma monopólica por el Estado. La apertura en materia de telecomunicaciones amplió el abanico de servicios, que actualmente están a cargo, en su mayor parte, al sector privado, creando asimismo una amplia oferta de nuevos servicios impulsados por la convergencia, y que desafían la concepción de comunicaciones tradicionales. Por otra parte, a raíz de la convergencia tecnológica, todos estos servicios son muy difíciles de definir [40].

El fenómeno de la convergencia ha fundido en un solo dispositivo (el ordenador personal) multitud de herramientas comunicacionales.

Con la reforma se amplían las formas comisivas de la estafa incluyendo el "engaño" a sistemas automatizados para evitar planteos jurisprudenciales que impedían aplicar esta figura a los ordenadores o máquinas automatizadas sin intervención de personas. De esta forma, se reconoce que, debido a la informatización, muchos bienes y servicios se encuentran "custodiados" por computadoras y la manipulación a los fines de obtenerlos indebidamente es una defraudación.

La ley 26.388 modifica el delito de daño en dos aspectos fundamentales: se permite el daño bienes intangibles, tales como el borrado de software o de datos contenidos en un ordenador, que en algunos casos puede ser hasta más perjudicial que la destrucción de documentos almacenados en soportes tradicionales. Se

[39] PALAZZI, Pablo, Los Delitos Informáticos en el Código Penal, Análisis de la ley 26.388, Bs. As., Abeledo Perrot, 2009, p. 31

[40] Por ejemplo: los más recientes teléfonos poseen tres o cuatro dispositivos en cada uno, sirven para escuchar música, para fotografiar o filmar, para hablar por teléfono y para conectarse a Internet. Un ordenador sin conexión a telefónica sirve permite comunicarse telefónicamente a través de Internet usando sistema de voz sobre IP gratuitos, (Skype) etc.

incluye asimismo como delito distribuir programas destinados a causar daños (por ejemplo, virus informáticos). El legislador añadió asimismo dos agravantes relacionadas con la informática.

Con la reforma también se amplía el concepto de correspondencia amparada por los delitos de violación de secretos, porque se incluye el correo electrónico y a cualquier otra comunicación electrónica. Si bien entendemos que constitucionalmente este amparo ya existía a nivel constitucional (art. 18 de la C. N.), en el ámbito penal resultaba necesario tipificar expresamente la intercepción, el acceso y el desvió de las comunicaciones electrónicas.

Se expande asimismo el bien jurídico protegido porque la privacidad de la información personal es un concepto mucho más amplio que la confidencialidad o el secreto amparado por los delitos de violación de correspondencia. Las nuevas figuras como el acceso ilegítimo a un sistema informático, o la unificación de los delitos introducidos por la Ley de Protección de Datos Personales, sumado al cambio de epígrafe del capítulo, amplían notablemente la noción de espacio digital amparado penalmente.

B.- Reservas: [41]

[41] https://www.boletinoficial.gob.ar/#!DetalleNormaBusquedaAvanzada/176168/20171215 Ley 27411 “artículo 1°. - Apruébese el Convenio sobre ciberdelito del Consejo de Europa, adoptado en la ciudad de Budapest, Hungría, el 23 de noviembre de 2001, que consta de cuarenta y ocho (48) artículos cuya copia auténtica de su traducción al español, así como de su versión en idioma inglés, como anexo i, forma parte de la presente. artículo 2°. - al depositarse el instrumento de adhesión deberán efectuarse las siguientes reservas: a) La república argentina hace reserva del artículo 6.1.b. del Convenio sobre ciberdelito y manifiesta que no regirá en su jurisdicción por entender que prevé un supuesto de anticipación de la pena mediante la tipificación de actos preparatorios, ajeno a su tradición legislativa en materia jurídico penal. b) La República Argentina hace reserva de los artículos 9.1.d., 9.2.b. y 9.2.c. del Convenio sobre ciberdelito y manifiesta que estos no regirán en su jurisdicción por entender que son supuestos que resultan incompatibles con el código penal vigente, conforme a la reforma introducida por la ley 26.388. c) La República Argentina hace reserva parcial del artículo 9.1.e. del Convenio sobre ciberdelito y manifiesta que no regirá en su jurisdicción por entender que el mismo sólo es aplicable de acuerdo a legislación penal vigente hasta la fecha, cuando la posesión allí referida fuera cometida con inequívocos fines de distribución o comercialización (artículo 128, segundo párrafo, del código penal). d) La República Argentina hace reserva del artículo 22.1.d. del Convenio sobre ciberdelito y manifiesta que no regirá en su jurisdicción por entender que su contenido difiere de las reglas que rigen la definición de la competencia penal nacional. e) La república Argentina hace reserva del artículo 29.4 del Convenio sobre ciberdelito y manifiesta que no regirá en su jurisdicción por entender que el requisito de la doble incriminación es una de las bases fundamentales de la ley de cooperación internacional en materia penal n° 24.767 para el tipo de medidas de cooperación previstas en artículo y numeral citados.”

Sin embargo, es de destacar, que Argentina, efectuó, seis reservas, que versan sobre diversos puntos. La primera refiere al artículo 6.1.b. del Convenio, relacionado con portar material, como dispositivos, contraseñas o claves de acceso para cometer delitos como el de acceso ilícito o ataques a la seguridad de sistemas. Argentina manifestó que ese punto no regirá "por entender que prevé un supuesto de anticipación de la pena mediante la tipificación de actos preparatorios, ajeno a su tradición legislativa en materia jurídico penal".

Las restantes reservas giran en torno a los artículos 9.1.d., 9.2.b. y 9.2.c. Refieren a los delitos relacionados con la pornografía infantil y ciertas definiciones.

El argumento para que estos delitos no rijan en jurisdicción nacional es que son supuestos que resultan incompatibles con el Código Penal vigente.

La mera tenencia de pornografía infantil, en dispositivos informáticos tampoco regirá, estipulada en el artículo 9.1.e. Se trata de una reserva parcial. "El mismo sólo es aplicable de acuerdo a legislación penal vigente hasta la fecha, cuando la posesión allí referida fuera cometida con inequívocos fines de distribución o comercialización", tal como lo define el artículo 128, segundo párrafo, del Código Penal.

En materia de jurisdicción, la regla que indica que se deberá adaptar la legislación para castigar el delito cometido por uno de sus nacionales, si el delito es susceptible de sanción en el lugar en el que se cometió o si ningún Estado tiene competencia sobre el mismo. Argentina entiende que "su contenido difiere de las reglas que rigen la definición de la competencia penal nacional".

La última reserva se refiere a la conservación rápida de datos informáticos almacenados, y más precisamente sobre los convenios de "doble jurisdicción". La norma estipula que cuando un arte exija la doble tipificación como requisito para asistencia mutua, se podrá reservar el derecho a prestarla cuando tenga el convencimiento de que, al revelar los datos, no se va a respetar la "doble tipificación".

En este último aspecto, el país entiende que el requisito de la doble incriminación es una de las bases fundamentales de la Ley de Cooperación Internacional en Materia Penal, que es norma nacional tras la sanción de la Ley N° 24.767.

CAPITULO IV

SUJETOS INTERVINIENTES EN LOS DELITOS INFORMATICOS SEGÚN NUESTRA LEGISLACIÓN PENAL:

A.- Sujeto Activo:

En presente capítulo, nos proponemos clasificar los posibles sujetos activos de los ataques contra un sistema o dato informático, o bien el sujeto activo de delitos que utiliza como medio las nuevas tecnologías de la información para cometer delitos reprimidos por la legislación penal argentina.

Las personas que cometen delitos creados en virtud de las nuevas tecnologías constituyen una esfera de estudio relativamente nueva. Se conocen bien las motivaciones de delincuentes más tradicionales como los pedófilos, autores de fraudes o traficantes de drogas. La adaptación de esos delincuentes a las nuevas tecnologías requiere un examen desde la perspectiva de la delincuencia relacionada con las redes informáticas[42].

Citando a Lilli y Massa[43], se ha observado que estas conductas son cometidas generalmente por personas de un determinado nivel de inteligencia y educación que superan al común (hackers). Pertenecen a sectores instruidos, con acceso a determinados oportunidades y conocimientos imprescindibles que les permiten incrementar su riqueza mediante el uso de modernas técnicas a las que tienen acceso por su ocupación o disponibilidad de medios, como así también otros fines diferentes a lo meramente económico[44].

---

[42] Naciones Unidas, Consejo Económico y Social, Comisión de Prevención del Delito y Justicia Penal, "Conclusiones del estudio sobre medidas eficaces para prevenir y controlar los delitos de alta tecnología y relacionados con las redes informáticas" 10° periodo de sesiones, Viena 8 a 17 de mayo de 2001.

[43] LILLIi, Alicia Raquel, citada por Riquert Marcelo Alfredo, Informática y Derecho Penal Argentino, Bs. As., Ad-Hoc, 1999, p.52.

[44] Los piratas ya no tienen un parche en su ojo ni un garfio en reemplazo de la mano. Tampoco existen los barcos ni los tesoros escondidos debajo del mar. Llegando al año 2000, los piratas se

Siendo potenciales autores: operadores, programadores, analistas, supervisores, personal técnico y de servicio, funcionarios superiores y de control, impostores, ex empleados. Por su parte es sumamente notable el crecimiento del número de adolescente que se ven involucrados en hechos de esta naturaleza, en donde se verifican diferentes hechos de piratería informática[45].

presentan con un cerebro desarrollado, curioso y con muy pocas armas: una simple computadora y una línea telefónica. Hackers. Una palabra que aún no se encuentra en los diccionarios pero que ya suena en todas las personas que alguna vez se interesaron por la informática o leyeron algún diario. Proviene de "hack", el sonido que hacían los técnicos de las empresas telefónicas al golpear los aparatos para que funcionen. Hoy es una palabra temida por empresarios, legisladores y autoridades que desean controlar a quienes se divierten descifrando claves para ingresar a lugares prohibidos y tener acceso a información indebida. http://www.monografias.com/trabajos/hackers/hackers.shtml

[45]http://sedici.unlp.edu.ar/bitstream/handle/10915/55608/Documento_completo.pdf-PDFA.pdf?sequence=1.SID 2015, 15º Simposio Argentino de Informática y Derecho. La problemática de los perfiles falsos en Facebook y su relación con el Cibercrimen Abog. Marcelo G. I. Temperini1 A.I.A. Maximiliano Macedo. “Año tras año, sigue aumentando la cantidad de usuarios que se suman a las nuevas tecnologías, en cualquier de sus distintas alternativas, entre ellas y quizás más populares: las Redes Sociales. Según distintos estudios, Facebook sigue liderando el ranking de usuarios que usan sitios de redes sociales. El presente trabajo pretende hacer foco sobre la situación de los perfiles falsos existentes en la Red Social Facebook, precisamente por ser reconocida como aquella de mayor utilización, tanto en Argentina como a nivel mundial. En el mundo del cibercrimen, son los perfiles falsos en Facebook una herramienta de uso cotidiano por parte de aquellas personas que realizan un daño, es decir, son en muchos casos estos perfiles el medio a través del cuál se cometen delitos como injurias, extorsiones, amenazas, estafas y en los peores casos, corrupción de menores y grooming”. La Audiencia Provincial de Segovia ha confirmado la Sentencia que dictó en el año 2008 el Juzgado de instrucción nº 4 de Segovia, condenando a dos jóvenes adolescentes a indemnizar a otra compañera con 12.400 euros (la Audiencia ha rebajado la cuantía de 18.284 euros a 12.400) por los daños morales ocasionados por suplantar su identidad en la red social twenti y utilizar dicho perfil para enemistarse y ser repudiada por el resto de sus compañeros. La Sentencia no recoge la petición de las demandantes consistente en que las condenadas publicaran la sentencia en sus respectivos perfiles sociales. Todo comenzó cuando a las dos condenadas se les ocurrió crear un perfil en twenti, haciéndose pasar por una compañera, y publicando su nombre, lugar de nacimiento y lugar donde estudió, y subiendo una fotografía de la suplantada. Las adolescentes valiéndose de este falso perfil, procedían a hacer comentarios denigrantes de otros compañeros que habían colgado fotografías en la red. Como es lógico, los compañeros, creyendo que dichos comentarios provenían de la denunciante, criticaron duramente a la chica, y provocó que estos le hicieran el vacío asilándola socialmente, retirándole incluso el saludo. Y es que en estas edades, para los adolescentes es muy importante la imagen que se proyecta a los amigos y compañeros, así como la aceptación e integración en el grupo, extremo que ha puesto de manifiesto la Audiencia al advertir del riesgo que conlleva el mal uso de las redes sociales, “dada la vulnerabilidad emocional que estos presentan debido a la corta edad y el momento evolutivo en el que se encuentran”. Es fundamental que los padres orienten y asesoren a sus hijos en el uso de Internet y en concreto de las redes sociales, ya que en este caso la sentencia condena al pago de una indemnización, sin embargo en otros casos similares (con la mayoría de edad) la condena podría ser de privación de libertad.
http://www.delitosinformaticos.com/06/2011/noticias/condenadas-dos-adolescentes-por-suplantar-a-una-companera-y-crear-un-peril-faso-en-la-red-social-tuenti

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los cometidos. De esta forma, la persona que “ingresa” a un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

El nivel típico de aptitudes del delincuente es tema de controversia, ya que para algunos en el nivel de aptitudes no es un indicador de delincuencia informática, en tanto que otros aducen que los posibles delincuentes informáticos son listos, decididos, motivados y dispuestos a aceptar un reto tecnológico. Sin embargo, teniendo en cuenta las características ya mencionada de las personas que cometen delitos informáticos, estudiosos en la materia los han catalogados como “delitos de cuello blanco”, término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en 1943.

El hecho que marca la mayor diferencia en los cambios criminológicos surge de la globalización, como también del surgimiento de las nuevas tecnologías donde se mezclan diferentes culturas, historias, creencias, rituales, ideologías, dando paso a relaciones sociales más conflictivas y complicadas, creando una criminalidad más compleja, lo que obligaría al cambio de estrategias para su resolución. En la actualidad se diferencia con tres cambios fundamentales: perfil del delincuente, exposición en la comisión del delito y la disminución al mínimo en la amenaza física dirigida al delincuente.

Las personas que cometen los delitos informáticos, son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes. Esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, bien hábiles en el uso de los sistemas informatizados, aún en muchos de los casos, no son actividades laborales que faciliten la comisión de este tipo de delitos. El hecho de que no sea considerado el sujeto activo un delincuente común está determinado por el mecanismo y medio de acción que utilice para producir el daño, quienes en la mayoría de los supuestos en que se manifiestan y las funciones que se desempeñan pueden ser catalogadas sujetos especiales. Representándose por un perfil determinado de los usuarios de las nuevas tecnologías e

Internet, estas personas tienen accesos a un computador, educación suficiente como para utilizar en forma adecuada y medios para su conexión a Internet[46].

B. Sujeto pasivo

En primer término, tenemos que distinguir que sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, en el caso de los "delitos informáticos" las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etc., que usan sistemas automatizados de información, generalmente conectados a otros[47].

Debemos que los organismos internacionales han adoptado resoluciones similares en el sentido de que "educando a la comunidad de víctimas y estimulando la denuncia de los delitos se promoverá la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos".

También podemos marcar una tendencia a la victimización masiva causada por delitos como la propagación de virus, porque el número de víctimas es sencillamente demasiado grande como para poder ser determinado y contado[48].

C. Conductas relacionadas con los delitos informáticos

Con el advenimiento de la era de la computación han surgido diversos apelativos que se emplean para designar a personas o grupos de ellas que se dedican a actividades ilícitas a saber:[49]

- Hackers:

[46] TOBARES CATALA, Gabriel H., CASTRO ARGÜELLO, Maximiliano J., Delitos Informáticos, ob. Cit. p. 92
[47] TOBARES CATALA, Gabriel H., CASTRO ARGÜELLO, Maximiliano J., Delitos Informáticos, ob. Cit. p. 95
[48] Naciones Unidas, Consejo Económico y Social, Comisión de Prevención del Delito y Justicia Penal, "Conclusiones del estudio sobre medidas eficaces para prevenir y controlar los delitos de alta tecnología y relacionados con las redes informáticas" 10° periodo de sesiones, Viena 8 a 17 de mayo de 2001.
[49] TOBARES CATALA, Gabriel H., CASTRO ARGUELLO, Maximiliano J., Delitos Informáticos, ob. Cit. p. 97

La definición más comúnmente asociada al término hacking hoy en día es intrusión sigilosa en un sistema informático sin autorización. La actividad del hacker en un sistema puede tener distintas finalidades, pero en general, en la mayoría de los casos, solo tiende a eliminar los pasos de seguridad del sistema con el solo objeto de ver el contenido de la información protegida. El hacker es una persona que se apasiona por las computadoras y se dedica a ellas más allá de los límites.

El hacking se considera una ofensa o ataque al derecho de gentes, y no tanto un delito contra un estado concreto, sino más bien contra la humanidad. El delito puede ser castigado por los tribunales de cualquier país en el que el agresor se halle. La esencia del hacking consiste en que el pirata no tiene permiso de ningún estado soberano o gobierno en hostilidades con otro. Los hackers son considerados delincuentes comunes en toda la humanidad, dado todas las naciones tienen igual interés en su captura y castigo.

Actualmente mientras la cibergalaxia oficia cada vez más de soporte para los archivos y el funcionamiento de medianas y grandes empresas, los ataques a sus redes están a la orden del día. El peligro de que sean vulneradas está siempre latente. En cuanto a las “amenazas” podemos clasificarlas en “internas” acechan porque los usuarios conocen la red y tienen accesos a ella por trabajo y “externas” en manos de atacantes que pululan por el mundo virtual empeñados en crearles problemas a las empresas.

Por fortuna, hace aproximadamente cinco años han surgido los denominados “hackers éticos”, pero ¿de quienes se trata? Es la pregunta recurrente, son personas diestras en vulnerar los sistemas de red ajenos privilegiando sus principios y decidieron con ello hacer negocio. Lo que hacen es lo contrario a “invadir” como su nombre lo indica, utilizan las herramientas de los hackers pero como auditores para chequear el estado de la seguridad de una empresa[50].

Los “hackers éticos” o “hackers blancos” trabajan lejos de la estigmatización y apasionados por la tecnología, depurando las fallas que encuentran en

[50] VENOSA, Paula, Licenciada en Informática de la Universidad de La Plata y titular de la Cátedra de Seguridad y Privacidad en Redes.

las redes de las empresas y que serían lugares potenciales de peligro en manos de un hacker corriente.

Un “hacker ético”, tal como lo explica el Ingeniero Osvaldo Falabella, consultor de IT (Informática y Tecnología) del Ministerio de Educación, Ciencia y Tecnología de la Nación, desarrolla dentro de una compañía las funciones de auditoría, control y revisión detección de fallas y posterior diagnóstico. Suele ser la persona que detecta las falencias y las reporta.

Pero ¿desde cuándo comenzó a requerirse éste tipo de servicios? La concientización en temas de seguridad en todo el mundo no lleva a más de cinco años de desarrollo. “Se utiliza desde que la información se convirtió en un activo importante, equiparándose con activos tan transcendentes como el dinero tangible. Por ende, la destrucción o robo de estos datos podría llevar a la bancarrota a muchas organizaciones”[51].

