# TRABAJO FINAL DE CARRERA

Delitos informáticos no tipificados

**TRABAJO REALIZADO POR: DYLAN AMIEL LAX**
MATRICULA: 10133721
UB TURNO NOCHE – CARRERA ABOGACIA
Tutor: JORGE VELÁZQUEZ

# CAPÍTULO I



# CAPÍTULO II

## MARCO TEÓRICO



# CAPÍTULO III

## EL CIBERBULLYING

## CAPÍTULO IV

## CIBEROCUPACIÓN



## CAPÍTULO V

## ROBO DE IDENTIDAD



## CAPÍTULO VI

## PORNOVENGANZA

## CAPÍTULO VII

## SPAMMING



## CAPÍTULO VIII

# Capítulo I

## INTRODUCCION:

La internet en un principio fue creada para facilitar la comunicación entre largas distancias, pero a medida que avanzo el tiempo y evolucionamos como sociedad, se le ha dado diferentes usos. La internet ha modificado muchos aspectos en nuestras vidas, ya sean relaciones económicas, políticas, sociales y también las personales.

Uno de los principales avances técnicos que brindo la internet es la enorme facilidad y rapidez con la que se accede, copia, modifica y distribuye todo tipo de información, siempre a distancia, pudiendo ocultar la realidad de uno mismo y dando la posibilidad de ser emisor o receptor de contenidos a la vez. En la actualidad, el uso de la internet se puede ver en todos lados, desde administraciones públicas, prestadores de servicios públicos, empresas, entidades privadas, hasta en los ciudadanos. Dichas entidades le dan un uso a la internet que permite nuevas formas de organización de la producción y de la comercialización, pero no hay que olvidarse de que la internet también puede ser usada como forma de diversión con las redes sociales y como forma de interacción social.

Todo lo anterior conduce a que, en la mayoría de los aspectos de nuestras vidas, se dependa de las tecnologías de la Información y la Comunicación (también conocidas como TIC), que integran un concepto amplio, abierto y dinámico, que engloba todos los elementos y sistemas utilizados en la actualidad para el tratamiento de la información, su intercambio y comunicación.

A medida que las redes de comunicación avanzan y brindan más servicios, de igual manera aumenta su vulnerabilidad y la forma de aprovecharse de sus usuarios. Es debido a este constante avance en la tecnología y en sus formas de delinquir por medio de la misma que nos encontramos con lagunas legales en nuestra legislación respecto a los ciberdelitos, y es por ello que hablare de esto mismo en la presente tesina.

## **OBJETIVO**:

1.1) Objetivos generales:

Realizar una investigación acerca de esta modalidad de delinquir, llamada delitos informáticos, analizando aquellos que todavía no fueron encuadrados en un marco legal, doctrina, y jurisprudencia al respecto, si es que existen proyectos de ley, y así especificando las características de estos delitos y las formas y medios en los que se realizan.

1.2) Objetivos específicos:

- Desarrollar el concepto de delito informático
- Estudiar y desarrollar la modificación del código penal mediante la ley 26.388
- Desarrollar los delitos informáticos no tipificados
- Analizar derecho comparado
- Explicar por cuales medios se cometen estos delitos, analizando a fondo cómo funcionan y explicando las maneras de evitar caer en ellos.

# CAPÍTULO II

# MARCO TEORICO

## 2 Comienzos de los delitos informáticos:

Como comenté en la introducción, con el avance de la internet y los medios informáticos y de comunicación, también avanzaron los delitos posibles de cometer a través o con ayuda de estos. Conjuntamente con el avance de los delitos, también se fueron produciendo diferentes definiciones y encuadres de los mismos, las cuales evolucionaron con el progreso de la tecnología.

En los años 80 algunos autores comenzaron a defender la autonomía de un "delito informático" (definición traída del término anglosajón "*computer crime*") con el fin de encuadrar en un marco legal delitos realizados con una computadora, tales como la estafa informática, el acceso ilícito a sistemas informáticos, el cracking, el hacking, daños informáticos o el espionaje informático.

La definición de delito informático encuadraba todo delito perpetrado en sistemas informáticos, en los que las redes, de ser utilizadas, tienen por lo general una relevancia bastante limitada y secundaria para las características de la conducta delictiva. Davara Rodríguez[1] define el delito informático como "*aquel en el que la realización de una acción, que reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software*"

Posteriormente, dicha definición fue abandonada con la implementación creciente de las redes electrónicas. Esto se debe a que la definición de delito informático solo abarcaba como delito aquellos cometidos en una computadora o hardware informático, y no abarcaba los cometidos en redes informáticas o por medio de ellas. Así con el paso del tiempo se terminó creando la definición de los ciberdelitos.

### 2.1 Concepto del ciberdelito:

Existen varias posturas en cuanto al concepto de ciberdelito, entre las cuales me referiré a dos.

Jewkes y Yar[2] definen el ciberdelito como "cualquier ilícito penal cometido por medio de (o con asistencia de) sistemas informáticos, redes digitales, internet y demás TIC (Tecnologías de la información y de la comunicación). Teniendo en cuenta esta definición, el concepto de ciberdelito abarcaría tanto los delitos específicos de internet (por ejemplo: ataque de denegación distribuida

[1] Davara Rodriguez – *derecho informático*
[2] Jewkes – Yar – *Handbook of internet crime*

de servicio) como también los delitos tradicionales cometidos por medios electrónicos, o algunos cuya comisión implica el uso de un aspecto electrónico.

Otra definición por la que se entienden los ciberdelitos se puede encontrar en el décimo congreso de las naciones unidas sobre prevención del delito y tratamiento del delincuente[3], en donde se define que "por delito cibernético se entiende todo delito que puede cometerse por medio de un sistema o una red informáticos, en un sistema o una red informáticos o contra un sistema o una red informáticos.

## 2.2 Ciberdelitos plasmados en el derecho argentino

El ordenamiento jurídico argentino a través del tiempo fue incorporando distintas leyes con tal de prevenir delitos y proteger a los usuarios de las redes. Una de estas se trata de la ley 25.326, la Ley de Protección de los Datos Personales, sancionada el 4 de octubre del 2000. Tal como lo estipula su primer artículo, esta ley tiene como objetivo la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamientos de datos, sean estos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre.

Otra ley encargada de proteger bienes que se podrían alterar o robar por medio de redes informáticas es la Ley de Propiedad Intelectual (Ley 11.723). Dentro de dicha ley se busca proteger la creación ya sea de una persona física o persona de existencia ideal. ¿Por qué tiene tanta importancia esta ley frente a los ciberdelitos? Esto se debe a que en su art. 1 contempla entre otras obras, los programas de computación fuente y objeto; las complicaciones de datos o de otros materiales, y muchas otras obras más las cuales pueden ser objetivo de un ataque cibernético (Por ejemplo: piratería de películas/música/programas o robo de datos de empresas). Cabe agregar que dicha ley fue modificada por medio de la ley 25.036 (ley de piratería de software) la cual agrego el encuadre de programas de computación, y otras obras intelectuales dentro de un marco informático.

Por último, la ley más importante en cuanto al tema abarcado es la Ley de Delitos Informáticos (ley 26.388). Esta ley (Sancionada el 4 de junio de 2008) no regula este tipo de delitos en un cuerpo normativo separado del código penal, sino que modifica, sustituye e incorpora figuras típicas a distintos artículos en vigencia.

Procederé a dar un vistazo general y resumido a los artículos de la ley de Delitos informáticos.

[3] Viena – 10 a 17 de abril de 2000

Se modificó el art. 77 del CP incorporando como términos "*documento*", "*Firma y suscripción*" e "*Instrumento privado y certificado*". Se sustituyó el Artículo 128 del CP, incorporando delitos contra la integridad sexual tipificando figuras o conductas típicas orientadas a la indemnidad sexual de menores de 18 años. Se sustituyó el epígrafe del Capítulo III, del Título V, del Libro II del CP de la siguiente manera "*Violación de secretos y de la privacidad*" (Incluyendo de esta manera la privacidad como bien jurídico protegido). Se sustituyó el artículo 153 del CP, agregando la definición de "*comunicación telefónica*", dicha definición fue agregada ya que previamente cuando se vulneraba una correspondencia electrónica o comunicación electrónica las acciones planteadas judicialmente eran rechazadas por inexistencia de delito. Ejemplo de esto es el caso "Lanata" (1999) en el que los delitos realizados sobre los correos electrónicos interceptados habían sido considerados atípicos, equiparándoselos a la correspondencia tradicional bajo los arts. 153 y 154 del CP. Se incorporo como articulo 153 bis del CP el delito de acceso a un sistema o dato informático de acceso restringido sin la debida autorización o excediendo la que posea (delito mayormente conocido como "hackeo"). Se sustituyó el artículo 155 del CP, penando a quien en posesión de una correspondencia o comunicación electrónica o telefónica o de otra naturaleza, no destinado a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros. Se sustituyó el articulo 157 del CP, introdujendo el termino de "*datos*". Se sustituyó el articulo 157 bis del CP, penando con prisión a quien accediere a banco de datos personales, proporcionare o revelare información de banco de datos personales, o alterare o inserte datos en un archivo de datos personales. Se incorporó como inciso 16 del art 173 del CP "*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*" agregando así una nueva figura frente a la estafa informática, y protegiendo el bien jurídico del patrimonio. Se incorporó como segundo párrafo del articulo 183 del CP dos figuras, la de alterar, destruir o inutilizar datos, documentos, programas o sistemas informáticos y la de vender, destruir o introducir en un sistema informático programas destinados a causar daños (malware). Se sustituyó el artículo 184 del CP, agregando como agravante del art 183 el ejecutar el hecho en archivos, registros, (…) datos, documentos, programas o sistemas informáticos públicos y por ejecutar el hecho en sistemas informáticos destinados a la prestación de servicios de salud, comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público. Por último, se sustituyó el articulo 197 del CP, penando a quien interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida.

## 2.3 Ciberdelitos no tipificados, su clasificación

Entre los delitos informáticos que necesitan regulación y no se encuentran contemplados en la ley 26388, los cuales estaré desarrollando en la presente tesis, se encuentran los siguientes:

- Ciberbullying
- Ciberacoso
- Ciberocupación
- Typosquatting
- Robo y suplantación de identidad
- Pornovenganza
- Spamming

# CAPÍTULO III

# 3 El Ciberbullying

## 3.1 Definición del bullying y ciberbullying

Para poder hablar del ciberbullying, primero tendré que explicar el bullying en sí.

El bullying es el acoso físico o psicológico realizado hacia un menor de edad. Este acoso es continuo y la finalidad del mismo es intimidar, dañar, humillar y amenazar a la víctima, con el fin de provocarle temor y para poder sentirse superior a él. El bullying se puede dar en cualquier lugar, aunque en la mayoría de casos siempre se presenta en un entorno escolar, ya sea llevado dentro o fuera de la institución, y comienza con una burla o broma, y va escalando cada vez más hasta terminar en una forma de acoso preocupante.

Este acoso, en la mayoría de los casos, termina causando perjuicios en la víctima, tales como:

- Ansiedad
- Depresión
- Irritabilidad
- Alteración del sueño
- Pensamientos destructivos

Por último, existen diferentes tipos de bullying, entre ellos se encuentran el bullying verbal, físico, social, sexual, y ciberbullying sobre el cual estaré hablando

Como antes mencione, normalmente el bullying se da en un entorno escolar, pero con el avance de la tecnología cada día vemos más y más niños que poseen acceso a las redes, y muy pocas veces (o nunca) están siendo supervisados por un adulto. Es así como niños realizan ciberbullying a otros, maltratándolos o humillándolos mediante la publicación de fotos, textos, imágenes, videos o audios en redes sociales, ya sean como Twitter, Instagram, Facebook, o incluso al momento de jugar videojuegos en línea, los cuales cuentan con chat de voz. La

consecuencia de usar estos medios para llevar a cabo este tipo de acoso, es que la dispersión de lo publicado se da a una gran escala, y es casi imparable una vez ya publicado.

Tomemos en cuenta por ejemplo el caso del video del chico que decía gustarle el arte, que en 2014 se hizo tendencia. En una reciente nota hecha en el año 2020[4] Juan Sánchez explico como él no fue afectado demasiado por el ciberbullying que le fue hecho producto del video viral, pero si menciono que necesito mucha protección por parte de su madre y también de un psicólogo. Además de esto, el en su momento al tener 13 años no tenía demasiado acceso a la internet, pero esto fue gracias a la protección de la madre, la cual es una protección que hoy en día no se ve mucho.

## 3.2 Características del Ciberbullying

- **Viralización:**

Al ser niños y niñas quienes perpetúan el acoso, estos no poseen la suficiente conciencia respecto al alcance que puede llegar a tener una publicación en una red social. Estos pueden ser compartidos o guardados (mediante captura de pantalla, por ejemplo), y así se expande el contenido a un número creciente de personas. Esta viralización causa un perjuicio grave en la víctima, ya que además de sufrir por la humillación causada, sufre por la viralización de la misma.

- **No hay derecho al olvido[5]:**

El derecho al olvido hace referencia a la facultad de una persona de solicitar que cierta información personal publicada sea borrada de las redes. Sin embargo, al estar hablando de un medio de comunicación tan masivo como lo es la internet, cierta cosa realmente no existe, ya que si una persona ya guardo la publicación esta seguirá compartiéndose, tal como en el caso del chico "*me gusta el arte*", cuya familia había pedido se dé la baja del video subido a YouTube, cosa que ocurrió, pero al ser compartido y guardado esto realmente no se pudo llevar a cabo, y esto hace que el sufrimiento de la víctima continúe indefinidamente.

- **Diversos dispositivos para perpetua el acoso:**

El ciberbullying se puede realizar a través de distintos medios electrónicos, ya sea por llamadas, correo electrónico, mensajes, redes sociales, y juegos online también.

- **Falsa sensación de anonimato:**

[4] https://www.youtube.com/watch?v=2Euu1GYMACc

[5] https://abogados.com.ar/derecho-al-olvido-por-primera-vez-en-la-argentina-la-justicia-lo-aplico-en-una-demanda-contra-google/26706

Al poder tener un nombre de usuario diferente al nombre real en muchas redes sociales, esto lleva a que gente que normalmente no acosaría a otros, a hacerlo en las redes, escondiéndose detrás de la pantalla y hostigando a otros. El problema de esta sensación de anonimato, es que además de que personas que no acosarían a otros en persona lo hacen online, estas piensan que hay una minimización de la agresión, ya que no pueden ver el efecto que causan en otros. Esto puede observarse muy seguido entrando a cualquier hilo de Twitter.

## 3.3 ¿Quiénes están involucrados?

En el bullying hay 2 involucrados, el acosador (quien debe ser un niño, sino estaríamos hablando de ciberacoso y no de ciberbullying) y la víctima (quien también es un menor), pero en el ciberbullying nos encontramos con un tercer sujeto, el cual es el espectador.

Los espectadores son quienes ven el acoso y la humillación desde afuera, y en la mayoría de casos estos no denuncian el acoso dado que se ven amenazados por las actuaciones del acosador, aunque cuando hablamos de ciberbullying, los espectadores suelen tomar mayor complicidad, dado a que estos alimentan el acoso compartiendo las publicaciones, y así implicándose de forma directa o indirecta en el acoso.

## 3.4 ¿Cómo detectamos un caso de ciberbullying?

Las víctimas de ciberbullying suelen mostrar cambios en su conducta, los cuales principalmente son la tristeza, depresión o agresión en casa, así también sufriendo en el ámbito escolar al conseguir un peor rendimiento. También suelen estar muy apegados a los dispositivos móviles, chequeándolos a cada instante para mantenerse al día sobre las publicaciones que hacen sobre ellos en las redes sociales. Además, las victimas suelen querer estar a solas en sus habitaciones.