En cuanto a la legislación que lo exige como condición de funcionamiento empresarial fue implementada hace ochos, pero recién hace dos años que comenzó a cumplirse.

Un dato importante, los que están en el ambiente asegura que los expertos en seguridad argentinos están cada vez mejor vistos en el mundo. En el país existen nueve empresas que se dedican exclusivamente a la seguridad informática. Se emplazan en Capital Federal, Córdoba y Entre Ríos y cuentan con veinte empleados cada una. A esos se les suma los “hackers éticos” independientes. Hoy en día, hay muchas empresas e instituciones gubernamentales que requieren estos servicios de profesionales capacitados para ello.

Pero ¿cuál es el perfil de un “hacker blanco”? El 90% tiene entre 25 y 30 años. Su tarea consiste en revisar códigos de aplicaciones y testear las configuraciones de los hosts de escritorios y los hosts servidores, y además velar por la configuración completa de las arquitecturas de red con todo su equipamiento. Para cada uno de sus procesos, se manejan en el más estricto ambiente de confidencialidad,

[51] COLANERO, Nicolás, Jefe de Redes de la Cooperativa Tres Límites Ltda. de la Localidad de Berazategui.

utilizando herramientas de revisión online para minimizar el riesgo de copiado de la información.

- Cracker:

Para las acciones nocivas existe la más contundente expresión “cracker” o “rompedor”. Sus acciones pueden ir desde simples destrucciones, como el borrado de información, hasta el robo de información sensible que puede vender. El cracker tiene como intención destruir. Presenta dos vertientes, el que se infiltra en un sistema informático y roba información o produce destrozos en él, y el que se dedica a desproteger todo tipo de programas, tanto de versiones shareware para hacerlas plenamente operativas como programas completos comerciales que presentan protección anti copia.

- Virucker:

Es aquella persona que se dedica “que programa virus informáticos que se insertan dolosamente en sistemas informáticos, siendo una variante el que inserta un programa contaminado sin haber intervenido en el diseño del programa destructor”

Existen dos tipos de virus, los benignos que molestan, pero no dañan, y los malignos que destruyen información o impiden trabajar. Suelen tener capacidad para instalarse en un sistema informático y contagiar otros programas e inclusive, a otros ordenadores a través de intercambio de soporte magnético, como disquetes o por enlace entre ordenadores.

- Phisher

Phishing es un término utilizado en informática con el cual se denomina el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta, como puede ser información detallada de tarjetas de créditos, una contraseña u otra información bancaria. Quien lo practica es conocido con el nombre de phisher.

La doctrina los define como aquellos piratas informáticos encargados de clonar páginas web de instituciones bancarias o financiera a fin de obtener

mediante ellas las claves de los usuarios del sistema de transferencias electrónica de los fondos.

CAPITULO V

ANALISIS DE LAS FIGURAS PENALES CONTEMPLADAS EN LA LEGISLACIÓN NACIONAL

A.- Figuras penales contempladas en el Convenio de Ciberdelincuencia y su influencia en la Legislación Argentina:

El objetivo de este capítulo, es analizar las figuras penales contempladas en el Convenio de Budapest y su influencia en la Legislación Argentina, mediante la cual se introdujeron nuevas figuras delictivas.

Tal como lo adelantamos, el Convenio sobre Ciberdelincuencia se estructura de la siguiente manera, legisla sobre derecho penal material, definiendo el Derecho penal sustantivo, en su Cap. II. Secc. 1, está destinada a crear una base común de delitos, que incluye los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos (arts. 2° a 6°), los delitos informáticos (arts. 7° a 8°), los delitos relacionados con el contenido (art. 9°) y los delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines (art. 10°).

Ahora bien, nuestra legislación nacional, circunscribiendo en análisis a la ley 26.388, podemos detallar, las siguientes figuras penales, que fueron incorporadas al Código Penal, a los fines de adecuar nuestra norma de fondo al Convenio de Budapest.

Así, en primer lugar, podemos mencionar la pornografía infantil. La Convención, en su artículo 9°, trata las infracciones relativas a la pornografía infantil, en su artículo 9.2, explica que “pornografía infantil” comprende cualquier material pornográfico que representa de manera visual a un menor. En el mismo artículo, autoriza a los Estados parte a formular reserva al aceptar el tratado respecto a la punición de la simple tenencia de pornografía infantil y la inclusión en el tipo penal de las imágenes simuladas.

Por su parte, Argentina actualizó mediante la Ley 26.388 el artículo 128 del Código Penal, el cual, se sustituyó, mediante la sanción de la Ley 27.436, quedando redactado de la siguiente manera: “Será reprimido con prisión de tres (3) a seis (6) 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 un (1) año el que a sabiendas tuviere en su poder representaciones de las descriptas en el párrafo anterior. Será reprimido con prisión de seis (6) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el primer párrafo 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. Todas las escalas penales previstas en este artículo se elevarán en un tercio en su mínimo y en su máximo cuando la víctima fuere menor de trece (13) años.

Con esta reforma, se castiga la tenencia de pornografía infantil, atento a que anteriormente, solo esta reprimida la producción y distribución de material pornográfico.

Es de destacar que, según datos oficiales, el 85 por ciento de los ciberdelitos que se investigan en la ciudad de Buenos Aires estén vinculados con la pornografía infantil y el grooming. A nivel mundial, la Argentina es uno de los países con más tráfico de pornografía infantil. Sumado a ello, en los últimos años se han duplicado las denuncias y causas judiciales.

Es necesario destacar, que la simple tenencia sin fines de distribución o comercialización (por ejemplo, con fines de consumo personal) sería atípica, dada la exigencia de ésta peculiar finalidad en el tipo penal que analizamos.

En cuanto al objeto, se trata de una representación, por lo cual cualquier imagen, fotografía o dibujo o video con fines sexuales, no es necesario que sea una imagen entera, basta que sea de sus partes íntimas.

La finalidad de la imagen “con fines predominantemente sexuales” es importante para diferenciarla de fotos artística. La representación debe buscar convertir al menor en un objeto sexual y ello tiene que surgir de la imagen.

a.- Violación de Secretos y de la Privacidad:

Por su parte el Convenio de Budapest, contempla en su Capítulo II, Sección 1, Título 1, las infracciones contra la confidencialidad, en su artículo 3, reprime, la interceptación, dolosa y sin autorización, cometida a través de medios técnicos, de datos informáticos, en transmisiones no publica- en el destino, origen o en interior de un sistema informático, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte tales datos.

Los nuevos delitos contra la privacidad constituyen la reforma más importante de la ley 26.388. Surgieron, por la necesidad de penalizar las frecuentes violaciones a la privacidad del correo electrónico y de otras formas de comunicación.

La reforma apunta a jerarquizar aún más el rango protectorio que tienen los delitos contra la libertad. Con razón se ha dicho que la libertad pertenece a la clase de derechos fundamentales denominados derechos de la personalidad, o inherentes a la personalidad, como derecho a la conservación de la propia existencia y a la integridad moral y física.[52]

a.1. Reconfiguración del bien jurídico

La reforma amplia el epígrafe del capítulo III, del Título V, de la parte especial del Código Penal, incluyendo la “privacidad” como bien jurídico protegido. Explica el dictamen del Senado que “sobre todo a tenor de lo prescripto por el inc. 3 del art. 157 bis del C. P., ya que la norma entiende más como afectación a la intimidad que al bien jurídico secreto[53]. Para varios autores el art. 153 bis del C. P., incluido en la reforma también refuerza la protección de este bien jurídico en ambientes digitales[54].

[52] GOSCILA, Antonieta, “Los bienes jurídicos penalmente protegidos” Lecciones y Ensayos, Segunda Época, 1, Temas de Derecho Penal II, diciembre de 1981, p. 25.
[53] CÁMARA DE SENADORES, Orden del Día N° 959/ 2007 (16/11/2007)
[54] PALAZZI, Pablo A., Los delitos Informáticos en el Código Penal, Análisis de la ley 26.388, Bs. As., Abeledo Perrot, 2009, p. 66

Hay que reconocer que la privacidad ya estaba amparada en el Código Penal en diversos delitos, tales como el de la violación de domicilio, el allanamiento ilegal, la violación de secretos y la de la correspondencia. Pero la inclusión de esta nueva terminología para denominar bien jurídico penalmente protegido tiene un claro carácter pedagógico e interpretativo.

Se ha dicho que “el bien jurídico penalmente protegido es el determinado previamente como tal por una comunidad ubicada en el tiempo y en el espacio, que, por decirlo de alguna manera, elige qué entidad merece ser considerada como bien por satisfacer sus necesidades individuales y sociales”.

Pues bien, no cabe dudas que las nuevas tecnologías han aumentado los riesgos y peligros para el derecho a la privacidad[55]. Hoy en día existen cientos de bases de datos almacenando datos personales; nuestros rastros, imágenes digitales quedan registrados en numerosos lugares en la web, en videocámaras de ingreso

[55] Google cambió su política de privacidad y hay polémica. Ahora puede cruzar los datos de sus usuarios recogidos en todos sus servicios. Varios países exigen a la empresa dar marcha atrás. Arguyen que viola derechos. El mito de que en internet todo es gratuito quedó desterrado con la publicidad que uno recibe sin ningún consentimiento. No conforme con recopilar datos del interesado, Google acaba de implementar un polémico régimen de privacidad que pretende ir un paso más allá. Ahora varios países exigen dar marcha atrás con esta medida. La acción de Google apunta a recoger y cruzar información privada entre cerca de 60 productos y servicios que brinda en forma gratuita. Esto se traduciría en avisos más efectivos y personalizados. Este cambio, que entró ayer en vigencia, generó confusiones que la firma trató de aclarar tanto a los particulares como a gobiernos de distintos países, quienes desean entender la forma en cómo la compañía maneja y administra esos datos. Una investigación de la Comisión de Protección de Datos francesa, por encargo de la Unión Europea, llegó a la conclusión de que la nueva regulación viola el derecho comunitario. A través de un comunicado, la empresa se defiende argumentando: "Nuestra política de privacidad ahora explica, para la gran mayoría de nuestros servicios, qué datos estamos recopilando y cómo podríamos utilizarlos, en un lenguaje sencillo". Otras firmas como Facebook, Microsoft, Apple y Sony -que también realizan un seguimiento- se diferencian porque poseen una visión fragmentada de cada usuario. En cambio Google es uno de los pocos privilegiados que puede obtener una perspectiva integral del interesado.

Además de saber hacia dónde se orientan sus búsquedas y qué puntos recorre con Chrome, su navegador, esto lo puede combinar con los videos que mira en Youtube, las citas que tiene en su calendario y el tipo de documentos que comparte. La clave para unificar todos estos servicios es el servicio de correo Gmail, que requiere estar registrado en forma permanente. Si a esto se le suma un teléfono inteligente con Android, que obligatoriamente requiere una cuenta de Gmail, la situación se complejiza un poco más. Para los críticos, la nueva política no da a los usuarios otra opción que aceptarla o dejar de usar los servicios de Google, lo que le otorga poderes sin precedentes para vigilar a los navegantes. A su favor señalan que "la nueva política no cambia ninguna configuración de privacidad existente ni la manera en que la información personal es compartida fuera de Google". Lo cierto es que no está diciendo cómo proteger la privacidad. Google sólo explica como reunirá información, combinándola de manera inteligente y usándola para vender más publicidad. Edición Impresa: sábado, 03 de marzo de 2012. http://www.losandes.com.ar/notas/2012/3/3/google-cambio-politica-privacidad-polemica-627597.asp

a edificios, en estadios, plazas y otros lugares públicos, en tarjetas usadas para el ingreso a oficinas, en correos electrónicos y comunicaciones por chat, en las búsquedas en internet, mensajes de textos telefónicos y mensajería instantánea.

La sociedad es consciente de todo ello. Se han aprobado marcos legales para poner límite al uso que se haga de estos datos como la inclusión de la garantía de hábeas data en la reforma constitucional del año 1994 y la Ley de Protección de Datos Personales (Ley 25.336)[56], junto a sus recientes reglamentaciones. Pero

[56] Sala II Causa n° ° 25.062 -Ilic, Dragoslav s/ medios de prueba-• Juzg. Fed. n* ° 7 Secret. N° ° 14. Expte. N° ° 6924/2006/3. Buenos Aires, 5 de junio de 2.007.Y VISTOS Y CONSIDERANDO: I Llegan estas actuaciones a conocimiento y decisión del Tribunal en virtud de la apelación deducida a f. 20/4 por Dragoslav Ilic, con el patrocinio letrado de los Dres. José M. Ubeira y Juan J. Ribelli, contra la resolución del Magistrado a quo que declaró ilegítima la utilización como medio de prueba de los mails agregados a f. 2/38 del principal y la imposibilidad de pronunciarse, a partir de ello, con respecto a su solicitud de ser tenido como parte querellante (puntos dispositivos I y II). El recurrente se agravia de lo así resuelto básicamente por entender que el acceso ilegítimo a una cuenta de correo electrónico, si bien un hecho claramente inmoral y enemistoso, no resulta típico a la luz de las normas penales que sancionan la violación de las comunicaciones arts. 153 y siguientes, por lo que las piezas obtenidas de tal modo no pueden reputarse -prueba ilícita-• ni por tanto ser excluida su valoración. Subsidiariamente, planteó la existencia en autos de vías independientes que habilitarí-an de igual modo la investigación de esta hipótesis delictiva. II Advierten los suscriptos que la pretensión del recurrente parte de un enfoque equivocado: es que se considere o no al hecho como típico del delito de violación de correspondencia debate que, inversamente a lo sostenido, no se encuentra zanjado en la jurisprudencia (Fallos 328:3324) no es lo que en su caso determinará la inadmisibilidad como prueba en el proceso de los elementos de tal forma adquiridos, sino la circunstancia de haberse obtenido mediante la transgresión a un derecho constitucional. Sentado lo anterior y ya en estricta relación al caso en estudio, cabe recordar que el artículo 19 de la Constitución Nacional también el Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana sobre Derechos Humanos (arts. 17 y 11) consagra el derecho a la privacidad y con ello la existencia de un ámbito de autonomía individual reservado a cada persona sólo penetrable por su libre voluntad, comprensivo de los sentimientos, hábitos, costumbres, aspectos de la personalidad y en suma de aquellas acciones, hechos o datos no destinados a ser difundidos (CSJN, in re -Ponzetti de Balbín-• , Fallos 306:1892). Es en protección de éste área de reserva que sin agotar su alcance el propio texto constitucional establece como garantías la inviolabilidad del domicilio, de la correspondencia epistolar y de los papeles privados (cf. en especial, Considerando 20 del voto del ministro Petracchi), las cuales encuentran su correlato a nivel legislativo en las respectivas disposiciones de los códigos sustantivos, los de procedimiento y otras normas, como la ley N° 25.520 que, en lo aquí pertinente, dispone: -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-• (artículo 5 °). Una adecuada y progresiva exégesis de las cláusulas involucradas revela entonces sin mayor dificultad que los intercambios que mantienen los individuos mediante el uso de nuevas tecnologías, como el correo electrónico, están comprendidas en el ámbito de autonomía propio del derecho a la privacidad (cf. en este sentido, Gelli, María Angélica, -Constitución de la Nación Argentina. Concordada y Comentada-• . La Ley, Buenos Aires, 2003, p. 203/8; y Maier, Julio B. J., -Derecho Procesal Penal. Fundamentos-• . Editores del Puerto, Buenos Aires, 1996, p. 694), que como tal importa un límite al poder estatal, pero también a la acción de los particulares, sólo franqueable por el consentimiento libre de su titular o en los casos que mediante una reglamentación razonable se establezcan por ley. Tal es, por otra

constantemente nos encontramos con nuevos casos de robo de identidad[57], de sustracción de información personal o de venta masiva de base de datos personales. Ante este

parte, el criterio también adoptado por otros tribunales (cf. de la C.C.C., Sala IV, causa n° 25.065 -Redruello-• del 15/11/04, y de la Sala I, causa n ° 19.418 -Grimberg-• del 11/2/03 y causa n° 20.009 -Yelma-• del 22/4/03). Ahora bien, ninguna de esas situaciones de excepción se presenta en el supuesto de autos: el acceso a la cuenta de correo electrónico de donde se extrajeron copia de los mails en cuestión no fue autorizada por su titular (cf. el testimonio del periodista Daniel Santoro a f. 54 del principal) como tampoco por alguna autoridad judicial en el regular ejercicio de su jurisdicción, por ejemplo, en uso de las facultades regladas en el artículo 231 o siguientes del Código Procesal Penal de la Nación. De allí, que no cabe sino concluir en que los elementos arrimados anónimamente al estudio de uno de los letrados patrocinantes del recurrente fueron obtenidos merced una ilegal intromisión en la privacidad pues más allá de que pueda ello reputarse o no un delito penal, sin dudas constituye un acto ilícito en los términos del Código Civil, Libro Segundo, Sección Segunda, Título VIII -De los actos ilícitos-• , artículo 1071bis en franca violación de un derecho constitucional y, por ello, deviene inadmisible su incorporación al proceso como prueba válida. Repárese en que una solución contraria, de conformidad con los precedentes de la Corte Suprema de Justicia de la Nación en la materia, comprometería la buena administración de justicia al pretender constituirla en beneficiaria del hecho ilícito a través del cual se adquirieron tales evidencias (Fallos 303:1938, 306:1752 y 308:733). Sólo resta señalar entonces que no es posible tratar a los dichos del damnificado, posteriores al suceso y específicamente relativos a ese actuar ilegítimo del que fue víctima, como un cauce de investigación independiente. Resulta manifiesto que ellos no pueden ser desvinculados de esa vía, máxime si se tiene presente la repercusión pública que adquirió el hecho. En mérito de todo lo hasta aquí expuesto, el punto dispositivo I de la resolución que viene apelada se confirmará. III Sin perjuicio de lo resuelto, debe señalarse que en su anterior intervención en autos la Sala ordenó sustanciar el debate precedente por considerar que la legitimidad o no de los mails como medio de prueba constituía una cuestión sin cuya previa dilucidación no era posible analizar la solicitud del impugnante que apoyándose en el contenido de esas piezas pretendía ser tenido como parte querellante (cf. auto del 26/10/06, reg. N° 25.928, cuya copia encabeza este legajo). Así, superado ese extremo, no existe óbice alguno para pronunciarse sobre su pedido y definir finalmente su situación procesal en estas actuaciones; lo cual, a esta altura, se impone. Por tal motivo, corresponde dejar sin efecto lo resuelto en el punto dispositivo II, debiendo el Juez a quo expedirse por la procedencia o no de su admisión como parte en el proceso. Por otra parte, se advierte que ningún temperamento se adoptó en torno a lo dispuesto por la Sala en el Considerando III de la citada decisión. IV Por último, en punto a la solicitud efectuada a f. 23 cabe hacer notar que tal como se desprende del principal la Comisión de Disciplina y Acusación del Consejo de la Magistratura ya ha tomado vista recientemente de la totalidad de este expediente (f. 143, 1144/5 y 1150). Por todo lo expuesto, el TRIBUNAL RESUELVE: I) CONFIRMAR el punto dispositivo I de la decisión impugnada, que declaró ilegítima la utilización como medio de prueba de los mails agregados a f. 2/38 del principal. II) DEJAR SIN EFECTO el punto resolutivo II de ese decisorio, DEBIENDO el Sr. Juez de grado, devueltas que le sean estas actuaciones, proceder del modo indicado en la presente. Regístrese, hágase saber al Sr. Fiscal General y remítase a primera instancia, donde deberán efectuarse las restantes notificaciones a que hubiere lugar. http://www.habeasdata.org/wp/2007/07/12/caso-Dragoslav-acceso-correo-electronico-sin autorizacion-ilegal/

[57] "De un día para el otro comencé a recibir reclamos e insultos por productos que yo no vendía y que ya habían sido pagados. Alguien había ingresado en mi cuenta con la que opero a través de Internet y yo nunca lo supe", dijo Nicolás Sánchez, de 28 años, quien compra y vende productos por Internet. El caso de Sánchez refleja cómo una persona puede ser víctima de un fraude, o bien de ser usada para estafar a terceros."Siempre tomé todos los recaudos para no ser víctima de ningún tipo de ataque en mi computadora: actualizaba el antivirus, miraba bien qué mails abría y cuáles no, era cuidadoso de los sitios en los que navegaba, pero me di cuenta de que nunca se puede estar 100% seguro." No bien notó las anomalías, Sánchez dio aviso a la empresa de lo que estaba ocurriendo. "Al otro día, me inhabilitaron para seguir operando hasta que se resolviera la situación mía y la de la gente estafada. Después de varios días, volvieron a contactarme y me explicaron que *hackers* de

panorama, el derecho penal debe acompañar estos cambios con nuevas normas que se adecuen a la realidad tecnológica actual, pero también con nuevos bienes jurídicos que conceptualicen esas necesidades. Por otra parte, la protección que este ámbito otorga al derecho penal es más necesaria, como claramente lo ha señalado la doctrina civilista[58].

El derecho a la privacidad es un fenómeno complejo y, por ende, su definición y conceptualización es difícil. Este bien jurídico puede ser susceptible de diversos ataques que merecen tutela penal. El más antiguo es el ingreso no consentido a la morada, recinto tradicional de la vida privada. La versión más moderna es el acceso no autorizado es el ilegítimo a sistemas informáticos, que la reforma incluye en como art. 153 bis del Código Penal[59].

Rumania habían ingresado en mi cuenta, ofrecían productos inexistentes y pedían a los usuarios que transfieran el dinero a cuentas de terceros."En los primeros días de 2012, el caso de fraude que tuvo como víctima a la familia Toscano, dueña de una corredora de cereales, salió a la luz, al poner en evidencia la normalidad y frecuencia en la que ocurren este tipo de delitos. Con un minucioso trabajo de inteligencia y mucha paciencia, los *hackers* monitorearon por varios días todos los movimientos de Marcelo Toscano, quien acostumbraba a manejar grandes cantidades de dinero."Los delincuentes sabían cuándo atacar, y lo hicieron a media mañana, momento en que las cuentas bancarias de la cerealera siempre registraban activos en su haber. Lograron hacerse de $ 87.000", dijo a La Nacion Marcelo Toscano."De un momento para otro, cuando terminé de realizar las operaciones de la mañana, mi sesión en Interbanking se cerró abruptamente. Como yo justo estaba saliendo, pensé que fue parte del proceso del sistema", dijo a La Nacion Marcelo Toscano."A las dos horas -agregó-, recibí un llamado del banco Santander Río en el que me informaban que no contaba con dinero suficiente para concretar las operaciones. Era imposible. Allí comenzó mi calvario.". http://www.lanacion.com.ar/1446144-vendian-cosas-a-mi-nombre-y-no-lo-sabia

[58] CASABONA, Romeo, "La reforma penal ante las nuevas tecnologías de la información", Informática e Dirito, año XIII, nro. 3, Instituto por la Documentanzióne Giuridica, Florencia, septiembre-diciembre de 1987, p. 123.

[59] El Gobierno de Canarias ha presentado ante la Fiscalía Provincial de Las Palmas una denuncia con el fin de verificar el acesso ilegítimo al ordenador de la magistrada Victoria Rosell, informó la Consejería de Presidencia, Justicia y Seguridad. El Gobierno de Canarias formuló ayer ante la Fiscalía una denuncia en la que pide que se investigue y se determinen las responsabilidades penales sobre la imputación a la administración de la posible manipulación del disco duro del ordenador de la magistrada Victoria Rosell, desde el que el periódico El Mundo asegura que se elaboró la denuncia del caso Salmón contra José Manuel Soria. La denuncia formulada ayer ante la Fiscalía Provincial, pretende que se esclarezca si existió un acceso ilegítimo al ordenador de la magistrada y desvirtuar la imputación de supuestas actividades delictivas atribuida a la Administración Pública de la Comunidad Autónoma de Canarias. La denuncia se produce después de que la magistrada Victoria Rosell dijese el pasado domingo a este periódico que sospechaba que alguien de la administración pudo hacer un uso delictivo de su ordenador, en relación a la filtración en el periódico el El Mundo de una información en la que se asegura que la denuncia presentada por su compañero sentimental, el periodista Carlos Sosa, fue redactada desde su ordenador. La magistrada reconoció que Sosa pudo remitirle la denuncia en un correo electrónico a su despacho y que la redactó en su portátil. La denuncia del Gobierno, anunciada por el consejero de la Presidencia, José Miguel Ruano, considera inadmisible la posibilidad de que la información publicada en El Mundo el pasado día 3 de diciembre fuese una filtración de los archivos del disco duro del ordenador de

Más allá de lo expuesto, a veces el objeto suele ser más amplio e incluir la imagen y la voz de las personas como elementos de la personalidad protegidos penalmente. Esto no fue el caso de la reforma argentina, pues el delito de captación ilegítima de voz e imagen no se incluyó finalmente en la aprobada. Ello sin perjuicio de que, si estas últimas están digitalizadas y almacenadas en un sistema de datos asociadas a una persona, pueden resultar aplicables a los delitos referidos a la protección de datos personales.

Algunas legislaciones como el Código Penal Español, agravan la pena si una vez que se ha accedido a esos datos, se los puede revelar, divulgar, ceder o vender. Lo cual no ha sido considerado por nuestros legisladores.

Hay que reconocer que la privacidad es un bien jurídico tenuemente amparado en el sistema penal argentino. Las penas siguen siendo bajas (solo hasta seis meses por interceptar un mail o conversación telefónica y la misma pena para acceder sin permiso a un ordenador). Además, estos delitos se cometen mediante dispositivos tecnológicos desde la clandestinidad, por lo que resulta muy difícil de descubrir quienes son los responsables que afectan la intimidad de las personas.

---

trabajo de Victoria Rosell, dado que, hasta la fecha, nadie ha procedido a recuperar la información del disco duro. La denuncia expone a la Fiscalía que la información aparecida en prensa parte de los datos que figuran en las «propiedades» del fichero que el periodista Carlos Sosa remitió a los medios de comunicación con la denuncia en la que aparece el rastro informático «Rosell» y guardado por «Carlos». Para el Gobierno de Canarias, el hecho de que la propia magistrada reconociera que la denuncia fue redactada por su compañero sentimental, el periodista Carlos Sosa, desde su ordenador portátil, descarta cualquier posibilidad de que la filtración pueda tener relación con el disco duro del ordenador de trabajo de la magistrada en su despacho del Juzgado de Instrucción número 8 de Las Palmas de Gran Canaria. Avala esta tesis del Gobierno el hecho de que la clave de usuario de la magistrada no es «Rosell», sino otra más compleja. La Dirección General de Relaciones con la Justicia, que es el órgano del Gobierno de Canarias que formuló ayer la denuncia, considera especialmente «grave» que la magistrada pretenda establecer algún tipo de relación entre la rotura del disco duro de su ordenador de trabajo y la información publicada por el periódico El Mundo el día 3 de diciembre pasado. Según el Gobierno se trata de hechos perfectamente diferenciados e independientes, como acredita en la denuncia. En todo caso, y para evitar todo tipo de sospechas, el propio Gobierno ha solicitado un informe de la cadena de custodia del disco duro desde que salió del Juzgado a petición de la propia magistrada el pasado día 26 de noviembre hasta su recepción.El Gobierno ha requerido a la empresa a la que se le solicitó la reparación del disco duro en Madrid que paralice el trabajo y lo devuelva a la Dirección General, para ser entregado de inmediato a la Fiscalía. La magistrada Victoria Rosell había renunciado a su reparación y solicitó que se le devolvieran a su juzgado. 09 DIC2010. PORTADANACIONAL.
HTTP://WWW.MAXINFORMACION.ES/INDEX/NS/ID/23

Además de la privacidad en espacios físicos, encontramos también la protección constitucional de los papeles privados y de la correspondencia (art. 18 de la C. N.). Por extensión natural, el correo electrónico y cualquier otra moderna forma de comunicación debe ser tributaria de la misma protección y esto es lo que se ha logrado con la reforma de la ley 26.388.[60]

a.2 Violación de correspondencia electrónica

La ley 26.388 sustituyó el art. 153 del C. P. por el siguiente: Artículo 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."

Es de destacar que la razón de este último párrafo se explica por el origen que tuvo el proyecto de ley, destinado a evitar la intercepción y acceso no autorizado a correos electrónicos de jueces y periodistas, según se difundió ampliamente por la prensa en el año 2006.

Con el mencionado párrafo y el agregado del segundo, el proyecto no innova creando nuevos tipos penales, sino que les agrega el término "comunicación electrónica" a los existentes para actualizarlos frente al desarrollo tecnológico.

[60] PALAZZI, Pablo A., Los delitos Informáticos en el Código Penal, Analisis de la ley 26.388, Bs. As., Abeledo Perrot, 2009, p. 67 y 68.

En este sentido, la Justicia ratificó que es un delito la violación de e-mails[61].

a.3. Antecedentes[62]

Hoy en día se ha incorporado a la vida del hombre una nueva forma de comunicación de alcance nacional e internacional. Los avances en la ciencia y la tecnología han sido plasmados en objetos e instrumentos que día a día cambian o influyen fuertemente en la vida de las personas a escala mundial. El hecho de poder comunicarse en forma simple y eficaz a través de una red de comunicaciones y datos, sea interna (Internet), ha generado una "revolución" en la era de las comunicaciones y de la informática. Surge la necesidad de proteger la información contenida en el mensaje, sea este escrito en un medio de papel electrónico, la correspondencia tradicional o los modernos sistemas informáticos o tecnológicos de comunicación, como son el correo electrónico de datos o e-mail y los mensajes de textos vía telefonía celular. Teniendo en cuenta estos avances tecnológicos que permiten bases de datos, terminales computacionales, sistemas de transmisión inalámbrico, microondas, satélite, celulares, etc., utilizados en los distintos medios, todos son avances maravillosos en cuanto a mejorar la calidad de vida del hombre, y que requieran la protección correspondiente en cada caso.

No podemos soslayar, que a medida que las tecnologías avanzan van creando y van surgiendo nuevas formas y alternativas de comunicación que son muy utilizadas gracias a su fácil acceso y costo reducido; tales como el chat en línea, mensajes de textos (SMS-MMS en telefonía celular) entre otros. Digno de tutela y protección a la par del correo electrónico, por involucrarse también el derecho a la intimidad de las personas.

---

[61] Un tribunal consideró que la violación de correo electrónico es equiparable a la de correspondencia tradicional. Fue al anular una resolución de primera instancia que mandó archivar una causa. La ley impone hasta un año de prisión a quienes incurran en la violación de correspondencia electrónica privada… Por sus características, el e-mail, "goza de una protección de la privacidad más acentuada que la clásica vía postal, ya que para su funcionamiento y utilización se requiere indispensablemente de un prestador del servicio, el nombre de usuario y clave de acceso destinados a impedir que terceros extraños se entrometan en los datos y contenidos que se emiten y reciben", agregó el tribunal. Fuente:
Télam.http://www.rosario3.com/tecnologia/noticias.aspx?idNot=33002

[62] TOBARES CATALA, Gabriel H., CASTRO ARGUELLO, Maximiliano J., Delitos Informáticos, Córdoba, Advocatus, 2009, p.205.

El Código Penal Argentino antes de la reforma ordenada por la Ley 26.388 establecía en su Capítulo III- Violación de Secreto-, en los arts. 153 a 157 bis una exhaustiva protección al contenido de las comunicaciones y los secretos que de ella surjan.

No obstante, ello, en virtud del principio de legalidad imperante en nuestro ordenamiento jurídico, no era factible asimilar los conceptos de correspondencia electrónica o e-mail, o la correspondencia tradicional, con la consecuente desprotección ocasionada por el vacío legal. Por ello es que su violación quedaba impune, generándose una evidente sensación de inseguridad en nuestra sociedad toda.

A pesar de esa situación, es destacable mencionar que se contaba con una normativa específica contemplada en la Ley de Telecomunicaciones (19.798) en sus art. 19, 20 y 21, la cual fue publicada en el Boletín Oficial, el día 23 de agosto de 1972 en el que disponen: "Art. 19. — La inviolabilidad de la correspondencia de telecomunicaciones importa la prohibición de abrir, sustraer, interceptar, interferir, cambiar su texto, desviar su curso, publicar, usar, tratar de conocer o facilitar que otra persona que no sea su destinatario conozca la existencia o el contenido de cualquier comunicación confiada a los prestadores del servicio y la de dar ocasión de cometer tales actos. Art. 20. — Las personas afectadas a los servicios de telecomunicaciones están obligadas a guardar secreto respecto de la existencia y contenido de la correspondencia, de que tengan conocimiento en razón de su cargo. Art. 21. — Toda persona que de cualquier manera tenga conocimiento de la existencia o contenido de la correspondencia de telecomunicaciones, está obligada a de guardar secreto sobre la misma con las excepciones que fija la presente ley."

No obstante, lo analizado hasta aquí, consideramos que además de la protección dispensada desde la normativa da fondo antes de su reforma y en especial por la ley de telecomunicaciones, cuando ésta define a las telecomunicaciones 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".

La Reforma de la Ley 26.388, que en primer lugar sustituye el epígrafe del Capítulo III, del Título V, del Libro II del Código Penal por de "Violación de secretos y de la privacidad" abarcando de esta manera un bien jurídico antes no expresado

y el cual con el de las nuevas tecnologías de la información y comunicaciones era de común su vulneración, proponiendo además la incorporación al texto del código de fondo en sus artículos 3° al 8°.

Dando la importancia suficiente al agregar la indistinta naturaleza de la comunicación, a aquellas que tanto en nuestros días se vienen utilizando gracias a los progresos de las nuevas tecnologías de la información y comunicaciones, y para todos aquellos que a raíz de los mencionados pueden generarse; y causados en cualquiera de sus facetas tecnológicas o de tráfico comunicacional.

Como podemos observar, la modificación del Código Penal en cuanto a los artículos señalados, añade nuevos bienes jurídicos protegidos como el correo electrónico u otra comunicación electrónica, que son objeto de tutela por estar dentro del ámbito de privacidad de la persona, adecuándose así a los avances tecnológico que nuestros tiempos están verificando. Por su parte, afirmamos la necesidad de preservar mediante soporte legal actualizado el concepto de transmisión y recepción de datos de comunicación electrónica (e-mail), chat y mensaje de textos y otras vías de comunicación electrónica, a través de cualquiera de los medios vigentes, resultando ser una realidad impostergable resguardar la intimidad de las personas, así como también fomentar estas formas de comunicarse, cada vez más, por sus características sobresalientes de rapidez y eficiencia[63].

En virtud de que la libertad exige mantener en reserva sobre lo que se piensa, hace, tiene o padece, la sanción penal va en su auxilio para resguardar esa esfera de intimidad o reserva.

Se trata de proteger aquella manifestación de la libertad individual, prohibiendo la intromisión de terceros en la intimidad del sujeto pasivo o la comunicación de sus secretos a otros por par parte de quienes-si bien tienen derecho a conocerlo o los han conocido ilícitamente- carecen de derecho de comunicarlo, ya sea porque efectivamente violan la esfera de reserva o porque crean un peligro para ella.

[63] Fundamento Proyecto de Ley Expediente N° 2981-D-2006. Trámite Parlamentario 63 (2/6/2006)

Con el fallo judicial “Martolio C/ Lanata, Jorge Ernesto por violación de correspondencia”[64], se cubrió un vacío judicial, pero no legislativo, estableció: el tan difundido e-mail de nuestros días es un medio idóneo, certero y veloz para enviar y recibir todo tipo de mensajes, misivas, fotografías, archivos, completos, etc., es decir, amplia la gama de posibilidades de gama de posibilidades que brindaba el correo normal al usuario que tenga acceso al nuevo sistema. Es más, el correo electrónico posee característica de privacidad más acentuada que la inveterada vía postal a la que estábamos acostumbrados, ya que para su funcionamiento se requiere un prestador del servicio, el nombre del usuario y el código de acceso que impide a terceros extraños la intromisión en los datos que a través de él pueden emitirse o archivarse. Este sistema ha ido

[64] Ratifican que el e-mail es privado, como las cartas. La Sala Cuarta de la Cámara de Casación rechazó una apelación del periodista Jorge Lanata contra un fallo de la Cámara del Crimen que había decidido, en abril del año pasado, que la privacidad del correo electrónico tiene la misma protección que la del correo convencional. La resolución confirma la sentencia que había ordenado investigar cómo accedió la revista Veintiuno, en julio de 1998, a cinco e-mails privados de Edgardo Martolio, quien era entonces director sociado del ex diario Perfil. La causa comenzó cuando Martolio demandó a Lanata por haber publicado, en la revista que dirige, los textos de cinco e-mails que circularon por el correo interno del diario Perfil días antes de su cierre. En esas cartas, Martolio y Jorge Fontevecchia, entonces director del diario, hablaban de la necesidad de reducir costos se planteaban alternativas para realizar recortes en el diario."Se advierte que el fantasma del cierre sobrevolaba el diario desde mediados de mes, aunque se mantuvo en el más estricto secreto", decía el artículo publicado el 6 de agosto de 1998 en Veintiuno, acompañado por facsímiles de los e-mails. Martolio reprochó a Lanata "haberse apoderado indebidamente" de correspondencia privada y haberla publicado "cuando no estaba destinada a tal fin" y "sin consentimiento". El primer fallo judicial, dictado por el juez correccional Eduardo Etcharrán, favoreció a Lanata. El juez rechazó la causa porque consideró que no había delito. Pero Martolio apeló el fallo, y la Sala VI de la Cámara del Crimen le dio la razón. Los camaristas —Carlos González, Carlos Elbert y Luis Ameghino Escobar— consideraron entonces que "nada se opone para definir al medio de comunicación electrónico como un verdadero correo en versión actualizada y goza de la misma protección incluida en los artículos 153 y 155 del Código Penal, cuando aún no existían este tipo de avances tecnológicos". Los jueces ordenaron investigar cómo llegaron los e-mails de Martolio a poder de Veintiuno, para establecer si se cometió o no el delito de "violación de secretos". El artículo 153 del Código Penal estable ce que será reprimido con prisión de 15 días a 6 meses el que abra indebidamente una carta, un pliego cerrado, un despacho telegráfico o telefónico, o de otra naturaleza, que no le esté dirigido. También determina que se aplicará prisión de un mes a un año si el culpable le comunica a otro o publica el contenido de esa carta. El artículo 155 fija, además, una multa para los que publiquen "indebidamente" una correspondencia no destinada a hacerse pública. Aunque estos artículos no se refieren específicamente al e-mail (que es posterior a su redacción), los jueces consideraron que podía encuadrarse en las comunicaciones "de otra naturaleza" mencionadas en el Código. Incluso, los jueces dijeron, en esa oportunidad, que el correo electrónico merecía más protección que la correspondencia postal, "porque un sobre se puede perder o lo pueden robar, pero para abrir un e-mail hay que acceder al código personal" (el password) del usuario. La defensa de Lanata presentó un pedido de excepción, argumentando (en contra de lo que habían decidido los jueces) que el hecho en cuestión no estaba tipificado. De haberse concedido este recurso, el caso se hubiera cerrado. Pero, primero la Cámara del Crimen, y ahora la Cámara de Casación, decidieron que no había motivos para conceder la excepción. De esta forma, los camaristas Gustavo Hornos, Liliana Catucci y Amelia Berraz de Vidal confirmaron el fallo que ordenaba continuar la investigación. http://edant.clarin.com/diario/2000/06/07/s-03504.htm

incorporándose a la vida de las personas y, por tanto, debe tenerse en cuenta los cambios de actitudes, debiendo resguardarse la "correspondencia" manipulada vía estas nuevas tecnologías, con el mismo concepto de una carta enviada en papel, por el tradicional sistema de correo[65].