## 3.5 ¿La ley habla del ciberbullying?

La ley no habla del ciberbullying en forma expresa, pero el menor de edad que sufre de este tipo de acoso está protegido por la **Ley de protección integral de los Derechos de las niñas, niños y adolescentes**, la cual en su artículo 9 estipula el "***derecho a la dignidad y a la integridad personal***". Este artículo estipula que, como sujetos de derecho y personas en desarrollo, los niños tienen derecho a un trato digno, sin tener que ser sometidos a un trato violento, discriminatorio, vejatorio, humillante e intimidatorio entre otras cosas. Por último, este artículo establece que "*Los Organismos del Estado deben garantizar programas gratuitos de asistencia y atención integral que promuevan la recuperación de todas las niñas, niños y adolescentes*"

Así que, ¿dónde podemos encontrar esta asistencia contra un caso de ciberbullying?[6]

El Gobierno de la Ciudad de Buenos Aires ofrece una línea mediante la cual denunciar casos de ciberbullying, brindando así asistencia gratuita a la víctima y familia de la víctima. El equipo detrás de esta línea y encargado de brindar ayuda en estos casos es el equipo de la Secretaria de Derechos Humanos (llamando al 102)

# CAPÍTULO IV

# 4 Ciberocupación

## 4.1 El DNS

El Sistema de nombres de dominio (Domain Name System) cumple la función de asociar cada dirección IP (el cual es el conjunto numérico que posee cada dispositivo conectado a la internet) con un nombre, el cual servirá para poder ingresar a esa IP sin tener que escribir cada número correspondiente a la misma. En palabras más simples, un dominio de internet es un nombre único que se utiliza para identificar de manera simple un sitio web cuando otras personas realizan una búsqueda desde su navegador.

Por ejemplo, cuando uno quiere dirigirse a la página principal de Google, normalmente lo que se escribe seria *www.google.com.ar*, eso sería el nombre de dominio, en el caso de no existir estos, uno tendría que escribir la IP para poder dirigirse a la página deseada, el cual en este caso es 8.8.8.8. en este caso es un número relativamente simple, pero normalmente se usan una mayor cantidad de números para otras páginas.

Sin el sistema de nombres de dominio, además de que tendríamos que ingresar número por número de cada IP, habría un número limitado de páginas web al que ingresar, ya que muchas veces las direcciones de IP se comparten en varios dominios por usar el mismo servidor, es así como el DNS logra compartir una misma IP con varios dominios.

Por último, la función más importante que cumple el DNS es la de un sistema registral, ya que hace posible la inscripción de nombres a equipos conectados a internet, asignándoles un dominio de nivel superior. En cada país hay diferentes organizaciones destinadas a manejar este sistema registral de dominios, y en la Argentina el encargado de esto es NIC Argentina (Centro de Información de la Red para Argentina), el cual es una oficina dependiente de la Secretaria Legal y Técnica de la Presidencia de la Nación.

[6] https://www.buenosaires.gob.ar/noticias/que-hacer-ante-un-caso-de-bullying#:~:text=Ante%20un%20caso%20de%20acoso%20llam%C3%A1%20al%20102

Las dos funciones que cumple NIC Argentina son:

- Permitir el registro de nombres de dominio en la Argentina
- Asegurar el funcionamiento del DNS para el dominio de nivel superior geográfico (Este dominio de nivel superior es la parte que vemos al final de cada nombre de una web, por ejemplo **.com o .net**, en este caso el dominio de nivel superior geográfico es el que se usa para cada país en específico, en este caso sería el **.ar**)

## 4.2 ¿Cómo se registra un dominio?

Según NIC Argentina, para poder registrar un dominio es necesario contar con el número de CUIT/CUIL y Clave Fiscal Nivel 2 o superior, esto sirve para poder saber quién es titular de cada nombre de dominio. Cabe aclarar que no solo las personas físicas pueden registrar su dominio, sino que las personas jurídicas también, pero estas lo hacen a través de sus representantes o un apoderado.

Luego de haber creado una cuenta con el número de CUIT/CUIL y Clave Fiscal, ya se podrá buscar el nombre de dominio que la persona desea registrar, el cual deberá estar disponible (lo cual la pagina indica). Una vez ya creado el dominio, lo único que faltará será delegar el dominio. Este es el proceso de configuración del nombre de dominio para poder asociarlo al servicio de hosting (la cual es servicio donde se almacenan la información que estará dentro de la página a crear).

## 4.3 Vencimiento del dominio

El artículo 24 de la resolución 20/2014 de la Dirección Nacional del Registro de Dominios de Internet estipula que el registro de un nombre de dominio tendrá una validez de 1 año, computado a partir de la fecha de su registración, pudiendo ser renovado en forma periódica. En caso de que pase el periodo de un año sin renovar el dominio, la ley otorga un periodo de gracia durante los primeros 30 días posteriores a la fecha de vencimiento durante los cuales el servicio no se encontrara disponible, pero el usuario no perderá la titularidad del dominio. El titular del dominio puede realizar el trámite de renovación 30 días antes de su vencimiento y hasta el último día del periodo de gracia.

En caso de pasar este periodo de gracia sin haberse registrado el dominio, este quedara disponible para ser registrado por cualquier individuo. Es aquí cuando nos encontramos con la figura de la ciberocupación (también conocida como Cybersquatting).

## 4.4 La Ciberocupación en sí

La ciberocupación es una conducta antijuridica no tipificada, la cual podría bien enmarcarse en el grupo de delitos en materia de marcas. Este es un proceso mediante el cual se busca registrar un nombre de dominio idéntico (**CIBEROKUPA**) o similar (**TYPOSQUATTING**) al de la marca de un producto o de una empresa.

La finalidad que tiene el sujeto que registra un dominio de mala fe puede ser (como en la mayoría de casos) para extorsionar a la empresa titular de la marca con el fin de venderle su dominio o bien para vender dicho dominio a la competencia. También hay casos en los que se okupa un dominio con el fin de usar la dirección para vender productos, para engañar a los usuarios que visiten el sitio haciéndose pasar por la empresa titular del dominio, o para llenarla de publicidad y generar un ingreso rápido.

Como podemos ver, el sujeto pasivo de este delito no es solo el dueño del dominio, sino que también pueden terminar siéndolo los consumidores de dicho sitio.

Como no hay ley alguna que regule el robo de nombres de dominio, NICar habilita a sus usuarios a iniciar un descargo de disputa. Este trámite permite a cualquier persona física o empresa reclamar para si la titularidad de un dominio que fue registrado previamente por otro usuario, siempre que tenga un mejor derecho sobre el mismo. Una vez iniciado el trámite, el individuo que tenga la titularidad actual del dominio tendrá 10 días hábiles administrativos para realizar su descargo. Este plazo empieza a correr a partir del primer día hábil posterior al de la notificación de inicio del trámite de disputa. El mismo podrá ser prorrogado por única vez y de forma excepcional por 10 días más siempre que existan circunstancias que lo justifiquen.

Luego de un plazo de 60 días (o mayor dependiendo de la complejidad de cada caso) se realizará la resolución de la disputa del dominio. En caso de no obtener una resolución favorable, el reglamento de Procedimientos Administrativos (decreto 1759/72) establece la posibilidad de presentar un recurso de reconsideración y un recurso jerárquico, dentro de los plazos improrrogables dispuestos (10 días para los recursos jerárquicos, y luego de los 10 días, 5 para los recursos jerárquicos, desde notificada la resolución).

En el caso de haber perdido la titularidad de un dominio a través de un descargo de disputa no se podrá realizar un nuevo trámite para recuperarlo, dado que Nic Ar establece que solo se puede iniciar un trámite de disputa entre las mismas partes y por el mismo dominio.

## 4.5 Como evitar caer en la trampa del Cybersquatting

No se puede garantizar que no vayamos a sufrir algún ataque de este tipo en algún momento, ya que como plantee en la introducción, las formas de realizar estos ataques varia y evoluciona con el paso del tiempo, pero si hay algunos recaudos que se puede tener en cuenta al momento de entrar a una página, tales como:

- **Contratación de agente que renueve el dominio**: En muchas empresas es común contratar a alguien que renueve el dominio web al estar cerca de su vencimiento.

- **Tener software de seguridad de internet actualizado**: Es crucial que el antivirus este actualizado, ya que este recopila archivos dañinos y páginas que pueden vulnerar el sistema del usuario y al mantenerlo al día se evitan estos ataques.

- **Escribir la URL donde uno quiere entrar manualmente**: Como mencione, en el caso del TYPOSQUATTING se hace una página con una URL muy similar a la de la página original, y se copia también el contenido de la página con el objetivo de robar información de quien caiga en la trampa (también conocido como phishing).

- **No abrir mails de dudosa procedencia**: Es recomendado siempre chequear el remitente del mail en cuestión, muchas veces el nombre del contacto de la persona que envía el mail dice ser por ejemplo “Correo Argentino” pero al inspeccionarlo vemos que es un spam. También es necesario corroborar que el hipervínculo adjuntado en el mail nos redirija a la página oficial a la que queremos ingresar, es por esto que siempre se recomienda ingresar el URL manualmente en el buscador

## 4.6 Jurisprudencia

Existen muchos casos sobre Cybersquatting y el más reciente en la argentina ocurrió en abril del 2021, cuando un joven argentino llamado Nicolas David Kuroña vio que el dominio de Google.com.ar estaba disponible y lo compro. La página estuvo caída durante varios minutos sin posibilidad de acceder a la misma porque se había vencido el dominio, y en el registro oficial de sitios web del país aparecía el nombre de este joven quien había comprado la titularidad de la URL. ¡Dentro de la página de Nic Argentina salía la leyenda “! Ufa! el dominio no está disponible” y por debajo en la razón social de la compañía aparecían los datos del nuevo dueño.

En redes sociales, Nicolas Kuroña aseguraba haber comprado el dominio de forma legal y que pudo hacerlo porque se venció el dominio.

Posteriormente en la cuenta de Twitter de Dominios Argentinos explico que el dominio no estaba vencido y que el mismo vencía el 8 de julio, por lo que alguien habría transferido el dominio u ocurrió un error en la página de Nic Argentina, hasta el día de hoy no se sabe que fue lo que ocasiono esto.

# CAPÍTULO V

# 5 Robo de identidad

## 5.1 Concepto de identidad

Desde el momento de su nacimiento, toda persona tiene derecho a obtener una identidad. La identidad incluye el nombre, el apellido, la fecha de nacimiento, el sexo y la nacionalidad. Es la prueba de la existencia de una persona como parte de una sociedad y es el conjunto de rasgos propios de un individuo que lo caracteriza y lo diferencia de los demás.

Esta puede ser extendida a través de la identidad digital, la cual se expresa y transmite a través de los diferentes medios electrónicos existentes. A modo de ejemplo, podemos encontrar como datos de identificación personal el nombre, apellido, documento de identidad, números o códigos de cuentas y servicios, contraseñas, datos biométricos, firmas digitales, etc.

La identidad a su vez, resulta ser un derecho personalísimo. Los derechos de la personalidad o personalísimos son derechos subjetivos privados, innatos y vitalicios que tienen por objeto manifestaciones interiores de la persona y que, por ser inherentes, extrapatrimoniales y necesarios, no pueden transmitirse ni disponerse en forma absoluta y radical. Se dijo también de ellos que eran plurales derechos subjetivos privados, que constituían una especie de los derechos humanos, clasificados y enunciados no de un modo cerrado y taxativo, sino como manifestaciones de las personas que dan cabida a otras, a medida que se van presentando las condiciones para su reconocimiento.

El derecho a la identidad en sí, se encuentra amparado en el artículo 24 del Pacto Internacional de Derechos Civiles y Políticos, en el artículo 18 de la Convención Americana sobre Derechos Humanos, en los artículos 7 y 8 de la Convención sobre los Derechos del Niño y, por último, en los mencionados tratados internacionales que poseen jerarquía constitucional, a través de la Constitución Nacional en su artículo 75 inc. 22.

- El Art. 24 del Pacto Internacional de Derechos Civiles y Politicos establece que "*Todo niño tiene derecho, sin discriminación alguna por motivos de raza, color, sexo, idioma, religión, origen nacional o social, posición económica o nacimiento, a las medidas de protección que su condición de menor requiere, tanto por parte de su familia como de la*

*sociedad y del Estado*" "*Todo niño será inscrito inmediatamente después de su nacimiento y deberá tener un nombre.*" "*Todo niño tiene derecho a adquirir una nacionalidad*"

- El art. 18 de la Convención Americana sobre Derechos Humanos establece "*Toda persona tiene derecho a un nombre propio y a los apellidos de sus padres o al de uno de ellos. La ley reglamentará la forma de asegurar este derecho para todos, mediante nombres supuestos, si fuere necesario*"
- Y, por último, la Convención sobre los Derechos del Niño en su Art. 7 establece que los niños tendrán derecho desde su nacimiento a un nombre y a adquirir una nacionalidad, así como el Art. 8 establece que "*Los Estados Partes se comprometen a respetar el derecho del niño a preservar su identidad, incluidos la nacionalidad, el nombre y las relaciones familiares de conformidad con la ley sin injerencias ilícitas*"

## 5.2 Que es el robo de identidad

El robo de identidad ocurre cuando alguien se apropia de la identidad de otra persona, haciéndose pasar por esta con el fin de cometer algún otro delito (como, por ejemplo, comprar con tarjetas ajenas, acceder a cuentas de banco con sus datos, escribirles a conocidos de la persona por la que se hace pasar para engañarlos y robarles, entre otras)

Además de las implementaciones económicas de este delito, la persona que se hace pasar por otra también puede tener otros fines, por ejemplo, la creación de perfiles falsos con el nombre de una persona, haciéndose pasar por ella para calumniarla, difamarla o afectar a terceros; Utilizar la identidad de un menor de edad para acosar a otros menores; Hacerse pasar por la otra persona si es arrestada; Usar su seguro médico; Divulgar imágenes privadas; Amenazas y extorsión; Sacar información de una empresa competidora, entre otros.

Actualmente la suplantación de la identidad avanza a grandes pasos en la Argentina, dada su falta de regulación. A esto hay que sumar el aumento de las bases de datos de empresas que comparten y venden información privada sobre las personas. Esto permite a los autores conseguir información con mucha más facilidad.

Si bien a través de la ley 26.388 se encuentra tipificado el indebido acceso a un sistema informático o dato restringido (art. 5 de la citada ley), se deja afuera otras formas de robo de identidad, donde el delincuente no accede a una cuenta ya existente para hacerse pasar por la víctima, sino que crea una cuenta o perfil nuevo (suplantación de identidad), utilizando datos como fotos, nombre y apellido, DNI, entre otros, con el fin de que el perfil sea creíble y poder realizar otros delitos como los antes mencionados.

## 5.3 Proyecto de ley

A través del proyecto de ley N° S-2630/18, presentado el 1/8/18 por la senadora Lovera, se busca agregar una pena al delito de robo de identidad al código penal. El mismo busca crear un Art. 139 ter que establezca lo siguiente:

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

Además, la pena será de 1 a 4 años en los casos en los que se realizare de forma continuada y con vocación de permanencia, o si la identidad creada, transferida o utilizada fuere de un menor de 18 años.