La denominada Ley de Delitos Informáticos incorpora la "comunicación electrónica" a la categoría de correspondencia, por lo que un ataque a la misma, ahora es tipificado y penado.

Se ha dicho también, que "indebidamente" viene a abonar el hecho que este delito se trata de un delito doloso, es decir de aquel que se cometió conociendo lo que se hacía y buscando el fin lesivo. Con ello quien no tenía la finalidad de interceptar o captar un e-mail, sino simplemente filtrar spam, o que lo ha hecho por descuido o error, no habría actuado dolosamente.

Por otro lado, la mencionada reforma al Código Penal, al sustituir el art. 155, castiga al que publicare indebidamente una correspondencia privada, comunicación electrónica, etc.. Esto es concordante con lo mencionado precedentemente en cuanto a la asimilación de los conceptos de correspondencia tradicional y comunicación electrónica, agregándose este último al tipo delictivo existente[66].

a.4. ¿Cuáles son los delitos informáticos que se pueden cometer por Facebook?

Recordemos que la nueva normativa tipifica como delitos la violación, apoderamiento y desvió de comunicación electrónica y la publicación de una comunicación electrónica.

Está claro que las comunicaciones que realizan los usuarios de Facebook, Twitter, My Space u otras redes sociales, encuadran perfectamente en el concepto de comunicación electrónica. Es importante tener en cuenta que cuando las comunicaciones están abierta al público en general quien accede a ellas no cometerá el delito en cuestión, sin perjuicio que el empleo que posteriormente haga de esa información puede configurar otro delito.

[65] Fundamento Proyecto de Ley Expediente N° 2981-D-2006. Trámite Parlamentario 63 (2/6/2006)

Es importante tener en cuenta esto a los efectos de determinar qué comunicaciones se quieren hacer públicas y cuáles no, previo publicar información en alguna de las redes sociales.

a.5. Delito ubicuo[67]

Es de destacar que el delito en estudio y la mayoría de los delitos informáticos, presentan la complejidad de ser llevados a cabo por personas de un país diferente del de las computadoras zombie que se utilizaron para perpetrar el delito e incluso afectan usuarios que residen en un tercero. Frente a este escenario ¿cómo actúa la ley? “A nivel derecho-explica el profesor Ricardo Saenz-, se puede decir que cualquiera de los jueces del lugar donde se manifiesta mucha colaboración internacional”.

Carla Delle Done señaló que “no habría una jurisdicción exclusiva, porque el delito se consuma en distinto lugares. Si bien se produce en diversas etapas, cada una de ellas se puede identificar como un delito independiente”. Actualmente, no existe ningún tratado de cooperación en materia penal que regule este tema. Sí se trabaja a través de notificaciones de la Interpol gracias a las que, por ejemplo, en España, se inició una investigación y se pudo averiguar que una dirección de IP que se utilizó corresponde a la de un usuario en la Argentina.

Según Sáenz, “en la práctica puede funcionar que sea competente el juez que esté en mejores condiciones de investigarlo, porque tiene pruebas más fáciles o porque tiene al imputado más a mano”. Este es el criterio que se utiliza en la Corte suprema Argentina. “Se llama Teoría de la Ubicuidad-aclaró Sáenz-, o sea que el delito se considera cometido en cualquiera de los lugares donde tuvo algún tramo, y en definitiva se va a considerar competente al que esté en mejores condiciones de investigarlo, o que asegure el derecho de defensa de los imputados o asegure la prueba. Esto es algo muy dinámico, muy cambiante y donde queda casi todo por hacer”, concluyó.

a.6 ¿Qué hacer si se ha sido víctima de un delito informático?

Es necesario aclarar que, si se ha sido víctima de un delito informático y se quiere denunciar, las formalidades no existen.

[67] www.catarina.udlap.mx/u_dl_a/tables/documentos/lfis/trillo_m_p/capitulo4.pdf

Si lo hace por escrito, el texto debe contener una descripción de los hechos, lo más precisa posible, indicando la prueba que posee y si sabe quién es la persona que lo realizó.

En cuanto a las Cuestiones Probatorias: Lo primero y más urgente que deberá hacer es juntar la prueba acudiendo a un informático junto a un notario o escribano y levantar un acta notarial. También imprimir copias de todo y guardarlo notarizando el contenido. Recuerde que todo lo que está en Internet se puede borrar en segundos y dejará de ser prueba para su caso. La mayoría de los delitos informáticos no tienen condena por falta de pruebas[68].

a.7. Situación del filtrado automático de comunicaciones[69]

Con la aclaración de que el desvió de correo electrónico es una figura exclusivamente dolosa, quedarían salvadas las objeciones de ciertos medios empresarios que abrigaban el temor de que ésta reforma fuera aplicada a acciones de un proveedor de acceso a Internet o de servicios a mail, que son muy comunes. Con frecuencia, para mejorar el servicio o por cuestiones técnicas, los proveedores proceden a desviar o filtrar un correo electrónico porque contiene un virus o porque un algoritmo o filtro lo clasifica como spam. Incluso algunas rutinas que funcionan en sistemas de webmail pueden detectar casos de phishing, cuya única finalidad es el robo de identidad. No es el objeto de la nueva figura prevista en el art. 153 del C. P., el penalizar tales situaciones[70].

Estas acciones se han incrementado en los últimos años, motivas, en parte, por el deseo de frenar actividades ilegales como el intercambio de obras intelectuales (generalmente música y películas) a través de redes p2p, el phishing, y más recientemente la pornografía infantil.

Por ejemplo, Yahoo y Google utilizan tecnologías de autenticidad llamada Domaninkeys para verificar el dominio del remitente del correo. Permite validar el origen del correo electrónico y detectar casos de phishing y amparar así a usuarios de eBays y Paypal. No hace falta mucha discusión para comprender la

[68] http://www.delitosinformaticos.com.ar/blog/como-denunciar-un-delito-informatico/
[69] PALAZZI, Pablo, ob. Cit. p. 84
[70] Cada tanto recibo un correo electrónico no solicitado (*spam*): eso no es delito, pero puede dar lugar a sanciones administrativas y civiles. http://www.delitosinformaticos.com.ar/blog/%c2%bfque-es-un-delito-informatico/

importancia de que los ISP pueden establecer estas tecnologías libremente, pues están destinadas, en último término, a amparar al usuario y a crear un internet más seguro.

Los ISPs argumentan que no leen el "contenido" de la comunicación, sino solamente los paquetes (a través de los datos de tráfico) con la finalidad de darle el destino correcto. Si no como intermediarios en la comunicación entre usuarios deben leer los paquetes para "rutearlos" en internet, la decisión de "retrasar" algunos o ponerlos en una "cola" haciendo más lenta la conexión no debería constituir un hecho con significancia penal.

En todos estos supuestos existe un desvió de comunicaciones electrónicas cuyo fundamento es la protección de los titulares de ellas, de la red o de la empresa proveedora del servicio.

Bajo la ley vigente, entendemos que nunca podría llegarse a tal resultado interpretativo por la carencia de dolo en tal accionar. Hay que recordar que el término "indebido", presente en el art. 153 del C. P., es, asimismo, sinónimo de realizado "sin derecho". En tal sentido, un ISP o proveedor de servicio de correo está en su derecho, según los términos y condiciones de uso que fijen para la prestación del servicio, de desviar o "etiquetar" correspondencia no solicitada (spam) que es ilegal en la Argentina[71], o suprimir

[71] Medida Cautelar concedida. Abstenerse de enviar SPAM contra los actores Dres.Taunus y Palazzi. Fecha:11/11/03. El 11 de noviembre de 2003 el Juez a cargo del Juzgado Civil y Comercial Federal Nº 3, Secretaría Nº 6 de la Capital Federal, Dr. Roberto Torti dictó la primera medida cautelar en un caso de SPAM. En esa decisión el juez dispuso que los demandados deben abstenerse de seguir enviando correos electrónicos a los actores mientras dure el litigio. Además de prohibir que los demandados envien mensajes de correo electrónico a las casillas de los actores, la medida cautelar dispone que también deberán abstenerse de "transferir o ceder a terceros las direcciones de correo electrónico u otro dato personal vinculado a ellos (arts. 1, 2, 5, 11 y 27 de la Ley 25.326 de Protección de Datos Personales), hasta tanto se resuelva el fondo de la cuestión. El caso se inició en febrero de este año cuando Gustavo Daniel Tanús y Pablo Andrés Palazzi, especialistas en derecho informático y privacidad, decidieron recurrir a la justicia luego que el demandado hiciera caso omiso a sus pedidos de que no les enviara más mensajes de correo electrónico con publicidad no solicitada (el demandado vende bases de datos en violación a la Ley citada y se anuncia enviando mensajes de correo electrónico a través de Internet). Fue así como se inició el expediente que terminó tramitando ante la Justicia Federal luego de una contienda negativa de competencia entre la Justicia Nacional en lo Comercial y la Justicia Federal de la Capital. En la demanda, Tanús y Palazzi acompañaron copias de los mensajes de correo electrónicos recibidos, que contenian direcciones a las que supuestamente podían solicitar ser removidos de la lista de distribución, pero que nunca funcionaron, y de los que ellos enviaban ejerciendo los derechos reconocidos por la Ley de Protección de Datos. El demandado es una persona que se dedica a la venta de bases de datos, muchas de las cuales contienen millones de datos personales de individuos que no han dado su consentimiento para el tratamiento de su información. La ley argentina en forma específica regula las comunicaciones de marketing y en su art. 27 establece que los que reciban este tipo de comunicaciones tienen derecho a acceder a los datos personales y a solicitar ser removidos de la

aquella que constituya una amenaza para la seguridad de su red o la de los usuarios si contiene virus o algún programa potencialmente dañino. Son conductas, entonces, que no son antijurídicas porque se realizan de conformidad con el marco legal que rige la prestación del servicio.

Esta postura se ve corroborada por dos antecedentes legislativos, primero el dictamen del Senado, que fundamenta así las conclusiones que venimos señalando, "con respecto al actual art. 153 del C. P., última parte del primer párrafo, es razonable la propuesta de la Cámara de origen de incorporar no solo la comunicación electrónica sino también la expresión "indebidamente" en el tipo, para que no le queden dudas al intérprete respecto a requerir la finalidad dolosa del autor del delito, y evitar cualquier hermenéutica tendiente a considerar comprendidos en el tipo a quienes en procura de mejorar el servicio que prestan a sus usuarios, activan mecanismos de protección para evitar lo se conoce como spam, o la recepción de correos no deseados por sus clientes[72].

Segundo, la exposición del miembro informante en la Cámara Alta Vilma Ibarra, que durante el debate de la norma en el recinto señaló: "Acá hay que dejar algo en claro para la interpretación ulterior de los jueces en materia de interpretación auténtica, a efectos de que no quede duda a quienes interpretan la ley de que la finalidad debe ser dolosa…Muchas veces, las empresas colocan filtros y desvían el spam, y esto no

---

base de datos (art. 27 ley 25.326). Si no lo hacen, al afectado le queda la posibilidad de iniciar una acción de habeas data.
En materia legislativa, la Secretaría de Comunicaciones había elaborado un anteproyecto que contenía fuertes sanciones de multa para aquellos que practicaran spam, pero el proyecto nunca obtuvo estado legislativo. En la actualidad, se encuentran en trámite en el Congreso dos proyectos de Ley que pretenden regular el correo electrónico no solicitado, conocido mundialmente como SPAM, aunque se desconoce en qué estado se encuentran dichos trámites. El problema del spam -que este año llego a constituir la mitad del correo electrónico que circula por la red-, es que hace recaer los costos de la publicidad en quien recibe el mensaje (los usuarios de Internet) y no en quien lo envia. A ello se suma el perjuicio que le causa a los proveedores de servicio de Internet que tienen que procesarlos y la que los filtros o programas para detenerlo no son 100% efectivos. Texto del Fallo. Buenos Aires, 11 de noviembre de 2003. Agréguese, y en atención a lo solicitado, documentación acompañada y el derecho a la protección integral de los datos personales, garantizado por la ley 25.326, dispónese que los aquí demandados se abstengan de seguir enviando mensajes de correo electrónico a las casillas de los actores y de transferir o ceder a terceros las direcciones de correo electrónico u otro dato personal vinculado a ellos (arts. 1, 2, 5, 11 y 27 de la ley citada), hasta tanto se resuelva el fondo de la cuestión. Notifíquese. A fin de dar cumplimiento a lo previsto por el art. 39 de la ley 25.326, córrase traslado a las demandadas por el plazo de cinco días, debiendo aportar la documentación pertinente. Notifíquese. Téngase presente la prueba ofrecida y la reserva del caso federal planteado. Fdo. Roberto Raúl Torti. Juez Federal.

[72] CAMARA DE SENADORES, Orden del Día N° 959/2007 (16/11/2007)

constituye la vocación de suprimirle para causarle un daño al otro. Entonces, esto lo dejamos claramente especificado, o sea la expresión “indebidamente” excluye, desde ya, la actividad empresarial para el desvió de spam”.

La voluntad del legislador es clara en cuanto a excluir de las conductas típicas a estos supuestos: no incurre en delito el proveedor que desvía un mail porque no es un correo electrónico no solicitado o porque contiene un virus.

El problema interpretativo surge porque en Argentina no existe una ley de privacidad de las telecomunicaciones actualizadas, como la que rige en otros países, y se carece de excepciones razonables como las relativas al mantenimiento por parte de empleados de la empresa prestadora del servicio, la reparación de redes, cuestiones comerciales o de monitoreo de la red por parte de sus propietarios con la finalidad de mejorar la seguridad, calidad o eficiencia de ésta. La ley de Telecomunicaciones (19.798), dispone que: “Art. 17**.** — No se cursará telecomunicación alguna que pueda afectar la seguridad nacional, las relaciones internacionales, la vida normal de la sociedad y sus instituciones, la moral y las buenas costumbres. Art. 18. — La correspondencia de telecomunicaciones es inviolable. Su interceptación solo procederá a requerimiento de juez competente. Art. 19**.** — La inviolabilidad de la correspondencia de telecomunicaciones importa la prohibición de abrir, sustraer, interceptar, interferir, cambiar su texto, desviar su curso, publicar, usar, tratar de conocer o facilitar que otra persona que no sea su destinatario conozca la existencia o el contenido de cualquier comunicación confiada a los prestadores del servicio y la de dar ocasión de cometer tales actos. Art. 20**.** — Las personas afectadas a los servicios de telecomunicaciones están obligadas a guardar secreto respecto de la existencia y contenido de la correspondencia, de que tengan conocimiento en razón de su cargo. Art. 21**.** — Toda persona que de cualquier manera tenga conocimiento de la existencia o contenido de la correspondencia de telecomunicaciones, está obligada a guardar secreto sobre la misma con las excepciones que fija la presente ley.”[73]

Estas normas, cuestionan la posibilidad de que un empleado de un ISP o de cualquier empresa puede revisar el correo electrónico, o más bien el flujo de tráfico que circula a través de su red, cualquiera sea su contenido y clase de

[73] http://www.infoleg.gov.ar/infolegInternet/anexos/30000-34999/31922/texact.htm

comunicación, desde un correo electrónico, hasta logs de conexión a un sitio web, pasando por paquetes de voz IP, o de conexiones en redes *peer to peer*[74].

Otro motivo por el cual se monitorea el tráfico en redes informáticos es para combatir la pornografía infantil. En el mes de junio de 2008, varios ISP de Estados Unidos se aliaron para bloquear de oficio el acceso a pornografía infantil y bajar la distribución de esos contenidos, aunque la decisión fue criticada[75].

Otro motivo, muy loable, por cierto, es el disminuir o controlar la "bajada" de obras intelectuales amparadas por leyes de propiedad intelectual[76].

---

[74]El 21 de enero de 2003, en el caso de RIAA vs. Verizon, una corte del distrito determinó que los titulares de derechos de autor podían obtener órdenes o citaciones para exigir a los proveedores de servicios en Internet (ISPs) revelar la identidad de sus clientes que hayan infringido derechos de autor, a través de sistemas de intercambio P2P. Cabe destacar que no todas las cortes coinciden en que la RIAA pueda enviar solicitudes a los ISP con este fin. También se pone en juego otra paradoja, ya que algunos sostienen que descargar música no es ilegal, y que lo ilegal es compartirla. http://www.hfernandezdelpech.com.ar/PUBLICAtrabajosDerechoAutorBajadaMusica.htm

[75] GROOMING: ACOSO INFANTIL A TRAVÉS DE LA RED. La operación "Lobos" llevada a cabo por la Brigada de Investigación Tecnológica de la Policía Nacional (BIT) en colaboración con las jefaturas de policía de casi todas las provincias españolas y los juzgados, se ha saldado con la detención de 78 personas por tenencia y distribución de pornografía infantil. La investigación se inició con la denuncia recibida por la BIT respecto a una web llamada Paisajes Lunares, en la que, presuntamente, tras visualizar algunas fotografías coincidentes con el tema de la página, podía accederse a pornografía infantil. Una de las prácticas más habituales últimamente en la red es la extorsión y chantaje a menores, curiosamente, cometidas también en gran número por menores de edad.. http://www.delitosinformaticos.com/06/2008/delitos/34/grooming-acoso-infantil-a-traves-de-la-red

[76] LA PROTECCIÓN DE LOS DERECHOS DE AUTOR – COPYRIGHT. Los derechos de autor describen los derechos concedidos a los creadores de obras literarias o artísticas. Es así que cuando un individuo crea una obra musical, literaria, científica o artística, se convierte en titular de esa obra y es libre de decidir acerca de su uso. Los derechos conexos son los que se otorgan a los titulares que entran en la categoría de intermediarios en la producción, grabación o difusión de las obras. Su conexión con el derecho de autor radica en que las tres categorías de titulares de derechos conexos intervienen en el proceso de creación intelectual dado que prestan a los autores asistencia en la divulgación de sus obras al público. La protección de los Derechos de Autor en la sociedad de la Información, es un problema jurídico que ha adquirido mayor relevancia, especialmente debido a la aceleración de los avances tecnológicos y nuevos modelos de distribución, consumo de información y contenidos, con especial repercusión en el marco de los fonogramas y el intercambio de los mismos gracias a Internet y al correo electrónico. El nacimiento de nuevas tecnologías ha posibilitado el intercambio de archivos musicales a terceros que no poseen esos derechos ni tampoco cuentan con la debida autorización de sus autores, compositores y/o productores discográficos para su difusión, lo cual constituye un ilícito. El impacto de este acto delictivo no se limita a la mera pérdida de ganancia sobre esa obra difundida, sino que daña en forma irreversible a la propia industria, desalentando a todos los involucrados en el proceso de producción y difusión (compositores, interpretes, discográficas y productores), y por consiguiente se generan grandes pérdidas de empleos y oportunidades para nuevos artistas. La descarga o intercambio de música en Internet en sí, no constituye un acto ilegal si quién publica el fonograma es poseedor de los derechos de propiedad intelectual sobre la obra. En la actualidad, es un hecho habitual la reproducción, distribución y comunicación al público de creaciones intelectuales sin el correspondiente

Pese a estas actuales tendencias, desde el punto de vista del derecho penal argentino, ninguno de esos motivos está receptado como una excepción válida para revisar las comunicaciones electrónicas. A menos que se cuente con una orden de juez, o el consentimiento del usuario, o exista otro marco legal en el cual dichas interceptaciones estén autorizadas (por ejemplo, los motivos señalados en el art. 34 del C. P., un juez podría concluir que resulta aplicable el art. 153 del C. P., en ciertas situaciones. Obviamente, como ya se explicó, esa no fue la intención del legislador.

a.8 ¿Es delito acceder al correo electrónico del trabajador?

La penalización del acceso indebido al correo electrónico reavivó la polémica sobre monitoreo en el ámbito laboral[77]. Existen diversas justificaciones por las cuales una empresa podría tener interés en revisar correos electrónicos de sus empleados: entre otros señalamos ejercer el derecho de propiedad sobre herramientas de trabajo, monitorear el rendimiento de los asalariados, cumplir con obligaciones de recopilar ciertos datos, derecho de preservar un medio ambiente libre de molestias del resto de los trabajadores, y la seguridad informática interna de la red de la empresa.

En doctrina existen diferencias acerca de cuáles son los límites legales vigentes. Para un sector mayoritario, (cuya opinión comparte el Dr. Pablo Palazzi) es posible que el empleador revise los correos electrónicos del trabajador si se trata de corporativo y se hace dentro del reglamento de la empresa[78]. Para otro sector

consentimiento de la persona autora de las mismas y por tanto, sin su correspondiente contraprestación económica.
http://www.hfernandezdelpech.com.ar/PUBLICAtrabajosDerechoAutorBajadaMusica.htm

[77] PALAZZI, Pablo, ob. Cit. p. 91

[78] CIUDAD DE BUENOS AIRES (Urgente24). Mediante la Resolución 464/2010, el ministro de Economía y precandidato a Jefe de Gobierno porteño, Amado Boudou, reguló el uso de Internet y de las herramientas laborales informáticas en el ámbito del Palacio de Hacienda según la cual se permite controlar los mails enviados por los empleados de esa cartera. Semejante decisión le valió una denuncia del diputado y candidato a gobernador bonaerense, Juan Carlos Morán (Coalición Cívica – Buenos Aires), ante la Justicia Federal por abuso de autoridad, violación de deberes de funcionario público y violación de secretos y de la privacidad. *"La justicia laboral entiende que es una facultad del empleador controlar el contenido de los correos electrónicos y de los archivos de los ordenadores que provee a fin de que el empleado pueda desarrollar sus tareas laborales",* consigna el texto elaborado y según consigna Diario Judicial. El escrito marca la diferencia entre el mail laboral y el personal ya que para el segundo para realizar cualquier tipo de control *"será imprescindible en todos los casos la orden judicial que así lo autorice".* Mientras que, en el mail corporativo *"lógico resulta que el empleador, insistimos, en el ámbito público y en el privado, quiera proteger sus intereses frente al uso indebido de Internet así como de las demás herramientas informáticas, y que para ello estime necesario monitorear la productividad de sus empleados".* No obstante, en el dictamen, los fiscales consideraron *"esencial"* el conocimiento del trabajador de *"las políticas de*

doctrinario más reducido, la revisión no puede tener lugar, salvo cuando el trabajador ha prestado su consentimiento. Algunos incluso vas más lejos y exigen que este consentimiento conste por escrito.

Dentro de la jurisprudencia cabe señalar, que sus numerosas decisiones judiciales, previa a la ley 26.388, habían aceptado la posibilidad de que el empleador revisara el correo (dada la época, se trataba de cartas epistolares) recibido en la empresa.

En el ámbito penal, la jurisprudencia consideró ilegal la obtención de correo electrónico sin orden del juez. En varias decisiones judiciales se anuló la prueba de correo obtenida dentro del ámbito laboral[79].

Hasta el presente, las cuestiones relacionadas con la intimidad personal en los lugares de trabajo no han generado mayores conflictos y los pocos supuestos que se conocen están más vinculados a abusos de poder que propiamente a la develación de la vida privada.

Con todo, ya hace aproximadamente tres décadas y en los albores del moderno desarrollo del derecho a la intimidad, Krotoschin plantea la protección de la personalidad moral del trabajador frente a las nuevas tecnologías de supervisión. Desde aquel entonces hasta el presente se ha producido un avance notable en el desarrollo de las tecnologías de monitoreo laboral.

---

privacidad o de las reglas de uso de Internet y del correo electrónico antes del comienzo de la relación laboral, conocimiento que debe notificarse por escrito mediante un acuerdo celebrado entre las partes". Asimismo se agrega: *"La expectativa del empleador de que las herramientas laborales se utilizarán para fines estrictamente vinculados al giro laboral justifica que, siempre que el empleado conozca las reglas de uso de Internet y del correo electrónico laboral y haya prestado formalmente su consentimiento, el empleador pueda realizar los controles que estime necesarios en el momento que considere oportuno".* Sin embargo destacaron que, al mismo tiempo, *"los empleados están protegidos por el derecho a no ser sometidos a injerencias arbitrarias en su ámbito de trabajo que involucren una afectación a su derecho a la intimidad".* Aunque precisaron que *"las computadoras y la dirección de correo electrónico suministrada por el empleador son de su propiedad y es, precisamente, por esa razón que cuenta con facultades de control".* No todo fue avalado totalmente en el informe realizado por los fiscales, puesto que otro de los puntos a lo que refiere la resolución es la prohibición de usar el mail personal en el ámbito del Ministerio. Recomendaron "e*l análisis de la razonabilidad de ese punto en particular a fin de determinar la existencia de un exceso en las facultades de reglamentación del uso de Internet y de las herramientas laborales informáticas por la vía administrativa pertinente".* h*ttp://www.delitosinformaticos.com.ar/blog/*

[79] Caso "Redruello" (C. Nac. Crim y Corr, sala 4°, 15/11/2004, JA 2005-II-661.

Los controles de acceso y desplazamiento por lectores ópticos, el video monitoreo, la lectura automatizada de los contenidos de las computadoras, la intercepción de los correos electrónicos y la obtención de extensa información personal, son algunas de las tecnologías que están modificando los lugares de trabajo. Sin perjuicio de analizar la incidencia, en la vida personal del trabajador, de determinadas tecnologías, en este momento de acelerado cambio tecnológico hay que poner de relieve los tradicionales principios generales, que son los que mejor permiten resolver las nuevas situaciones producidas por los cambios tecnológicos.

La innovación científica puede modificar las formas de supervisión, pero no debe alterar los derechos cuya elaboración y vigencia no dependen, en principio, de medios mecánicos, sino de una concepción de valores que en mucho trasciende el uso de instrumentos técnicos.

En el ámbito laboral está presente tanto del derecho del empleador a ejercer industria lícita, como el derecho que, como persona, le corresponde a todo trabajador.

En el análisis de la privacidad en los lugares de trabajo, la principal tarea es la armonización de los derechos del empleador con los derechos del trabajador.

Por reconocimiento expreso de nuestra Constitución Nacional, el empleador tiene el derecho a ejercer industria lícita y consecuentemente la facultad de organizar su empresa de acuerdo a sus propios criterios personales.

El derecho del empleador está además reglamentado en los artículos 64 y 65 de la ley de contrato de trabajo.

No debe pues quedar duda sobre el derecho legítimo que tiene el empleador a utilizar nuevas tecnologías para controlar la diligencia y probidad laboral. Desde ya que el derecho del empleador no es absoluto y que al igual que todos los derechos requiere un ejercicio funcional.

A su vez, el trabajador, por la circunstancia del empleo no deja de ser persona y por consiguiente goza de todos los atributos de la personalidad reconocidos universalmente en los diversos tratados sobre los derechos del hombre, que

además han sido incorporados a la Constitución Nacional por la reforma del año 1994 y antes de ello por las declaraciones de derechos y garantías de la primera parte de la Constitución de 1853.

Además de la protección constitucional, el trabajador se encuentra protegido en su intimidad por el artículo 1071 bis del Código Civil y por los artículos 62, 65, 66, 68, 73 y 75 de la L.C.T..

De la ponderación de los derechos del empleador y del trabajador se puede explicitar criterios que hacen a la protección de la intimidad en el ámbito laboral.

a) El grado de intromisión

En los supuestos que el grado de intromisión sea mínimo, la necesidad de su justificación disminuye e inversamente, mecanismos altamente intrusivos son de muy difícil legitimación. Controles moderados de vestimenta y de aspecto físico para vendedores o empleados de empresas de servicios no parecen requerir de extensa justificación, en cambio testeos de personalidad y análisis psicológicos sólo serían legítimos en ocupaciones de alto riesgo (personal armado, bomberos, pilotos de aeronaves, etc.). El grado de intromisión no puede resultar de la sensibilidad individual de las partes involucradas y debe provenir de los criterios generales vigentes en la comunidad (art. 909, Código Civil).

b) Los controles no deben ser subrepticios, ocultos o sin conocimiento fehaciente del trabajador.

El trabajador debe tener pleno conocimiento de que es monitoreado a fin de que pueda proteger su intimidad cuidando sus expresiones, y conductas para no exponer situaciones personales íntimas. No es permitido "espiar" al trabajador y el anteproyecto de correo electrónico condiciona la legitimidad de la intercepción de los *e-mails* laborales a la previa notificación del trabajador. El control invisible además de violar la privacidad del trabajador, constituye un ejercicio anti funcional del derecho de monitoreo del empleador y vulnera la regla de la buena fe contractual.

c) El control debe referirse exclusivamente a aspectos relacionados con el trabajo.

El basamento del ejercicio del derecho del empleador es el control de la productividad de la empresa y resulta evidente que salvo supuestos especiales lo ajeno a lo laboral no puede legitimar la función de control.

Livellara[80] expresa que dentro del obrar genérico de buena fe (art. 62, 63, LCT) y por respeto a la privacidad del trabajador, se considera que el empleador debe requerir sólo la información que sea necesaria y relacionada con la función a cumplir. Si en la rutina de control aparecen involuntariamente aspectos íntimos del trabajador, estos deben ser eliminados del control y no tomados en cuenta.

d) El empleador debe justificar la concreta necesidad del medio empleado a tal fin de responder a una identificada exigencia productiva.

No son suficientes consideraciones genéricas de beneficios o mejoras para justificar la reducción del ámbito de privacidad de los trabajadores. El Tribunal Constitucional de España estableció que la mera utilidad o conveniencia para la empresa no justifica sin más la instalación de aparatos de audición y grabación y que la modulación del derecho a la intimidad del trabajador sólo se produce en la medida estrictamente imprescindible para el correcto desenvolvimiento de la actividad productiva.

e) El medio de monitoreo, siendo eficaz y proporcionado al fin empresario, debe ser entre todas las alternativas posibles el menos invasivo a la privacidad del trabajador.

Es sabido que la obtención del control empresario presenta tanto alternativas de medios como de modos, así por ejemplo contralores al azar de los correos electrónicos de los trabajadores son por lo general suficientes para la función empresaria, en cuyo supuesto un control total de toda la correspondencia electrónica no tendría en principio justificación ya que el fin empresario puede obtenerse de un modo menos invasivo.

El Tribunal Constitucional Español en pronunciamiento ya mencionado expresó que las limitaciones tienen que ser las estrictamente necesarias, de manera que si existe posibilidad de satisfacer el interés empresarial por medios menos

[80] LIVELLARA, Carlos A., La Reforma Constitucional de 1994 y el derecho a la intimidad del trabajador, La Ley, V.J., 1998-2-204;

agresivos es necesario emplear las de menos afectación por cuanto se trata de la aplicación del principio de la proporcionalidad.

Este autor considera como “Criterios de escasa relevancia”

-Consentimiento del trabajador

-Lugar de monitoreo

Consideramos que en lo que se refiere a la intimidad del trabajador, tanto el consentimiento como el lugar en que se realiza el monitoreo, no son factores a ser tenidos en cuenta para resolver sobre la legitimidad de una intromisión en la privacidad del trabajador. Sabido es que, en materia de intimidad, el consentimiento constituye una de las causas más frecuentes de exclusión de ilicitud, tal es así, que la publicación de las situaciones más íntimas no constituye violación a la intimidad cuando existe autorización de la persona cuya intimidad se expone. Sin embargo, en materia laboral el consentimiento del trabajador no puede ser considerado como vinculante en la renuncia de los derechos (Art. 12 LCT) de tal modo que el consentimiento, sea este tácito o expreso, no debe ser tomado en cuenta para resolver sobre la licitud de la restricción a la privacidad del trabajador.

El segundo aspecto que nos parece irrelevante es el lugar o zona de monitoreo. En materia de intimidad, sobre todo en la doctrina proveniente de Estados Unidos, se considera que la protección de la intimidad sólo se produce cuando se develan actividades privadas ocurridas en lugares privados.

El Tribunal Constitucional Español, en el caso ya mencionado, estableció que no corresponde limitar el alcance del derecho a la intimidad de los trabajadores a las zonas del centro de trabajo donde no se desempeñen los cometidos propios de la actividad profesional (-vestuarios, lavabos, etc.-) dado que pueden producirse intromisiones ilegítimas dentro del ámbito de desempeño de la tarea profesional. Al ser la intimidad un atributo de la personalidad, no se concibe que la misma tenga límites geográficos y a lo sumo podría presumirse que quien se exhibe en público podría estar configurando una renuncia tácita, pero por cierto este no es el supuesto del trabajador cuando se desplaza por áreas laborales.

En síntesis, no es el lugar, sino la persona, lo que protege el derecho a la intimidad.

La intimidad del trabajador frente a los accesos del empleador a los "e mails" remitidos y recibidos en el ámbito laboral.

A partir de la creación de la computadora personal y de la desaparición de los clásicos centros de cómputos, la integración de los servicios telefónicos con la informática ha puesto a disposición de los trabajadores, terminales autónomas que permiten la comunicación electrónica.

Por cierto, que la puesta a disposición de computadoras personales con capacidad de comunicación externa, lo es a fin de lograr resultados empresarios y no con el propósito de atender un uso personal del trabajador.

Pero más allá del objetivo empresario, no puede negarse que es una realidad, que existe cierto grado de uso personal de las computadoras como medio de expansión personal. Remitir y recibir bromas, visitar alguna página web, enviar mensajes, son distracciones que realizadas con prudencia contribuyen al clima de trabajo.

Quienes propugnan un amplio derecho de auditoria empresaria sobre los *e mails* recibidos en los servidores de la empresa, justifican la legitimidad del monitoreo sobre la base de las siguientes argumentaciones:

-Que la empresa es la propietaria o legítima usuaria de los servidores.

-Que la puesta de disponibilidad de las computadoras y de la facilidad de correo electrónico es con el fin de realizar una actividad productiva.

-Que a través del uso de correo electrónico se pueden producir supuestos de responsabilidad refleja para la empresa.

-Que a través de la remisión de los *e mails* se aumentan las posibilidades de introducir virus y *cookies.*

-Que por sus características el correo electrónico facilita la fuga de información confidencial.

-Que, en razón de su configuración, no existe una razonable expectativa de privacidad en el correo electrónico.

A su vez, quienes consideran que el acceso por el empleador a los *e mails* de los empleadores constituye una invasión a la esfera de privacidad del trabajador argumentan:

-Que la comunicación es uno de los ámbitos que hacen a la realización de la persona mediante el intercambio de pensamiento y la intromisión se traduce en una de las fracturas más graves del ámbito de libertad y privacidad.
-Que el correo electrónico tiene suficientes similitudes como para asimilarlo al correo postal y que en general y a todos los efectos se acepta esta asimilación.
-Que en el correo electrónico se utilizan claves personales de elección y uso exclusivo de cada trabajador.

-Que para realizar controles de diligencia y probidad no es necesaria la lectura de los *e mails* y que existen otros medios sin necesidad de la lectura de los mensajes personales.

De la evaluación de las argumentaciones antes expuestas y de los principios generales podría construirse alguna línea tentativa de solución al conflicto, en lo que se refiere a la auditación de correos electrónicos.

Conforme a las pautas generales estamos ante un supuesto de elevado grado de intromisión, por ende, la justificación empresaria debe ser considerada con criterio estricto, respondiendo a una expresa necesidad y acreditando que no existen otras alternativas de control menos invasivas.

Nos parece que la auditación o no de los *e mails* de los empleados, no pueden resolverse en términos absolutos (todos o ninguno) y que es preciso considerar cada supuesto en forma particularizada, aceptando el control donde se produzca una verdadera necesidad y rechazando el mismo, cuando no hay una justificación imperiosa[81].

[81] http://www.losrecursoshumanos.com/contenidos/325-el-derecho-a-la-intimidad-en-el-ambito-laboral.html

A nivel legislativo[82] podemos mencionar que en Congreso Nacional se encuentra en trámite de aprobación, del Proyecto de Ley de Incorporación del Art. 86 bis de Regulación del correo electrónico laboral a la Ley 20.744 de Contrato de Trabajo, cuyos fundamentos se transcriben a continuación: “Señor presidente: El presente proyecto tiene por finalidad incorporar a la legislación argentina la regulación del correo electrónico o e-mail en la relación laboral.

La evolución tecnológica constante en la que nos vemos inmersos y el gran desarrollo que ha alcanzado la informática en general, Internet y el correo electrónico en particular, hacen necesario que la legislación contemple nuevas situaciones, y más específicamente la legislación laboral.