Asimismo, el 27/7/18, la diputada nacional Burgos a través del proyecto de ley N° 3868-D-2018 propuso incorporar al Código Penal un articulo 139 ter. Que reprime con prisión de 6 meses a 2 años al que "*suplantare o se apoderare de la identidad digital de una persona humana sin su consentimiento, a través del uso de su nombre, apellido, foto o imagen, o cualquier otra característica que indefectiblemente la identifique como tal, utilizando para tal fin las Tecnologías de la Información y la Comunicación, con la intención de cometer un delito o causar un perjuicio a la persona cuya identidad se suplanta o a terceros.*". En este caso, la pena también seria de prisión de 1 a 4 años en los casos en los que se realizare de forma sostenida en el tiempo o de modo tal que obligue a la víctima a alterar su proyecto de vida, o en los casos en los que la identidad creada, apropiada o utilizada fuere de un menor de 18 años.

Por último, otro proyecto de ley presentado respecto al robo de identidad es el presentado por el Senador Pichetto el 19/7/18, proyecto N° S-2449/18) propone agregar un artículo 138 bis al Código Penal, el cual pena con 1 mes a 1 año de prisión, o una multa de $20.000.- a $200.000.- , a quien "*Usurpare la identidad de una persona a través de Internet, redes sociales, o cualquier otro medio virtual*." En este caso no hay un agravante para el caso de menores, sino de figuras públicas el cual busca establecer que la pena sea agravada de 6 meses a 2 años de prisión, o una multa de $40.000.- a $400.000.-

En todos los casos en que se presentan estos proyectos de ley buscando penalizar el robo de identidad, los fundamentos en general, comparten la preocupación por el rápido avance y crecimiento de los supuestos de robo de identidad y suplantación de identidad, y la falta de una respuesta legislativa adecuada, y hablan de que el robo de identidad siempre es utilizado como herramienta para cometer otros delitos aún más graves como los anteriormente mencionados.

## 5.4 Jurisprudencia

Uno de los casos más conocidos y recientes de robo de identidad ocurrió el 15/7/20, cuando las cuentas de famosos como Bill Gates, Jeff Bezos o Elon Musk fueron hackeadas. En todas las cuentas se había publicado un mensaje, haciéndose pasar por el dueño de la cuenta, diciendo "Estoy devolviendo a la comunidad. ¡Todo el bitcoin enviado a esta dirección les será devuelto con el doble! Si tu envías $1000, yo devolveré $2000. Solo estaré haciendo esto por 30 minutos". Si bien estamos frente a un caso de Hacking frente a la ley 26.388 (Art. 5), también estamos frente a un caso de robo de identidad, como bien hemos dicho antes, la persona que realiza el delito se está haciendo pasar por otra con el fin de engañar a otros haciéndolos creer que es el, con el fin de cometer otros delitos más graves. En total 14 famosos fueron hackeados (Kanye West, Elon Musk, Bill Gates, la cuenta de apple, Cash app, Uber, Mike Bloomberg, Jeff Bezos, Joe Biden, Warren Buffett, Wiz Khalifa, Barack Obama, Mr Beast y Floyd Mayweather).

Al ver que esto es twitteado por varios famosos uno podría llegar a dudar y pensar que tal vez no es un intento de Scam, más porque quien realizo el tweet puso que había un plazo de 30 minutos por el que podrían enviar dinero, dejando poco tiempo para poder darse cuenta de que esto no es real. La billetera de la persona quien realizo los hackeos y el robo de identidad, según esta página habría recibido casi $300 mil dólares en bitcoin.

## 5.5 Derecho Comparado

En Estados Unidos, el robo de identidad se encuentra regulado en el 18 U.S CODE § 1028 como un delito federal (esto en el caso de que el robo de identidad se haga en un estado, y la persona que roba la información este en otro). Según el código citado, el robo de identidad ocurre cuando alguien utiliza la información personal de otra persona con un fin de ganancia económica o para suplantar la identidad de otra persona, y estas ofensas federales suelen estar acompañadas de fraude, mentiras (deception), hechos falsos o representaciones falsas. El código de USA diferencia la información personal de la económica. En los casos de robo de información de identificación personal, esta puede incluir el Social Security Number, numero de licencia de conducir, número de identificación personal, entre otros.

La mayoría de casos que involucran robo de identidad en USA son procesados en la corte criminal del estado (State Criminal Court). En casos de robo de identidad federal, el gobierno solo se involucrará si alguien roba grandes cantidades de dinero, o usa múltiples identificaciones para cometer otros delitos.

La persona encontrada culpable de cometer el delito federal de robo de identidad involucrando la producción o transferencia de identificaciones, falsificación de identifaciones, o si la persona culpable poseyera equipo para producir documentos, las penas incluyen hasta 15 años en prisión federal, y grandes multas.

En el caso de ser encontrado culpable por robo de identidad con el fin de traficar drogas, o que el robo de identidad esté conectado a un crimen violento, o en los casos que el culpable ya haya sido procesado por un robo de identidad, las penas pueden incluir hasta 20 años de prisión.

Por último, en los casos de que el robo de identidad sea realizado con el fin de cometer o ayudar a cometer terrorismo nacional o internacional, las penas podrían incluir prisión de hasta 30 años.

# CAPÍTULO VI

# 6 Pornovenganza

## 6.1 Definición

Como ya he mencionado anteriormente, el desarrollo de las nuevas Tecnologías de la información (TIC) conlleva a nuevos medios de difusión de información. Es así como los espacios cibernéticos relacionados a la intimidad sexual cuentan con muchísimo más contenido que nunca.

La pornovenganza (también conocida como “revenge porn”, concepto utilizado en Estados Unidos, aunque en el sentido original del término se limitara al envío de textos, ya que en el lenguaje anglosajón “sex” significa sexo y “texting” envío de mensajes de texto vía SMS) consiste en la difusión no consentida de imágenes o videos íntimos a través de las redes sociales o sitios web (las más usadas siendo foros de internet, WhatsApp, Snapchat, Instagram, Twitter, Telegram, Etc.). El problema con la pornovenganza es que para la obtención de dicho contenido por parte de quien lo publica, suele ser en un marco de novios, parejas, exparejas, y hoy en día también se encuentra facilitado por el sexting o los nuevos medios de difusión de contenido creado por uno mismo (como por ejemplo “only fans” o “cafecito”). La pornovenganza se produce incluso en los casos en los que para obtener el contenido hubiere existido un acuerdo entre las partes involucradas.

El Centro de Estudios en Libertad de Expresión y Acceso a la Información ha definido a la pornovenganza como “La publicación o puesta a disposición, o la amenaza de hacerlo, al público en general o de terceros en particular, de forma deliberada, utilizando la internet u otra tecnología de la comunicación de imagen/es, o audio/s o contenido/s audiovisuales de naturaleza sexual explicita, sin el consentimiento de la víctima, por parte de un individuo con el que esta estuviera manteniendo una relación íntima”.

Actualmente se suele denominar a la pornovenganza como la “difusión no consentida de material intimo” ya que al eliminar el termino de “Venganza” se amplió la figura ya que no se considera únicamente aquellas situaciones donde el sujeto activo actúa por venganza o donde las partes tenían una relación previa, sino que también se expande a terceros no relacionados con el hecho en si de la captación original de la imagen. Si bien como mencionamos, el contenido normalmente es difundido por ex parejas quienes estuvieron involucrados en la generación de esas imágenes o videos, también se pueden dar casos de hackers quienes vulneran sistemas de seguridad y de datos, aunque en estos casos si estaríamos frente a un delito enmarcado en el código como “hacking” previamente mencionado.

Este tipo de delito adopta las características propias de la internet, siendo el ataque personalizado y, al mismo tiempo, masivo. Masivo debido a su difusión, pero no solo eso, sino que también es masivo debido a los participantes del mismo, ya que estos luego ayudaran con la distribución del contenido. A su vez, la pornovenganza hoy en día está siendo cada vez más vista, esto se debe también a sitios web que distribuyen contenido sexual, en los cuales denominan videos bajo la etiqueta de “*revenge porn*”, y este contenido puede o no ser real, pero aun así termina generando el deseo de consumir más en la persona que utiliza estos sitios.