El correo electrónico presenta una de estas situaciones que merecen ser receptadas en nuestra normativa.

Cada día es mayor la correspondencia que se trasmite en el país originada y transportada por medios informáticos, es decir que la correspondencia postal tradicional está dando paso a la utilización masiva de un nuevo medio de comunicación, cual es el e-mail.

---

[82] PROYECTO DE LEY DE INCORPORACION DEL ART. 86 BIS DE REGULACION DEL CORREO ELECTRONICO LABORAL A LA LEY 20.744 DE CONTRATO DE TRABAJO.
Exp: 0623-D-2007
Firmantes: BISUTTI, Delia Beatriz - GARCIA, Susana Rosa - QUIROZ, Elsa Siria - GORBACZ, Leonardo Ariel - RIOS, Maria Fabiana.
El Senado y la Cámara de Diputados,
Artículo 1°.- Incorporase el Artículo 86 bis a la Ley 20.744, Ley de Contrato de Trabajo, el que quedará redactado de la siguiente manera: Artículo 86 bis.- Correo electrónico laboral.- "Cuando el correo electrónico sea provisto por el empleador al trabajador en función o con motivo de una relación laboral, se entenderá que la titularidad del mismo corresponde al empleador siempre y en todos los casos, independientemente del nombre y clave de acceso que sean necesarias para su uso.
El empleador se encuentra facultado para acceder y controlar toda la información que circule por dicho correo electrónico laboral, como asimismo a prohibir su uso para fines personales.
El empleador no podrá prohibir el uso de las direcciones de correo electrónico que pudiera tener el trabajador que sean de carácter personal o privado, aunque los mismos sean abiertos desde el lugar de trabajo.
El empleador deberá asimismo, notificar fehacientemente al empleado su política respecto del acceso y uso de correo electrónico personal en el lugar de trabajo, así como las condiciones de uso y acceso al correo electrónico laboral al momento de poner a su disposición el mismo.
En caso de que la dirección de correo electrónico laboral se conforme con el nombre o parte del nombre del trabajador, una vez finalizada por cualquier causa la relación laboral, el empleador deberá, en un plazo no mayor de 24 horas, eliminar esa dirección de correo electrónico".
Artículo 2°.- Comuníquese al Poder Ejecutivo.-

Creemos que, sin importar el soporte técnico en el que en uno y otro caso (correo electrónico y correo postal) se transmite el mensaje, el derecho a la privacidad de la correspondencia, reconocido constitucional y penalmente, debe ser resguardado, por ser este derecho un elemento clave de la vida en democracia.

A los fines entonces, de la garantía constitucional de inviolabilidad, contemplada en el artículo 18 de la Ley Fundamental, se equiparán ambas modalidades de transmisión de comunicaciones.

Asimismo, esta equiparación fue recientemente reconocida también por esta Honorable Cámara, cuando aprobó el proyecto que trata sobre los "Delitos contra la Privacidad", por el cual en su artículo 3º se equipara expresamente la correspondencia epistolar con la de telecomunicaciones. Lo mismo sucede cuando en ese proyecto se modifica los artículos 153 y 155 del Código Penal de la Nación, equiparando una comunicación electrónica con una carta, un pliego cerrado o un despacho telegráfico.

Sin embargo, tal equiparación reconoce una excepción, en tanto el e-mail tenga como base una relación laboral. Ello es así puesto que consideramos que las nuevas tecnologías deben integrarse a la relación laboral, verificando que su utilización no producirá consecuencias disvaliosas, tanto para el trabajador como para el empleador.

Partiendo de esta premisa, y considerando que el contrato de trabajo y la relación de trabajo se rigen por la Ley de Contrato de Trabajo -Ley Nº 20.744- (con las reformas de la Ley Nº 21.297 t.o. 1976, según decreto Nº 390/76 y sus modificaciones posteriores), por las leyes y estatutos profesionales, por las convenciones colectivas o laudos con fuerza de tales, por la voluntad de las partes y por los usos y costumbres, entendemos que todo lo concerniente a la relación entre el trabajador y el empleador respecto de la política de confidencialidad y uso de las herramientas de trabajo debe ser regulado de manera especial.

Ello debido a que el correo electrónico, otorgado a un trabajador como consecuencia de la relación laboral existente, es asimilable a una herramienta más de trabajo que el empleador provee a su empleado.

No puede desconocerse que el uso de esta herramienta, es cada vez mayor y la simplicidad de su técnica y rapidez en la comunicación llevan a cualquier persona a valerse de sus ventajas. Por eso, el tiempo que puede insumir su uso y la lectura de los mensajes recibidos, no deben quedar fuera de la esfera de aplicación de los principios del derecho laboral.

No podemos olvidar tampoco que, si bien la dirección del correo puede incluir el nombre o las iniciales del empleado y se le otorga una clave o *password* para su acceso, muchas veces también aparece en esa misma dirección el nombre de la empresa a la cual esa persona pertenece, comprometiendo por este medio un nombre comercial.

Encontramos que el Capítulo VII del Régimen de Contrato de Trabajo contempla los derechos y deberes de las partes, estableciendo en el artículo Nº 62 las obligaciones genéricas que las partes deben seguir. Se les impone un obrar de buena fe, lo que es propio de un buen empleador y un buen trabajador (artículo Nº 63 del mismo cuerpo legal), determina las facultades de organización económica y técnica de la empresa - artículo Nº 64 ley citada-, como así también la facultad de dirección, atendiendo a los fines del establecimiento.

Por su parte, el trabajador debe observar todos aquellos deberes de fidelidad que deriven de la índole de las tareas que tenga asignadas, guardando reserva o secreto de las informaciones a las que tenga acceso (artículo Nº 85 del mismo cuerpo citado). Luego, en el artículo Nº 86 se establece el deber de cumplimiento de órdenes e instrucciones que debe observar el trabajador, sobre el modo de ejecución del trabajo. Y, posteriormente, es que solicitamos incorporar el artículo 86 bis el cual regula el uso del correo electrónico laboral.

Asimismo, y porque entendemos que el correo electrónico es hoy una herramienta más de trabajo, no puede olvidarse el derecho de "propiedad" -por así llamarlo- que el empleador tiene sobre esa herramienta que pone a disposición de su empleado, como consecuencia del vínculo que los une.

El empleador tiene a su alcance el artículo 70 del RCT, que contempla sistemas de controles personales para los trabajadores, destinados a la

protección de sus bienes, siempre salvaguardando la dignidad del trabajador, como lo establece la ley.

Estos sistemas de control, en tanto estén destinados a la totalidad del personal y sean puestos en conocimiento del trabajador y de la autoridad de aplicación -artículo Nº 7 de la ley citada-, no pueden ser desconocidos y son por lo tanto incluidos en las disposiciones de la presente ley.

El conflicto se da entre los derechos de los empleadores a efectuar un seguimiento de las actividades de los trabajadores para los propósitos legítimos de su empresa y el derecho de estos últimos a la privacidad en las comunicaciones electrónicas.

No obstante, y por tratarse de una herramienta de trabajo de naturaleza diferente, entendemos que deben tomarse ciertos recaudos mínimos. En especial, en lo que respecta a la información brindada previamente al trabajador, tanto respecto del uso del correo electrónico laboral, como del correo electrónico personal que el trabajador pudiera tener.

En ese sentido, y a partir de los avances tecnológicos, el correo electrónico se ha transformado en un medio práctico y cotidiano de comunicación para las personas, por ese motivo prevemos expresamente que el empleador deberá notificar a su empleado la política respecto del uso de su correo electrónico personal en el lugar de trabajo, pero no podrá de ninguna manera prohibir su uso.

Finalmente, creemos importante citar algunos precedentes de la jurisprudencia nacional en lo que respecta al uso del correo electrónico, en los cuales ya se equipara el e-mail con la correspondencia privada, tal el caso del famoso "Fallo Lanata", por el cual la Sala VI de la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Capital Federal en el año 1999 establece que tanto el artículo 153 como el art.155 del Código Penal, han dejado abierta la descripción típica a los "despachos de otra naturaleza" y a cualquier "otro papel privado"; pudiendo considerarse equiparado entonces el correo electrónico a la correspondencia tradicional.

También consideramos de relevancia, para finalizar, el fallo sobre el uso del correo electrónico en el lugar de trabajo, dictado por la Sala VII de la

Cámara Laboral de la Ciudad Autónoma de Buenos Aires, en marzo de 2003 en los autos "Pereyra, Leandro Ramiro C/ Servicios de Almacén Fiscal Zona Franca y Mandatos S.A. S/ DESPIDO", en el mismo se establece que la demandada en ningún momento denuncia con precisión cuál es el procedimiento que debió observar el actor en el cumplimiento de sus funciones específicas ni cuáles eran las normas internas y/o las instrucciones impartidas por la patronal sobre el uso de la red informática y, más concretamente, cuál era el control que había implementado sobre el uso del correo electrónico por parte de sus empleados. Así las cosas, es evidente que el correo electrónico es hoy una "herramienta" más de trabajo. La cuestión sin duda debe analizarse de acuerdo a los derechos y deberes de las partes (arts. 62 y sgtes. de la LCT) y de acuerdo al principio de buena fe (art. 63) y el art. 70 de dicha norma, que faculta al empleador a realizar las facultades de controles personales, destinados a la protección de los bienes de la empresa. Si una empresa no tiene una política clara en el uso de esta herramienta, no advirtiendo al empleado que dicho uso debe ser realizado exclusivamente en función de su actividad laboral y haciéndole conocer el derecho de la compañía a controlar el correcto uso del e-mail, podría crear una falsa expectativa de privacidad..." (Hermida, Beatriz Miranda de "El e-mail laboral en la Argentina" - DT-2001-B-pág.1892). Como vemos, vale recalcar que en los fallos analizados se hace hincapié en varios principios recogidos por nuestro proyecto.

Convencidos de la necesidad de este proyecto, por el que se legisla sobre un vacío en nuestro cuerpo normativo, y por todo lo expuesto precedentemente es que solicitamos a esta Honorable Cámara la aprobación del presente Proyecto de Ley”[83].

b.- Estafa informática:

La Convención sobre Ciberdelito propuso legislar el fraude informático en el artículo 8, donde menciona “Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la producción de un perjuicio patrimonial a otro, de forma dolosa y sin autorización, a través de: la introducción, alteración, borrado o supresión de datos informáticos, cualquier forma de atentado al funcionamiento de un sistema informático, con

[83] http://www.protecciondedatos.com.ar/proyecto35.htm

la intención, fraudulenta o delictiva, de obtener sin autorización un beneficio económico para sí mismo o para un tercero."

Se incorporó como nuevo inc. 16 el artículo 173 del Código Penal, el siguiente "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 evolución tecnológica ha abierto paso, a estafas sofisticadas, como la imitación de páginas web para obtener contraseñas de accesos a bancos o el número de tarjetas de crédito, o la instalación inadvertida de un malware en el equipo de la víctima para conseguir tales datos. En estos casos se produce una manipulación informática, dando lugar al delito de estafa informática.

Se pueden enumerar las modalidades delictivas de estafas relacionadas con la informática, así será posible apreciar en qué medida se diferencia de la prevista en inc. 16 del artículo 173 del C. P.

b. 1. Alteración de registros informáticos:

Es una de formas más tradicionales de realizar estafas informáticas, se altera el registro informático, cuyo contenido es sistema toma en cuenta para adoptar decisiones de pago o de disposiciones patrimoniales. De esa forma, el sujeto activo obtiene fraudulentamente sumas de dinero o beneficios que de otra forma no le corresponderían.

b. 2. Uso no autorizado de tarjetas y claves falsas o sustraídas o de sus datos:

El fundamento de esta modalidad de estafa, adaptada y ampliada a la nueva realidad de utilización indebida de tarjetas de crédito y medios de pago electrónico, sigue residiendo en la mayor facilidad que supone la utilización de estos medios para realizar la maniobra engañosa, poniendo además en peligro fiabilidad y credibilidad del tráfico mercantil. Asimismo, la mayor facilidad con la que en la actualidad pueden producirse utilizaciones fraudulentas de estos medios de pago aconseja una mayor

protección de sus titulares también frente a perjuicios que no estaban contemplados anteriormente, o podían darse únicamente de manera esporádica o residual[84].

Se incluyen aquí, los supuestos de *carding,* consistentes en el copiado fraudulento de tarjetas de crédito y débito para la posterior adquisición de bienes y servicios.

Relacionado con el inc. 15 del artículo 173 del Código Penal, se puede considerar, que se incrimina al que defraudare mediante el uso de tarjeta de compra, crédito o débito, cuando ella hubiere sido falsificada, adulterada, hurtada. Robada, perdida u obtenida del legitimo emisor mediante ardid o engaño. O mediante el uso no autorizado de sus datos, aunque lo hiciere a través de una operación automática.

Esta última modalidad lo que ha hecho es receptar la posibilidad de estafar sistemas automatizados.

b.3. Cajeros automáticos:

En este supuesto, se utilizan dispositivos unidos a una laptop y disimulado en el cajero automático con el fin de copiar datos sensibles de diferentes clientes de tarjetas de crédito para posteriormente, proceder a su duplicación.

b. 4. Estafa de telecomunicaciones:

Esta modalidad de estafa tiene lugar cuando se obtiene la prestación de un servicio de comunicaciones sin haberlo abonado previamente.

En nuestro país, la ausencia de previsión especifica en el Código Penal no ha impedido que en estos supuestos se aplicara el tipo penal de estafa.

b. 5. *Phising* y robo de identidad.

El *phishing* (pescador) es una modalidad defraudatoria que consiste en remitir un correo electrónico engañoso a clientes para que revelen información personal, tales como su número de tarjetas de crédito o débito o claves de cuentas

[84] BARRIO ANDRES, Moisés. “Ciberdelito 2.0. Amenazas criminales del ciberespacio”, Bs. As., Astrea, 2020, pág. 97.

bancarias- a través de sitios *web* simulados. Usualmente, los correos electrónicos y sitios web con gráficos atractivos para engañar a los clientes haciéndoles creer que el renitente o dueño del sitio web es el banco o una entidad gubernamental que ellos conocen. Algunas veces el pescador fraudulento solicita a las víctimas que "confirmen" la información de cuenta que ha sido "robada" o esta "perdida". Otras veces, el pescador fraudulento incita a las víctimas a que revelen información personal diciéndoles que han ganado un premio especial o que se merecen una jugosa recompensa.[85]

85 http://www.bcra.gov.ar/Noticias/Como-evitar-estafas-virtuales.asp**.** ¿Cómo podés cuidar tus datos bancarios y confidenciales?

- No des tus datos confidenciales (usuarios, claves, contraseñas, pin, Clave de la Seguridad Social, Clave Token, DNI original o fotocopia, foto, ni ningún tipo de dato), por teléfono, correo electrónico, redes sociales, *WhatsApp* o mensaje de texto.
- No ingreses datos personales o bancarios en sitios a los que hayas accedido a través de *links* recibidos por correo electrónico, redes sociales, *WhatsApp* o mensaje de texto.
- Usá contraseñas robustas mezclando mayúsculas, minúsculas y números. Evitá fechas de cumpleaños o información que pueda ser obtenida por otras personas.
- No uses la misma clave para distintas aplicaciones, cuentas o plataformas.
- Ante el ofrecimiento de premios, préstamos o beneficios tomá los recaudos necesarios para confirmar que no se trata de una estafa. No des datos de tus cuentas o tarjetas, ni realices pagos o transferencias para acceder al supuesto beneficio.
- No aceptes asistencia -presencial o telefónica- para operar en cajeros automáticos.
- No uses equipos públicos para acceder a las aplicaciones o sitios web de bancos.
- No uses redes de *wi-fi* públicas para acceder a sitios web que te pidan contraseñas.
- Si vas a realizar compras o trámites en sitios web que te generan dudas, podes contactarlos y pedirles más información sobre algún producto o buscar opiniones en foros, redes sociales y reseñas para asegurarte de que sea el sitio oficial del banco, organización o comercio donde estarás operando y de que la conexión a través de la cual realizarás la compra o trámite es segura.
- Ante la menor duda o situación sospechosa, contáctate con tu banco a través de sus canales oficiales.
- Tomate siempre un minuto antes de actuar, #VosSosLaClave para proteger tu información personal y operar de manera segura.

¿En qué consisten algunas modalidades de engaño?
-*Phishing*: un correo electrónico que aparenta ser legítimo que es utilizado para que la persona destinataria responda brindando datos personales y confidenciales.

-*Smishing*: un mensaje de texto o cualquier aplicación de mensajería que solicita información mediante un engaño.

¿Sabes cómo diferenciar un perfil verdadero de uno falso en redes sociales?

-Las cuentas confiables tiene junto a su nombre un ícono de verificación (tilde azul).

-Los perfiles falsos generalmente son recientes, podes revisar los posteos y comentarios para tener en cuenta la antigüedad de la cuenta.

-Las cuentas falsas suelen tener pocos seguidores y muchas veces buscan, contactan o invitan por mensajes directo a los seguidores de las cuentas oficiales indicando que son cuentas de ayuda para personas clientas.

Una variante del *phishing* es el *smishing,* que se caracteriza porque en este caso el canal utilizado para cometer el engaño son los mensajes SMS de telefonía móvil. Las pautas de actuación son idénticas, permitiendo al delincuente beneficiarse económicamente de los datos suministrados por la víctima del engaño.

Este tipo de ciberdelito se cometen en muchas ocasiones por grupos criminales organizados, de los que rara vez se logra identificación. En cuanto a las víctimas, suelen acudir preferentemente a la jurisdicción civil para reclamar a las entidades bancarias el reembolso del importe del delito. Con carácter general, se considera que, salvo actuación fraudulenta, incumplimiento deliberado o negligencia grave por parte del titular de la cuenta, la responsabilidad es de la entidad bancaria.[86]

Se debe incluir en el delito de estafa informática, aquellos supuestos en los que se interfiere con el navegador de internet para aparentar ante el usuario que se está en un sitio *web* determinado, cuando en realidad se está redireccionando a una página *web* distinta de la pretendida, a pesar de que formalmente se asemeja a la original, y de que incluso los certificados de seguridad parezcan correctos. Se denomina como *pharming*, y se caracteriza por afectar el servidor de nombres de dominio (DNS).

Como todo delito contra el patrimonio, esta nueva modalidad de estafa requiere que exista perjuicio patrimonial y ello se debe producir mediante la disposición patrimonial.

c.- El daño a bienes intangibles y la distribución de virus informático:

La ley 26.388 incorporó como segundo párrafo del art. 183: “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 causa daño”.

- Tené en cuenta que se crean perfiles falsos para obtener información bancaria de las personas clientas y así poder realizar estafas y ciberdelitos. En general, son estas cuentas falsas las que inician una conversación con vos cuando @ arrobas a tu banco ante dudas o consultas en sus canales digitales. ¡Tené cuidado! No brindes ningún dato a través de estos medios.

[86] BARRIO ANDRES, Moisés. “Ciberdelito 2.0. Amenazas criminales del ciberespacio”, Bs. As., Astrea, 2020, pág. 95.

El delito puede recaer sobre “datos, documentos, programas o sistemas informáticos”. Esta es la principal modificación que requería nuestro código penal. La ausencia de tales objetos en la descripción del art. 183 del C.P., llevó em numerosos casos a concluir que su destrucción resultaba atípica.

La norma amplió mucho el tipo penal, de modo tal que se tendrá aplicación fuera del ámbito de los ordenadores, sino que podrían estar contenido en la denominada “nube”. Ello es así, porque el nuevo tipo penal no requiere expresamente que los datos o programas estén contenido en una computadora.

Los datos a ser destruidos no necesariamente, deben ser personales, sino también anónimos, estadísticos o de cualquier naturaleza.

Este delito, comprende desde la infección con virus, gusanos o bombas informáticas, hasta la actuación de cibercriminales que, por medio de varios métodos informáticos como el *phishing, spywares* (programas espías), r*ootkits* (programas que permiten el acceso remoto sin conocimiento ni autorización del usuario) *ransomwares* (programas que restringen el acceso al sistema de la víctima y exigen el pago de un rescate para eliminar la traba) y todo tipo de técnicas informáticas y de *malware* (programas dañinos), acceden ilícitamente al sistema informático y alteran o destruyen elementos en él.

Entre las prácticas más habituales, incluyen el descifrado de contraseñas *(password guessing*) la creación de puertas traseras (*backdoors*), la instalación de caballos de Troya, trampas y bombas lógicas, la captura de los paquetes de datos *(sniffing*), el acceso o control remoto *(remote access tolos; RAT).*

La inmensa potencialidad de estos programas puede provocar daños con un alto valor al detener el funcionamiento de sistemas informáticos dedicados a numerosas tareas esenciales y de interés público. La criminalización de estas acciones está claramente justificada y no hay razones técnicas o legales para permitir la legalidad de un virus informático.

d.- Interrupción de Comunicaciones Electrónicas:

La ley 26.388, en el artículo 197 dispone que Será reprimido con prisión de seis meses a dos años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza…".

Esta reforma ha sido importante porque el tipo anterior, estaba teñido con la idea de lo público, ya que lo que se protege es la seguridad pública y en esa situación era muy difícil pensar en tipicidad cuando se trataba de redes de uso particular o privado.

Pero la voluntad del legislador a través de la reforma de la ley 26.388 fue ampliar el tipo penal a cualquier nuevo medio de comunicación, con independencia de su naturaleza pública o privada.

e.- Alteración de pruebas:

El artículo 255 del Código Penal, reformado por la ley 26.388, protege la preservación de objetos destinados a servir de prueba ante la autoridad pública, o de registros y documentos que interesan al servicio público puestos en custodia a tal efecto.

Este tipo penal, se aplica a objetos destinados a servir de prueba ante la autoridad competente, incluyendo registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público.

B.- FIGURAS NO CONTEMPLADAS EN LA REFORMA

En el presente apartado analizamos algunas figuras que no han sido contempladas por la ley 26.388 de reforma al Código Penal. A nuestro entender, se trata de conductas reprochables que afectan a los usuarios de Internet y las nuevas tecnologías de la información cuyos agentes se valen de éstas para perpetrar sus ataques, ocasionando así serios perjuicios e inconvenientes para la sociedad toda, los que lamentablemente no han sido previstos por nuestro legislador[87].

[87] TOBARES CATALA, Gabriel H., CASTRO ARGUELLO, Maximiliano J. Castro Arguello, Ob. Cit., p. 210/218

a. Calumnias e injurias

Se entiende por calumnias, el delito contra el honor de las personas, consistente en la imputación falsa de la comisión de un delito de los que dan lugar a procedimientos de oficio; o sea, al ejercicio de la acción pública. Por su parte el derecho *de injurias* hace referencia a todo expresión proferida o acción ejecutada en deshonra, descrédito o menos precio a otra persona.

Si por algo se ha destacado Internet, es la posibilidad que ofrece a todo el mundo de expresarse con gran libertad, de manera fácil, barata y cómoda, ya sea mediante la publicación de contenidos en páginas personales, fotografías o aportaciones en foros y listas de correo, entre otros.

Sin embargo, esta libertad y el anonimato que aporta muchas veces la red ha contribuido a que se lleven a cabo conductas tan poco lícitas y molestas como la emisión de mensajes injuriosos y calumniosos contra otra persona[88].

[88] Sin embargo, esta libertad y el anonimato que aporta muchas veces la Red, ha contribuido a que se lleven a cabo conductas tan poco licitas y molestas como la emisión de mensajes injuriosos y calumniosos contra otras personas. El Código Penal Español de 1995, en su articulo 205, define el delito de calumnia como:"La imputación de un delito hecha con conocimiento de su falsedad o temerario desprecio hacia la verdad" Así, mismo, el artículo 208 de la misma norma define injuria como: La acción o expresión que lesionan la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación. Solamente serán constitutivas de delito las injurias que, por su naturaleza, efectos y circunstancias, sean tenidas en el concepto publico por graves. Las injurias que consistan en la imputación de hechos no se consideraran graves, salvo cuando se hayan llevado a cabo con conocimiento de su falsedad o temerario desprecio hacia la verdad. Las calumnias e injurias hechas con publicidad verán incrementadas su pena. (Artículos 206 y 209 C.P). El articulo 211 C.P establece que los delitos de calumnia y la injuria se reputaran hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante. Y es aquí donde entra en juego Internet, medio que posibilita la difusión de un contenido o información a muchos lugares distintos al mismo tiempo, permitiendo que la propagación de la calumnia o injuria sea infinitamente superior. Por tanto, puede incluirse en este supuesto la difusión de mensajes injuriosos o calumniosos a través de Internet, en especial a través del entorno world wide web. El articulo 212 C.P establece la responsabilidad solidaria del propietario del medio informativo a través del que se haya propagado la calumnia o injuria. En el caso de Internet, la responsabilidad civil solidaria alcanzaría al propietario del servidos en el que se publico la información constitutiva de delito, aunque debería tenerse en cuenta, en este caso, si existió la posibilidad de conocer dicha situación, ya que el volumen de información contenida en un servidor no es comparable con cualquier otro medio de información, como puede ser una revista, una radio, un programa de televisión o un periódico. El ofendido deberá interponer querella contra el presunto autor, tal y como establece el Articulo 215 C.P: 1. Nadie será penado por calumnia o injuria sino en virtud de querella de la persona ofendida por el delito o de su representante legal. Bastara la denuncia cuando la ofensa se dirija contra funcionario público, autoridad o agente de la misma sobre hechos concernientes al ejercicio de sus cargos....Si el Juez o Tribunal reconoce la falsedad o la falta de certeza de las imputaciones, podrá ordenar, a petición del ofendido, la publicación de la retractación

En la actualidad se evidencia una utilización masiva de la red como uno de los tantos medios de comunicación, dada la simplicidad en su uso y el abaratamiento en sus costos para su adquisición. Esto y muchas causales, han favorecido el crecimiento vertiginoso de publicaciones, de ideas que establecen la importancia acerca de la utilización, su control en el manejo de los medios masivos de comunicación como es este caso es Internet.

Al tener capacidad de acceder a la población en general y al mundo a través de dicho medio, se tiene una gran ventaja de poder llegar a un número indeterminado de personas para que dicha información, en el tema en que se trate, pueda ser receptada en poco tiempo y con un costo bajo e incluso de manera gratuita. Pero en la realidad actual se ha notado que si se utiliza inadecuadamente puede generar distorsiones sobre las finalidades lícitas y morales en su difusión.

Pueden surgir por dicho comportamiento, favoritismos políticos, económico respecto de algunos sectores de la población, menoscabando ideas, individuos, difamaciones, comentarios injuriosos, ofendiendo la personalidad o integridad moral, protegida como un bien jurídico por el Código Penal; o calumnias desmedidas atacando, no solo el honor sino también poniendo en peligro a la víctima de dicha calumnia, frente a la posibilidad de ser investigada por falsas atribuciones de un delito dirigido a una o varias personas o grupos, como también discriminaciones de todo tipo, racial, cultural, religiosa entre otras.

Con motivo de nuevas tecnologías se fueron originando nuevos modos de realizar variadas e ingeniosas injurias, donde las cualidades que reviste a la persona en su relación social, calidades éticas o morales, como también vinculadas en relaciones profesionales son afectadas de una manera infrenable y tornándose muy difícil la forma de evitar estas conductas para lograr así algún tipo de protección contra ellas.

Navegando por la web se puede localizar innumerables ejemplos de tales actividades, como también antecedentes en sus juzgamientos por

---

en el mismo medio en el cual se vertieron dichas declaraciones. (Articulo 214 C.P). http://www.seguridadydefensa.com/informes/calumnias-e-injurias-2071.html

estados, que ya comenzaron a incluir dentro de su realidad legislativa las injurias o calumnias “cibernéticas”.

a.1.-Bien jurídico protegido:

El bien jurídico protegido con sanción penal es el “honor”. Es así que los modos de afectar el honor son perjudicando la fama u ofendiendo moralmente, con independencia de que se lo haga en forma pública o privada.

Se señala que la injuria es el género y la calumnia la especie. La especialidad surge del carácter de la atribución deshonrante –una imputación específica- y de que-además del ataque al honor-nace para el sujeto pasivo la posibilidad de ser sometido a procedimiento judiciales vinculados con la imputación de ese delito. Requiere la afectación de la honra o el crédito del sujeto pasivo, posiblemente afectados con la utilización de las nuevas tecnologías de la comunicación, como medio de vulneración del antedicho bien jurídico, tanto en espacios virtuales como comunicaciones electrónicas.

a. 2. Acción

Respecto de la calumnia, la acción típica consiste en atribuir-imputar- falsamente a una persona o grupo de personas determinadas un delito que dé lugar a la acción pública, utilizando la red de redes como medio idóneo para expresar la imputación.

La atribución del delito debe ser falsa, y que la imputación verdadera no constituye delito.

La falsedad de la imputación debe probarse; y comprobada la verdad de la imputación el suceso es atípico de calumnia. El delito que el agente atribuya debe ser una conducta que éste penalmente contemplada y debe atribuirse como tentado o consumado; además, tiene que ser un delito de los que “dé lugar a la acción pública”, puesto que, si es de acción privada, claramente no será calumnia, pero podría constituir una injuria.

El tipo contempla medios específicos, como son la difusión de la imputación a través de Internet, correo electrónico, o cualquiera relacionado con las

nuevas tecnologías, que permite inferir que el autor atribuye a la víctima la comisión de una conducta tipificada legalmente.

Es en principio un delito “formal”, que se consume cuando la imputación llega a conocimiento del damnificado u otros individuos desacreditándolo, sin que sea necesario que efectivamente haya sentido deshonrado, o que efectivamente se produjera el descrédito porque un tercero extraño conoció la falsa imputación. Dependiendo de las modalidades de comisión utilizadas cabría la posibilidad de tentativa, como por ejemplo, el envío de un correo electrónico en el que se imputa falsamente un delito a una persona y cuya recepción no se produce por circunstancias ajenas al autor.

En cuanto a la figura de la calumnia, que se puede afectar el honor ajeno en forma: directa, dirigiendo la ofensa al sujeto pasivo; indirecta, dirigiéndola a un individuo para que recaiga sobre otro, por ejemplo: “hijo de ladrones”, explícita, a través de expresiones unívocamente ofensiva, implícita, dándole a expresiones que pueden tener un significativo diferente, carácter ofensivo, entre las que encontramos las injurias equívocas encubiertas.

La acción típica consiste en deshonrar o desacreditar. La conducta del autor debe ser objetivamente injurioso. Supone la exteriorización un pensamiento lesivo del honor ajeno. La injuria es imputativa, ya que implica un desmedro de las calidades estructurantes de la personalidad. Requiere imputaciones de calidad, costumbres o conductas que pueden ser apreciadas como peyorativas. Es necesario que el carácter imputativo esté presente aun cuando el agente recurra a las vías de hecho para negar una calidad valiosa de la persona atribuyéndole una disvaliosa. La injuria puede consistir en un ataque a la honra del individuo, a su honor subjetivo- o a su derecho a que se respete su personalidad según sus cualidades que se le asignan como persona-, sin importar la trascendencia de la ofensa a terceros, ni que el sujeto se sienta moralmente herido. Igualmente, puede consistir en una ofensa al crédito, al honor objetivo del individuo, o juicio o apreciación que los demás tienen de la víctima- o su derecho a exigir que el sujeto activo no incite a los demás a formarse mala opinión de él. Así, la acción de desacreditar supone hacer una manifestación ante terceros de imputaciones ofensivas que puedan menoscabar la reputación que tiene el sujeto pasivo frente a aquéllos. Por esta razón, requiere que la ofensa trasciende a uno o más individuos distintos del ofendido siendo indiferente que éste presente o ausente la víctima. Desacreditar supone tratar de quitar

crédito y reputación, implica difamación. Para llevar adelante su cometido, el agente se puede valer de cualquier medio relacionado con Internet y las nuevas tecnologías de la información y comunicaciones que le sea útil para atribuir tal ofensa objetivamente injuriosa. Por ejemplo: la colocación de frases ofensivas en los portales de Internet, llamados “blogs personales”, en los que los individuos tienen la libertad -bajo ciertos parámetros controlados por “moderadores”- de expresar sus ideas o intereses, difamando a la víctima con tal accionar.

El delito es formal y se consuma con la realización de la conducta que deshonra o desacredita, aunque el ofendido no se haya sentido deshonrado o no se haya alcanzado el descrédito ante los demás. Si es necesario que la ofensa llegue a conocimiento de terceros que pueden comprender su carácter ofensivo, sin que sea necesario que la conozca el ofendido.

Tampoco se requiere la publicidad de la injuria, la que se puede llevar a cabo simplemente mediante comunicación electrónica privada (un mensaje de texto, chat o un correo, por ejemplo); sin embargo, la mencionada publicidad se ve altamente favorecida por la difusión generalizada del acceso que presenta la red de redes, en las que cualquiera que tenga la posibilidad de utilizar una computadora tiene oportunidad- dependiendo de las restricciones que pudieran presentarse en el caso concreto- de enterarse o interiorizarse de la mencionada calumnia, cuando ésta se materializa en páginas web de uso masivo.

Podemos que por Internet se puede injuriar (deshonrar o descreditar públicamente a otro) y calumniar (imputar falsamente a otro un delito que dé lugar a la acción pública). Cualquier medio expresivo es idóneo para ofender, basta que pueda ser vehículo de una voluntad ofensiva y que por alguien pueda ser entendido.

Más problemático resulta definir, entre otros temas, si el servidor puede ser incluido en la figura autónoma del art, 113 del C. P. que reprime “como autor de las injurias o calumnias” al que “publicare o reprodujere por cualquier medio, injurias o calumnias inferidas por otro”. Como vemos, las acciones típicas son las de “reproducir” y “publicar”. Reproduce la injuria o calumnia vertidas por otro quien repite la especie ofendida, llevándolo a conocimiento de personas que no habían captado cuando el autor original la produjo, divulgándola así entre un número mayor o menor de personas.

Publica las ofensas quien la produce de modo que pueda llegar a conocimiento de un número indeterminado de personas.

Un dato a tener presente es lo que se puede verificar cuando un tribunal juzga por primera vez las injurias vía Internet. Utilizar la red para divulgar acusaciones personales no exime al responsable de ser juzgado por injurias, calumnias o difamación, según el Superior Tribunal de Brasil, fue este Tribunal, el primer órgano judicial en tomar en cuenta una denuncia por injurias en Internet.

Cualquier persona puede deshonrar o desacreditar a otra haciendo uso de la web como un medio para cometer su accionar, ya sea enviando un simple e-mail personalizado, dirigido únicamente al destinatario de dicha conducta o bien enviando de un modo desenfrenado un mensaje injurioso por medio del reenvió que se realiza que se realiza en un correo electrónico o en la creación casera de una página web, sin tener la necesidad de una identificación, tanto personal como geográfico de su origen.

La injuria no requiere que el conocimiento de la deshonra o difamación llegue a terceras personas para consumarse. Es por ello que puede consumarse la conducta con el envió de un correo electrónico, o mensajes instantáneos de texto al teléfono móvil de la víctima[89]; o la simple expresión de una idea que puede llevarse a cabo por medio de los denominados “chat”, donde los usuarios se conectan en tiempo real, mediante la referencia de palabras injuriosas, verbales o escritas, dada la posibilidad que

[89] El representante de la empresa constructora Sacyr Vallehermoso presentó el pasado 21 de febrero ante la Brigada de Investigación Tecnológica, Grupo de Fraudes a las Telecomunicaciones, una denuncia para investigar el envío de mensajes SMS a través de teléfonos móviles que decía así: "Próxima suspensión de pagos de Sacyr Vallehermoso. El PSOE, responsable de pactar inmunidad y pagar a los responsables de dicha compañía a cambio de aguantar hasta después de las elecciones. Zapatero se ha jugado el puesto. Pásalo". Así, el Juzgado de Instrucción número 1 de Madrid ha abierto diligencias para investigar el origen del mensaje difundido a través de los teléfonos móviles en el que se asegura la "próxima suspensión de pagos" de Sacyr Vallehermoso. Los responsables de Sacyr consideran que el mensaje es una "injuria" que podría ser constitutiva de delito, al igual que una alteración del precio de las cosas, agravado por el hecho de interferir en el proceso electoral. Pide "la identificación de los responsables, las circunstancias de los mismos y que se acuerden medidas cautelares". Varios empleados de la empresa recibieron dichos mensajes y pusieron sus terminales a disposición de la policía para que pudieran rastrear la procedencia de los mismos. Según los denunciantes estos mensajes hicieron que la evolución de la cotización de la empresa en bolsa se resintiera. En el escrito presentado a la policía destacan precisamente que "su valor [en Bolsa] puede verse alterado por la difusión de rumores o de información ficticia y mal intencionada". A tal efecto, consideran que el envío de un SMS con la petición "pásalo" es un medio idóneo para conseguir una rápida expansión de la información, que califican de "mendaz", y de "manipular los precios". http://www.delitosinformaticos.com/03/2008/delitos/calumnias-e-injurias/investigacion-judicial-de-mensajes-sms-por-posibles-injurias

brinda dicha comunicación por medio de micrófonos incorporados a las computadoras; o por gestos ofensivos manifestados por medio de *web cam*. La difamación o el descrédito, fácil en su producción dada la posibilidad que la información pueda trascender fronteras, llega en segundos a portales de Internet donde sus usuarios son incontables. Imágenes injuriosas, palabras ofensivas pueden propagarse y circular por este mundo virtual, donde la posibilidad y el anonimato son características de las que se vale el agente para llevar a cabo sus intenciones[90].

En cuanto a la posibilidad de tentativa del delito, teniendo en cuenta los medios empleados para realizar los actos ejecutivos- Internet y nuevas tecnologías como correo electrónico, páginas web, mensajes de textos a telefonía celular, etc, por ejemplo: el envío de e-mail con contenido ofensivo que no llegue a su destinatario por un error del servidor.