Entre los motivos por los cuales se lleva adelante esta práctica existen 3 grupos: El primero consiste en lucrar con las imágenes de los afectados, el segundo en intentar extorsionar a la víctima para sacar provecho de índole económica o sexual, bajo la promesa de no divulgar y borrar la información, y en tercer lugar se puede llegar a buscar también humillar públicamente a la otra persona (el cual es el motivo más común).

También es importante destacar la diferencia entre la Pornovenganza y la Sextorsión, la cual también es muy popular hoy en día.

En el caso de la sextorsión la víctima es amenazada y extorsionada para obtener dinero u obligarla a hacer algo a cambio de no difundir las imágenes o videos íntimos. En cambio, en el caso de la pornovenganza no es requisito que exista amenaza o extorsión, o ganancia de algún tipo por parte de la persona que realiza el hecho delictivo, ya que el fin también puede ser degradar, hostigar o acosar a la víctima.

## 6.2 Derechos vulnerados

Al momento de realizar esta conducta, el derecho principalmente vulnerado es el que emana del artículo 19 de la Constitución Nacional. El artículo establece que “*Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe*”

Como podemos notar, el artículo citado establece un ámbito de autonomía personal, el cual no debería ser vulnerado por nadie a menos de que lo que uno haga afecte a terceros. La vulneración de dicho ámbito privado implica peligro para la intimidad de la persona.

Otro derecho que podemos encontrar vulnerado en el caso de la divulgación de este material sería el artículo 12 de la Declaración Universal de los Derechos humanos el cual establece que "*Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.*". Asimismo, el Pacto Internacional de Derechos Civiles y Políticos en su artículo 17 Inc. 1 establece que "*Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación*" y en su Inc. 2 "*Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.*".

La Convención Americana sobre los Derechos Humanos establece en su artículo 11 que toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad, nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, ni de ataques ilegales a su honra o reputación, y que toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques. Si bien este artículo titula la Protección de la honra y de la dignidad, la Corte Interamericana de Derechos Humanos ha expresado que su contenido incluye también la protección de la vida privada, concepto que comprende entre otros ámbitos protegidos, la vida sexual (Caso Masacres de Rio Negro c/ Guatemala. Excepción Preliminar, Fondo, Reparaciones y Costas). A su vez, el Tribunal Europeo de Derechos Humanos también ha determinado que el concepto de vida privada alcanza a la integridad física y moral de una persona, en consecuencia, incluye su vida sexual (European Court of Human Rights, case of X and Y versus the Netherlands, Judgment of 26/3/1985).

Por otro lado, nuestro Código Civil y Comercial abarca los daños contra la dignidad e intimidad, en sus artículos 51, el cual establece que la persona humana es inviolable y tiene derecho al reconocimiento y respeto de su dignidad, el articulo 52 habla sobre afectaciones a la dignidad, estableciendo que "*La persona humana lesionada en su intimidad personal o familiar, honra o reputación, imagen o identidad, o que de cualquier modo resulte menoscabada en su dignidad personal, puede reclamar la prevención y reparación de los daños sufridos*", y en su artículo 53 el código defiende el derecho a la imagen, estipulando que para captar o reproducir la imagen o la voz de una persona, de cualquier modo, que se haga, es necesario su consentimiento, excepto en los casos taxativos que enumera la norma. Por último, el CCYCN en su artículo 1770 regula la protección de la vida privada, estableciendo que quien se entrometa en la vida ajena y publica retratos, difunde correspondencia, mortifica a otros en sus costumbres o sentimientos, o perturba de cualquier modo su intimidad, debe ser obligado a cesar en tales actividades, si antes no cesaron, y a pagar una indemnización que debe fijar el juez, de acuerdo a las circunstancias.

Además, a pedido de la persona agraviada se puede ordenar la publicación de la sentencia en un diario en el caso de que esta medida resulte procedente para una adecuada reparación.

Como podemos ver, podría llegar a haber una condena por delitos contra la intimidad o privacidad, pero no una por el delito de divulgación de fotografías sin consentimiento en sí por parte del derecho penal. Nuestro código penal no regula este hecho delictivo, si bien se podría llegar a alguna otra condena por otros delitos (en los artículos del 118 al 133 del código penal, delitos contra la integridad sexual, por ejemplo, en los casos en los que se involucran menores como en el ciberacoso o grooming), no habría condena por la distribución sin consentimiento de las imágenes en sí. También se puede llegar a encuadrar este delito bajo la imagen de delitos contra derechos intelectuales, de las injurias o por hostigamiento o chantaje (como en el caso de la sextorsión).

En el caso del derecho intelectual, se podría tomar este delito por el lado del articulo 155 del Código Penal, el cual sanciona con multa a quien "*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.*". El problema con el encuadre en este artículo es que el mismo no menciona la difusión de imágenes intimas de terceros. Además, el articulo 157bis reprime con la pena de prisión de un mes a dos años a quien "*A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;*" a quien "*Ilegítimamente proporcionare o revelare a otra información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.*" O a la persona que "*Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales*." (Articulo sustituido por el art. 8 de la ley 26.388). Este artículo tampoco hace mención a la difusión de imágenes intimas de terceros.

## 6.3 Proyecto de ley

Actualmente se encuentra presentado un proyecto de ley que busca la penalización de la publicación y/o difusión de imágenes no consentidas de desnudez total o parcial y/o videos de contenido sexual o erótico de personas. El proyecto de ley S-2119/16 busca incorporar un artículo 155 bis al Capitulo III del Título V del código penal, el cual es redactado de la siguiente manera "*ARTICULO 155 BIS: Será reprimido con la pena de prisión de seis (6) meses a cuatro (4) años, el que hallándose en posesión de imágenes de desnudez total o parcial y/o videos de contenido sexual o erótico de una o más personas, las hiciere pública o difundiere por medio de comunicaciones electrónicas, telecomunicaciones, o cualquier otro medio o tecnología de transmisión de datos, sin el expreso consentimiento de la o de las mismas para tal fin, aun*

*habiendo existido acuerdo entre las partes involucradas para la obtención o suministro de esas imágenes o video.*". Como podemos observar, el presente articulo busca sancionar estos actos delictivos demandado una normativa específica para su penalización. Se incluye una pena de prisión, y se penaliza la divulgación del contenido sin el consentimiento de la otra persona aun haya existido algún acuerdo entre las partes para obtener ese material.

El 23 de julio del 2020 el Senado de la Nación dio sanción a un proyecto de ley para regular la difusión no consentida de imágenes intimas. Dicha sanción paso a la Cámara de Diputados, pero luego no fue sometido a debate parlamentario. En una entrevista con ANCCOM, Martina Benitez Demtschenko dijo que "*Técnicamente, todos los proyectos son espantosos, adolecen de falencias que son preocupantes y terminan siendo muy desprotectores en el caso en que se conviertan efectivamente en ley. Lo que no se tuvo en cuenta a la hora de redactar estos proyectos, es que, en este tipo de delito, se requiere de una inmediatez absoluta y que no puede ser tratado de la misma manera que la violencia física; el contenido es imposible de bajar de la web, el agresor es omnipresente y existen otros agresores potenciales que son quienes difunden el material.*" Razón no le falta al decir que este es un hecho delictivo el cual debe ser tratado con inmediatez, pero debido a la rápida difusión del material y a la sencilles de la difusión de datos de la internet esto es casi imposible. En mi opinión, debería haber un ente del estado el cual atienda este tipo de consultas por medio online y pueda dar de baja con rapidez el material subido a sitios web.