---

[90] Son cada vez más numerosas las querellas criminales que se presentan en los Tribunales por presuntos delitos de injurias y calumnias a través de Internet, normalmente por mensajes contenidos en foros de discusión. Los autores de esos mensajes suelen escudarse en el anonimato que Internet proporciona y obviamente no facilitan sus datos considerando que de esta manera actúan con total impunidad, lo cual no es cierto, ya que en muchos casos es posible descubrir quien se encuentra detrás de un mensaje injurioso o amenazante. Para ello son necesarios una serie de datos que los prestadores de servicios de intermediación de la sociedad de la información pueden facilitar en la mayoría de los casos a petición de la autoridad judicial.
Son prestadores de servicios de intermediación de la sociedad de la información aquellas empresas o profesionales que:
1.- facilitan el servicio de acceso a Internet.
2.- trasmiten datos por redes de telecomunicaciones.
3.- realizan copias temporales de las páginas de Internet solicitadas por los usuarios.
4.-alojan en sus propios servidores datos, aplicaciones o servicios suministrados por otros.
5.- proveen de instrumentos de búsqueda, acceso y recopilación de datos o de enlaces a otros sitios de Internet.
Es habitual que los injuriados, calumniados o amenazados, ante el desconocimiento de quién es quien efectivamente ha escrito el mensaje presuntamente delictivo, denuncien al prestador de servicios de intermediación que es el único cuyos datos conocen a través de la web y que normalmente es el titular de la página donde se aloja el foro.
91La legislación sobre la materia es clara en este punto. La Ley 34/2002, de 11 de Julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico exonera de responsabilidad a los prestadores de servicios de alojamiento o almacenamiento de datos siempre que no tengan conocimiento efectivo de que la actividad o la información almacenada es ilícita o si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos.
Debido a que estamos ante una materia muy reciente no existe demasiada jurisprudencia al respecto, aunque ya contamos con algunas Sentencias y Autos de Archivo como el del Juzgado de 1ª instancia e instrucción de Cazalla de la Sierra, de 25 de enero de 2006, o el del Juzgado de Instrucción nº 2 de Melilla, de 27 de julio de 2005 e incluso de Audiencias Provinciales como la Sentencia de la Audiencia Provincial de Murcia de 18 de mayo de 2006 (Rollo Apelación Juicio de Faltas 58/06).
hhtp://www.delitosinformaticos.com/06/2008/delitos/la-responsabilidad-penal-de-los-prestadores-de-servicios-de-intermediacion-de-la-sociedad-de-la-informacion

De alguna manera, los tribunales argentinos están recepcionando y dando lugar a causas donde esta temática se ve plasmada en expedientes civiles, pero de alguna forma son un importante aporte al momento de evaluar elementos que pueden ser contemplados en nuestra materia. Así, por ejemplo, la circulación de una página web con mensajes que afecta el buen nombre y honor de una persona, y que contempla la misma problemática de los delitos cometidos por medio de la prensa escrita u oral, por televisión, etc[91].

b.- Ciberacoso (*cyberstalking*):

El delito de acoso a través de los medios de comunicación, que se denomina también delito de acecho u hostigamiento, y en el derecho anglosajón se conoce como *ciberstalking*, se lleva a cabo mediante llamadas telefónicas continuas, seguimientos o cualquier otra fórmula que pueda lesionar gravemente la libertad y el sentimiento de seguridad de la víctima, aunque no se produzca violencia. A diferencia de las conductas de amenazas o coacciones, en el ciberacoso el autor no solo utiliza frases de naturaleza amedrentadoras, sino que actúa de modo sistemático para restringir la capacidad de decisión de la víctima, siendo una de sus expresiones más usuales el empleo de medios electrónicos para hostigarla y alterar, de forma grave si vida cotidiana[92].

El bien jurídico protegido, es la libertad que es menoscaba por medio de la creación de una situación o contexto intimidatorio para que la víctima, que teme padecimiento de un mal indeterminado e incierto es cuando al momento y de forma de causación, puede incluso afectar de forma mucho más grave a su libertad personal que el anuncio de un mas en sentido estricto.

c.- El delito de captación ilegal de datos, imágenes y sonido:

En nuestro país, no constituye un delito penal, la obtención o captación de la imagen, sonido o datos de una persona en forma ilegal, ni su difusión.

En la jurisprudencia, las cámaras ocultas han sido objeto de controversias, habiéndose admitido su uso por parte de la prensa en algunas decisiones

---

[92] BARRIO ANDRES, Moisés. “Ciberdelito 2.0. Amenazas criminales del ciberespacio”, Bs. As., Astrea, 2020, pág. 108.

judiciales de naturaleza civil y especialmente en casos de corrupción, pero se consideran ilícitas en otros, sobre todo porque en muchas situaciones donde no hay interés público legitimante, significan un avance no consentido sobre la propiedad o la privacidad de terceros.

Si se usan para recopilar prueba en un proceso penal, claramente se requerirá orden judicial si los datos captados provienen de un lugar privado.

Sin embargo, cuando la imagen y otros aspectos de la personalidad de los individuos, cuando son captados ilegítimamente y producen un daño, encuentran amparo en la faz civil.

CONCLUSIONES

Las nuevas tecnologías de la información y comunicaciones son y serán una herramienta esencial en el desarrollo y evolución de toda comunidad (cualquiera de sus diferentes sectores), favoreciendo el crecimiento y afianzamiento de la nueva cultura comunicacional, de las que las sociedades no pueden prescindir y en las que las fronteras nacionales se tornan difusas, a raíz de la virtualidad que logran las mayorías de las actuaciones que cualquier persona pueden realizar a través de ella.

No cabe dudas que la “era digital” ha otorgado y seguirá proporcionando innumerables beneficios a nuestra sociedad; sin embargo, no podemos desconocer que este desarrollo tecnológico ha propiciado la aparición de nuevas modalidades delictivas, las cuales presentan una serie de aspectos impensables para la criminalidad convencional clásica, que hace más de una década eran desconocidas en nuestro ordenamiento jurídico.

Es así que el actual panorama tecnológico nos ofrece una amplia gama de perspectivas de actuación, tornándolas atractivas a nivel global. Ahora bien, este uso que se les otorga, en la mayoría de los casos se hace conforme prácticas que respetan cánones legales, la buena fe, usos y costumbres aceptados de manera general, y que coadyuvan a la difusión de posibilidades que estos ofrecen, para facilitar mecanismos de comunicación interpersonal, empresarial y hasta gubernamental.

No obstante, todo este abanico de alternativas tecnológicas, han sido el caldo de cultivo de numerosos accionares ilícitos y conductas disvaliosas que atacan a un incontable grupo de bienes jurídicos que el derecho protege.

Adicional a ello, es necesario plantear la premisa de que es muy importante contar con un personal altamente entrenado y capacitado para llevar a cabo de la manera más adecuada, los procesos anteriormente descritos, dado que, por la facilidad de manipulación de la información, un solo error al momento del proceso puede llevar a que una investigación criminal digital pueda no llegar a los términos esperados.

En el desarrollo del presente trabajo -el que se presentó a través de cinco capítulos- se comenzó detallando qué son las “computadoras” y cuáles son los dispositivos con los que cuentan, definiendo términos como “informática” y “telemática”, para luego avanzar sobre el origen de Internet y la importancia de este servicio -que ha sido considerado de tamaña envergadura- y que llevó a nuestro país a la sanción del Decreto de Necesidad y Urgencia (DNU 69/20), constituyendo a partir de allí un servicio público, para finalizar definiendo qué es un delito informático, aportando importantes nociones sobre el tema.

En el primero de los capítulos, dadas las características de Internet, las cuales podemos sintetizar diciendo que es descentralizado y transnacional, se determinó el rol de los organismos internacionales, y la necesidad de contar con una legislación internacional que regule las actuales y complejas modalidades delictivas que se originan en el ciberespacio.

Se evidenció la urgencia de una mayor colaboración internacional, la cual fue plasmada en un Acuerdo, siendo el Convenio de Budapest una valiosa herramienta para lograr una política penal común destinada a prevenir el delito en el ciberespacio, y de hacerlo mediante la adopción de una legislación apropiada y la mejora de la cooperación internacional. Resultó este Convenio la principal fuente de influencia para sancionar en nuestro país la Ley 26.388 denominada “Ley de Delitos Informáticos”.

Además, se desarrolló cómo se estructura el Convenio de Budapest, a los fines de señalar la normativa de fondo que contiene.

En el Capítulo II, fueron analizados los antecedentes nacionales referidos a las nuevas tecnologías de la información.

En el Capítulo III, se desarrolló el aspecto de la incidencia del Convenio de Budapest en la Legislación Argentina.

En el Capítulo IV, se analizaron los sujetos intervinientes en los delitos informáticos según la legislación penal Argentina, determinando los sujetos activo y pasivo, como así también las conductas relacionadas con los delitos informáticos.

Por último, en el capítulo final, fueron estudiadas las figuras penales contempladas en la legislación nacional, las cuales guardan relación con las normas en materia penal de fondo, descriptas por el Convenio de Ciberdelincuencia.

Luego del abordaje de los temas propuestos inicialmente, llegamos a esta instancia convencidos, como se anticipó en la hipótesis para este trabajo oportunamente propuesta, de que “la escasa previsión normativa de la legislación nacional se ha solucionado con la adhesión al Convenio de Budapest”, ya que ha sido, dicho instrumento internacional, la principal influencia y motivación para que la legislación nacional penal de fondo se adecue a la nueva “era digital”. En primer lugar, con la sanción de la ley 26.388, la que vino a actualizar algunos conceptos jurídicos, tales como “documento”,” firma”, “suscripción”, “instrumento privado”, “certificado”, y por cuanto, además, vino a reprimir conductas que antes de su sanción eran consideras atípicas, sea por la forma de comisión o por el objeto sobre el que recaían. En segundo lugar, y con posterioridad a la reforma de la ley 26.388, se sancionaron dos importantes leyes, a saber, la 26.904 que data del año 2013, por la cual se incorpora la figura de “Grooming” y la ley N° 27.436, que castiga la simple tenencia de material pornográfica infantil.

Sin perjuicio de ello, el análisis del Convenio de Budapest, ha llevado a concluir, que aún resta mucho camino por recorrer, ya que el mismo posee grandes virtudes, pero también algunos inconvenientes.

Entre las virtudes, podemos señalar que, al adherir nuestro país a dicho Convenio por medio de la sanción de la Ley 27.411, resultó actualizado y enriquecido el escenario legislativo del país, sobre todo en los aspectos de fondo, procesales y de cooperación internacional en la lucha contra el cibercrimen. La adhesión a este Convenio, implicó la incorporación de conceptos y pautas legislativas que Argentina no tenía hasta el momento. Cabe recordar que por ley 26.388 ya se habían dispuesto ciertas modificaciones en la parte especial del Código Penal, incorporando figuras delictivas de conformidad a las previsiones del Convenio de Budapest, lo que también formó parte del proceso de adhesión al mismo.

Entre sus inconvenientes, advertimos que faltan muchos países de la región que aún no se han adherido y, a ello se suma, que su adhesión implica un compromiso estatal para la sanción de leyes tanto de fondo como de forma, para adaptar

la legislación local a las normas de la Convención. Por último, es necesaria una actualización del instrumento a los fines de regular, por ejemplo, el acceso a la “nube”.

Asimismo, se observa que han quedado delitos sin incorporar, como son las calumnias e injurias y el ciberacoso.

En síntesis, el avance de las nuevas tecnologías a nivel mundial y nacional, cuyo ritmo no es proporcional a la elaboración y dictado de una legislación que lo regule y controle, hace que sean plausibles todas las iniciativas para actualizar el Convenio de Budapest, a través de los Protocolos Adicionales y los proyectos locales para renovar nuestros Códigos de forma y de fondo.

Advertimos que, antes de la reforma al Código Penal en materia de delitos informáticos, se presentan en este nuevo escenario, conductas reprochables con alto grado de similitud a las previstas y tratadas en nuestra legislación penal, pero, por su carácter tecnológico no podían ser sancionados por él, por no estar contemplada en las normas. Por su parte también se verificaban otras que, por lo innovadora que son, configuraban un accionar no previsto por la ley, teniendo como resultado la misma impunidad que las conductas antes mencionadas.

En este orden de ideas, y teniendo siempre presente los principios constitucionales que rigen la materia, sobre todo el “principio de legalidad” que surge del art. 18 de nuestra Carta Magna, y que deriva del aforismo latino “*nullum crimen, nulla poena sine praevia lege*”, no se podía interpretar que un acto cualquiera sea delictivo e incurso en sanción penal, si no ha sido considerado expresamente como tal en una norma anterior.

De esta forma, a través de la sanción de ley 26.338, hemos logrado insertarnos en el concierto de las naciones que en el tema han logrado transformar la falta de legislación en una solución adecuada a la necesidad imperiosa antes presentada.

Estamos frente a una realidad en constante evolución, por lo que es de esperar que la doctrina y la jurisprudencia colaboren para la construcción de la tarea iniciada por el Congreso de la Nación, en la lucha contra la criminalidad informática, así como es una obligación de todos nosotros como partes integrantes de una sociedad, informarnos y luchar por una utilización segura y responsable de estas tecnologías.

BIBLIOGRAFÍA

MOISES BARRIO, ANDRES, “Ciberdelito 2.0, Amenazas criminales del Ciberespacio”, Astrea, Buenos Aires, 2020.

PALAZZI, Pablo A. “Los delitos informáticos en el Código Penal. Análisis de la Ley 26.388”, Abeledo Perrot, Buenos Aires, 2016

BIELLI, Gastón Enrique; ORDOÑEZ, Carlos Jonathan Ordoñez, “La Prueba Electrónica, Teoría y Práctica”, Bs. As., Ed. Thomson Reuters, La Ley, 2019.

SAIN, G. (2016). “Actualización del código procesal penal de la Nación en materia informática jurídica y criminalística digital. Obtenido de www.rubinzalculzoni.com.ar: RC D 306/2016.

RIQUERT, M. A. (. Ciberdelitos. Hammurabi, Buenos Aires: Hammurabi, 2014.

TOBARES, Gabriel H.; CATALA, Maximiliano J., CASTRO ARGUELLO, “Delitos Informáticos”, ADVOCATUS, Córdoba, 2009, p. 19.

ABOSO, Gustavo Eduardo; ZAPATA, María Florencia, “Cibercriminalidad y Derecho Penal”, Editorial B de F, Buenos Aires, 2006.

CABANELLAS DE LAS CUEVAS, Guillermo; MONTES DE OCA, Ángel, “Derecho de Internet”, Heliasta, Bs. As., 2004, p. 58.

-DIEZ DE VELAZCO, Manuel, “Las organizaciones internacionales”, 9° ed. Tecnos, Madrid, 1996, p. 37.

LUCERO, Pablo Guillermo- KHOEN, Alejandro Andrés, “Delitos Informáticos”, 1 Ed. Buenos Aires, D y DSRL, 2010.

RIQUERT, Marcelo A. “Delincuencia Informática en Argentina y Mercosur”, Ediar, Buenos Aires, 2009.

Sitios web consultados:

http://www.tribunalmmm.gob.mx/biblioteca/aldemadelia/indice.htm.

http.//personales.ciudad.com.ar/roble/thaisdelitosinformaticos.htm

http.www.delitosinformaticos.com/delitos/colombia

http./www.derechotecnológico.com/delitos.html

www.universidadabierta.edu.mx/Biblio/E/Estrada%20MiguelDelitos%20informaticos.htm

http://www.monografias.com/trabajo22/delitosinformaticos/delitosinformaticos.shtml#clasif.

http://infoleg.mecon.gov.ar/infolegInternet/anexos/140000-44999/141790/norma.htm

htpp://www.segu-info.com.ar/boletín-113-080607.htm

Htpp://psi.gov.ar/queeselpsi.htm
Legislación internacional sobre delitos informáticos. Disponible en htpp://www.delitos informaticos.com/06/2008/delitos/la-incorporacion-de-los-delitos-informaticos-al-codigo penal-argentino. Ley de delitos informáticos. Martin Carranza Torres y Horacio Bruera.
http://usuarios.lycos.es/keus99/delito informaticos.htm
AbogadosPortaley.com
delitosinformaticos.com
www.chiaravollotasociados.djt.com.ar
http://scielo.sld.cu/scielo.php?pid=S1024-43520030003000006&script=sci_arttext&tlng=pt
http://infosurhoy.com/cocoon/saii/xhtml/es/features/saii/features/economy/2011/02/10/feature-02
http://tecnologia.iprofesional.com/notas/40495-La-Argentina-segunda-en-ranking-de-inversiones-tecnolgicas
http://www.lanacion.com.ar/1446184-los-hackers-atacaron-una-de-cada-dos-empresas-argentinas
www.fiscalia.org
http://www.derf.com.ar/despachos.asp?cod_des=371532&ID_Seccion=42&Titular=Mendoza:%20La%20polic%EDa%20allan%F3%20una%20casa%20de%20Maip%FA%20en%20busca%20del%20hacker%20que%20boicote%F3%20varias%20p%E1ginas%20web%20del%20Gobierno.html
http://www.losandes.com.ar/notas/2012/3/3/google-cambio-politica-privacidad-polemica-627597.asp
http://www.habeasdata.org/wp/2007/07/12/caso-Dragoslav-acceso-correo-electronico-sin-autorizacion-ilegal/
www.rosario3.com/tecnologia/noticias.aspx?idNot=33002
http://edant.clarin.com/diario/2000/06/07/s-03504.htm
www.catarina.udlap.mx/u_dl_a/tables/documentos/lfis/trillo_m_p/capitulo4.pdf
http://www.hfernandezdelpech.com.ar/PUBLICAtrabajosDerechoAutorBajadaMusica.htm
http://www.losrecursoshumanos.com/contenidos/325-el-derecho-a-la-intimidad-en-el-ambito-laboral.html
Informes consultados:
UIT-Unión Internacional de Telecomunicaciones. “Informe sobre el Desarrollo Mundial de las Telecomunicaciones 2002-Resumen de Conclusiones”, marzo de 2002.
Fundamentos a Ley 26.388 “Delitos Informáticos”. APROBADO POR LA CÁMARA DE SENADORES DE LA NACIÓN EL 28.11.2007 Y DEVUELTO a la CÁMARA DE DIPUTOS.

APROBADO POR LA CAMARA DE DIPUTADOS Y SANCIONADO COMO LEY 26388. http://www.congreso.gov.ar/

Publicado en el VI Congreso Latinoamericano en 1998, en Colonia, Uruguay. La Ley, Nros. 202 del 23 de octubre de 1998 y 215 del 11 de noviembre de 1998, Argentina.

Datos aportados por la División de Delitos Tecnológico. Policía en Función Judicial. Dirección de Investigaciones de la Provincia de Mendoza.

Naciones Unidas, Consejo Económico y Social, Comisión de Prevención del Delito y Justicia Penal, “Conclusiones del estudio sobre medidas eficaces para prevenir y controlar los delitos de alta tecnología y relacionados con las redes informáticas” 10° periodo de sesiones, Viena 8 a 17 de mayo de 2001.

Proyecto de Ley de Incorporación del art. 86 bis de regulación del correo electrónico laboral a la ley 20.744 de Contrato de Trabajo.