## 6.4 Como evitar que ocurra

Existen varias precauciones que uno puede tomar a la hora de sextear o subir fotos intimas a redes, entre ellas la más efectiva es enviar las imágenes en los modos efímeros de algunas de las aplicaciones que poseen esta característica (por ejemplo Snapchat o el chat privado de Instagram, uno puede enviar una foto con la opción de que esta pueda ser abierta y vista solo una vez, y en caso de que la otra persona tome una captura de pantalla, quien envio la foto obtendrá un aviso, sabiendo así que la otra persona no es de confiar). También se debe tomar como recaudo tratar de no compartir imágenes de este tipo con gente que no se conoce del todo bien, y en caso de que se vaya a enviar una de estas imágenes, tratar de evitar que no salga la cara o cualquier otro rasgo que pueda identificar a la persona (como tatuajes). Las historias de Instagram también pueden capturarse y compartirse sin consentimiento, y se puede capturar imágenes de redes sociales o servicios que no permitan esta característica teniendo otro celular con el que se saca las fotos. Como ultimo recurso, el art 16 de la ley de Protección de Datos Personales (ley 25.326) establece varios supuestos en los que en casos que se divulgaran datos personales (guardados en archivos, registros, bancos de datos públicos o privados y que estén guardados para dar informes, o en este caso, imágenes o videos privados) se puede solicitar la baja de las fotos o los videos (similar al derecho al olvido que mencionamos previamente). Según

el inciso 2 de esta norma, el responsable de la divulgación de estos datos privados debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias dentro de un plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos. Cabe mencionar que, si bien la medida pide la baja de datos de la internet, no siempre es posible la eliminación permanente de estos.

## 6.5 Jurisprudencia

Si bien hay una gran variedad de casos en los que se da la pornovenganza en la argentina, el primer caso que fue llevado a juicio fue el de Paula Sanchez Frega, quien en 2017 en La Rioja llevo a su ex pareja a juicio por difundir sus videos y fotos intimas tras separarse. Su ex pareja, Patricio Pioli tatuador a quien conoció cuando fue a tatuarse, fue procesado en el 2017 con prisión preventiva (con beneficio de excarcelación) por los delitos de coacción y lesiones leves calificadas, embargado por 30 mil pesos y enviado a juicio oral tras una causa en el Juzgado N°3 de La Rioja a cargo del magistrado Gustavo Farías. Paula conto que "*fue una relación toxica y conflictiva que duró 8 meses, lo conocí cuando me fui a tatuar al local de él. Iniciamos una relación y termino viviendo en mi casa.*", Empezaron a discutir por cualquier cosa según conto Paula, y además de daños psicológicos hubo lesiones físicas. Cuando Paula no pudo soportarlo más le pidió que fuera a vivir a otro lado en el 2016, pero Patricio Pioli no soporto la ruptura y tras ser abandonado empezó a amenazar de muerte a Paula y decidió viralizar por WhatsApp sus fotos y videos íntimos. Mientras los familiares y amigos de su ex usaban las redes para atacar a Paula, ella empezó a circular varios audios intimidantes que el tatuador le había enviado diciendo cosas como "*Te voy a hundir, te voy a destrozar la vida*" y "*Te voy a matar*".

Ante estos audios Paula no se amedrento y decidió recurrir a la Justicia presentado todas las pruebas que había recaudado, donde se consideró a Pioli culpable de los delitos de coacción, lesiones leves calificadas y por haber ejercido violencia de genero por filtrar fotografías y videos íntimos. Frente este caso la presidenta de la Asociación de Mujeres Penalistas de la Argentina (AMPA), explicó que, a diferencia del grooming, la sextorsión no está tipificada en el Código Penal, como si lo está en el Código Penal español, por eso la condena es por coacción.

Para los jueces quedo acreditado que todas las situaciones de violencia y hostigamiento hacia la victima provocaron en ella un daño psicológico, un daño o quiebre en su salud mental caracterizado por sensación de desamparo, desvalimiento y sensación de encontrarse en situación de peligro real, perdiendo la confianza y seguridad en sí misma.

Paula considero la condena de 5 años un fallo ejemplar para un caso de pornovenganza en el país. Además, la justicia ordenó en este caso destruir los objetos tecnológicos secuestrados, facilitadores de la difusión no consentida del contenido.

Según datos de la Asociación Argentina de Lucha Contra el Cibercrimen (AALCC), una ONG porteña dedicada a la materia que brinda talleres de capacitación a fuerzas de seguridad y cuenta con un gabinete psicológico para víctimas, las denuncias por difusión de material intimo se incrementaron en un 20% entre 2016 y 2018, mientras que las de sextorsión subieron un 35%. Cabe destacar que en los últimos 2 años desde el inicio de la pandemia por COVID 19, al no poder salir de casa como se habituaba, la gente recurrió más a las redes sociales, y el sexting estuvo más presente que nunca, acompañado esto también de más casos de difusión de material intimo sin consentimiento.

## 6.6 Derecho comparado

Al día de hoy, varios países regulan la pornovenganza como delito.

El primer país en penalizar la divulgación de imágenes intimas no consentidas fue Filipinas en el 2009 en el REPUBLIC ACT No. 9995. La ley en su artículo 2 estipula que el estado valora la dignidad y privacidad de cada persona humana, y garantiza el total respeto de los derechos humanos, y para este fin, el estado penalizara actos que destruyeran el honor, dignidad e integridad de una persona. Asimismo, la ley da varias definiciones de términos como “Broadcast”, “Capture” o “Under circumstances in which a person has a reasonable expectation of privacy” (bajo circunstancias en las que una persona tenga una razonable expectación de privacidad).

Asimismo, en el 2013 el Estado de Victoria en Australia penalizo también la pornovenganza, y luego en el 2014 Israel lo penalizo como delito a la integridad sexual, y a sus víctimas como víctimas de abuso sexual, modificándose la ley sobre acoso sexual e incluyendo penas de hasta cinco años de cárcel.

España también incorporo en su código penal esta figura, por medio de la reforma del 2015 en cumplimiento de la directiva 2013/40/UE. El artículo 197.7 del código penal español contempla en su primer apartado un tipo básico del delito contra el derecho a la propia imagen, castigando con una pena de prisión de 3 meses a 1 año o multa de 6 a 12 meses al que sin autorización difunda, revele o ceda imágenes o grabaciones audiovisuales de otra persona, que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros cuando la divulgación menoscabe gravemente la intimidad personal de esa persona. Por otro lado, en su segundo apartado se establecen tres agravantes, disponiendo que la pena se imponga en su mitad superior en los casos que a) Cuando quien cometiere el delito sea el cónyuge o por persona que este o haya estado unida a la víctima por análoga relación de afectividad, aun sin convivencia, b) cuando la víctima fuera menor de edad o una persona discapacidad necesitada de especial protección, y c) cuando los hechos se hubieran cometido con una finalidad lucrativa.

Entre otros países que penalizan la divulgación no consentida de contenido también se encuentran Japón, Estados Unidos, Canadá, Reino Unido, Nueva Zelanda, Alemania, México, Brasil, Perú y Puerto Rico.

# CAPÍTULO VII

# 7. Spamming

## 7.1 Abuso de sistemas de mensajería

El spam es un abuso que vemos en el día a día pero que no le damos la importancia la cual debería de ser dada. El spam es un delito que vulnera tanto el derecho a la privacidad (Por ejemplo, al vulnerar la libre elección de un consumidor) y el derecho a la intimidad el cual mencione previamente. La definición de correo Spam surgió en 1957 cuando la empresa estadounidense Hormel Foods lanzó al mercado un nuevo producto llamado “Spam” (diminutivo de “Shoulder of Pork Ham”), el termino de Spam comenzó a utilizarse en el mundo informático luego de un sketch de Monty Python’s en el cual había un restaurante cuya carta solo tenia productos a base de Spam, por lo que la camarera lo repetía de manera constante. Un grupo de vikingos leyendo la carta se dieron cuenta de que todo contenía Spam por lo que empezaron a repetir sin parar la palabra Spam, así asociando la palabra Spam con algo molesto.

El spam o Spamming es el abuso de cualquier medio de sistema de mensajes electrónicos mediante el cual una persona o una empresa genera correos electrónicos y los envía de forma masiva y repetida, con el fin de ofertar, comercializar o tratar de despertar interés respecto de un producto, servicio o empresa en el destinatario.

El Spam además de ser usado con fines comerciales, también puede ser utilizado para causar fraude, Scam, Phishing (Por ejemplo, en los casos en los que se envían varios mails diciendo ser de una red social por ejemplo “Facebook”, con asunto en el mail diciendo “te robaron la contraseña cámbiala”, de esta manera la persona al ver varios mails diciendo esto cederá ante el engaño), Pharming, entre otros delitos.

Hoy en día las empresas están obligadas a incluir un botón de desuscripcion a los mails abusivos, para así no recibirlos más, pero en caso de no presentarse dicho botón no existe una pena. Otra forma para evitar ser sujeto pasivo del Spam es marcar los correos indeseados como “correo no deseado” de esta manera los mails provenientes del mismo remitente irán a la casilla de correo no deseado, el problema con esto es que hoy en día varias empresas o personas que realizan el Spam, lo hacen desde cuentas Bots, a las cuales se le carga la base de datos con mails a los que enviar el mismo correo varias veces, de esta manera si uno marca la casilla de origen como correo no deseado, le llegara el mismo mail pero desde otra casilla de correo.

## 7.2 Primer caso de jurisprudencia argentina sobre Spam

El 7/4/2006 el juzgado civil y comercial federal Nro. 3 dictó la primera sentencia que trató el Spam en Argentina.

La demanda fue interpuesta por dos abogados especializados en el derecho informático (Dres. Pablo A. Palazzi y Gustavo D. Tanús c/ Carlos A. Copsa y Ana C. Magraner, con fundamento en el art. 43 de la CN (acción de amparo) y en la ley 25.326 (ley de protección de datos) en su artículo 27 más específicamente, el cual regula los bancos de datos y establece en su tercer inciso que el titular de los datos podrá en cualquier momento solicitar el retiro o bloqueo de su nombre de los bancos de datos al que se refiere el artículo. La acción fue iniciada a fin de obtener el acceso a los datos personales suyos, incluidos en las bases de datos que los demandados utilizaban para enviarles mensajes de correo electrónico no solicitado, también se pedía la eliminación de dichos registros y el cese de todo tipo de tratamiento de su información y bloqueo de toda dirección de correo electrónico vinculada con los actores. Los demandados bajo el nombre de la empresa "PUBLICC SOLUCIONES INFORMATICAS" se dedicaban a vender base de datos que contenían información personal de terceros, además de direcciones de correo electrónico con el fin de hacer publicidad de forma masiva. Los demandados al momento de contestar demanda negaron que tuvieran a su cargo base de dato alguna y argumentaron que solo se limitaban a vender información sobre direcciones electrónicas de acceso público y gratuito orientado a fines publicitarios. En su alegato, explicaron que las direcciones de correo electrónico habían sido obtenidas directamente desde la internet, y que luego enviaban el correo y con el mismo método buscaban otros, escapando de la figura del spam y encuadrando su conducta en el Art. 5 Inc. 2 de la ley 25326, el cual establece que no es necesario el consentimiento cuando los datos se obtengan de fuentes de acceso público irrestricto. El magistrado entendió probada la existencia de una base de datos por parte de los demandados, y que estos a su vez transferían datos de manera onerosa y gratuita a través de internet, con referencias sobre conductas de consumo.

La sentencia no estableció condena por daños (dado a que estos no fueron pretendidos), y se dictó una medida cautelar para ordenar a los demandados permitir el acceso de los actores a sus propios datos, y que estos fueran retirados y bloqueados, siendo impuestas las costas de la demanda a cargo de las accionadas.

## 7.3 Derecho comparado

En Estados Unidos el Spamming se encuentra regulado por la CAN-SPAM Act del 2003 (Ley de Control de Asalto a la Pornografía y Comercialización No Solicitada), la cual establece requisitos

para quienes envían mails comerciales. La ley entro en vigencia el 1 de enero de 2004 y cubre principalmente los correos electrónicos que tienen el propósito de publicitar o promocionar un producto o servicio comercial. La ley a su vez no hace excepción de correos de empresa a empresa. Cada mail que viole la ley de CAN-SPAM Act puede ser sujeto de multa de hasta $46.517 dólares.

Entre los requisitos que establece la CAN-SPAM Act. se encuentran el no usar como asunto o encabezado del mail información falsa o engañosa. El remitente debe estar especificado de forma clara. Los mails deben indicar si el mismo es un anuncio. Se debe indicar a los receptores del mail la ubicación del remitente (ya sea código postal, la dirección de calle, un domicilio de correo físico, entre otros). El requisito más importante que introduce esta ley, es que el mail debe indicar en forma clara la forma en que los usuarios que lo reciban pueden desuscribirse (normalmente es un botón de tamaño pequeño que se encuentra debajo de todo el mail, así se dificulta encontrarlo). Por último, la ley obliga a que las compañías, en caso de que contraten a una persona para que maneje la casilla de correo electrónico, deben controlar los mails que salen de igual manera, porque en caso de no cumplir con los requisitos que esta ley establece la compañía será responsable.

# CAPÍTULO VIII

# CONCLUSIÓN

El objetivo principal de este trabajo es definir los delitos informáticos y explicar cuáles no se encuentran tipificados en la ley 26.388, ni regulados por otra ley en la ley argentina. Como mencione repetidamente en este proyecto, la informática avanza a pasos agigantados a medida que pasa el tiempo, y cada día pueden surgir más delitos nuevos sin ser tipificados. El problema se encuentra principalmente en que la comisión de los delitos mencionados en esta tesina no es penada como tal, sino que se los ve más como MEDIOS de comisión de otros delitos (por ejemplo, así como el SPAM se ve como un medio de cometer el delito de estafa o Phishing entre otros). Considero necesaria la regulación de los delitos enumerados y de un comité especial que se dedique a la tipificación de dichos tipos antijuridicos, dado el avance de la internet y de las TIC, esto debido a los derechos vulnerados en los delitos mencionados, como el derecho a la privacidad, al consumidor, a la dignidad e integridad personal, al honor, a la identidad, entre otros los cuales son derechos importantes que enmarca nuestra constitución y el derecho internacional. Además de la legislación, debe de introducirse la implementación de investigaciones y una forma de perseguir estos delitos, buscando así la manera de disminuirlos y tener cada día menos personas que busquen cometerlos, consiguiendo así la seguridad informática de los argentinos.

En síntesis, actualmente la legislación argentina no logra encuadrar en su totalidad los delitos informáticos, y con el avance de la tecnología estos son cada día más presentes, por lo que la normativa que encuadre estos temas debería ser actualizada y controlada de manera constante con suma prioridad.

- **BIBLIOGRAFÍA**


- MOISÉS BARRIO ANDRÉS, Ciberdelitos 2.0, 2ª edición actualizada y ampliada, Astrea,
- JULIO TÉLLEZ VALDÉS, Derecho Informático, cuarta edición.
- FEDERICO GARCIA VIDAL “Cibercrimen y Propiedad Intelectual” (CIBERCRIMEN I Daniela Dupuy. Mariana Kiefer. Ed. Bdef
- PABLO PALLAZZI. “Delitos informáticos en el Ccódigo Penal” Ed. Abeledo Perrot.
- PABLO PALLAZZI. “Delitos contra la intimidad informática” Ed. CDYT
- CRISTIAN BORGHIELLO – MARCELO TEMPERINI. “Suplantación de la Identidad Digital” (CIBERCRIMEN II Daniela Dupuy. Mariana Kiefer, Ed. Bdef
- FERNANDO TOMEO. “Redes y Tecnologias” ED. Astrea.
- GUSTAVO E. ABOSO “Ciberdelitos: Análisis doctrinario y jurisprudencial” Ed. El Dial
- PATRICIA ROCA DE ESTRADA. “Delito informático, virus y legislación” SAIJ