UNIVERSIDAD DE CHILE

FACULTAD DE DERECHO

DEPARTAMENTO DE DERECHO PROCESAL

USURPACIÓN DE IDENTIDAD EN LAS REDES SOCIALES: FACEBOOK Y TWITTER. TRATAMIENTO LEGAL Y JURISPRUDENCIAL EN CHILE.

Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales

NICOLE EDEN FERRADA BUBNIAK

FERNANDA JESUS INIESCAR MEDINA

Profesor guía: Alex Pessó Stoulman

Santiago de Chile,

2015

TABLA DE CONTENIDO

RESUMEN

El uso de Internet y las redes sociales se ha vuelto imprescindible en la vida cotidiana de los seres humanos, y por ello, se hace necesario que nos identifiquemos en el ciberespacio al igual que en el mundo real.

La extensión que hacemos de la identidad personal a un contexto digital, por lo general nos lleva a representarnos fielmente a nosotros mismos en este plano, sin embargo, y en virtud de la carencia de reglas que hay a este respecto en la Web, conduce a muchos a inventar un usuario ficticio, o simplemente a utilizar indebidamente la personalidad de otro.

Actualmente, el tipo penal de usurpación de nombre -establecido en el artículo 214 del Código Penal- no contempla la identidad como bien jurídico protegido ni que tal ilícito se dé en Internet y las redes sociales, por lo que en noviembre de 2014 se presentó el Proyecto de Ley que “modifica el Código Penal, con el propósito de sancionar la suplantación de identidad

realizada a través de Internet y redes sociales, ocasionando daños a terceros", con el fin de completar este vacío legal.

El presente trabajo busca determinar si es necesario este cambio en la legislación penal de nuestro país o si es suficiente la norma existente para amparar el derecho a la identidad personal, cuando el delito de usurpación de identidad se dé en un escenario informático. Para responder a esta interrogante, se esclarecerá en: los conceptos de identidad, persona y derecho a la identidad personal; se hará una relación expositiva del funcionamiento de las redes sociales y se ahondará en la naturaleza jurídica de las mismas. Se realizará una breve revisión de los delitos informáticos y del ilícito de suplantación de identidad, y su tratamiento normativo en el Derecho Comparado, asimismo, se analizará la fundamentación del Proyecto de Ley en cuestión, y la viabilidad de su aprobación. Y finalmente, se hará un estudio jurisprudencial de algunos casos de usurpación de nombre que se hayan presentado en el mundo virtual.

INTRODUCCION

En los últimos 30 años, Internet se ha posicionado como una de las herramientas más útiles para la sociedad, tanto así que hoy en día no se concibe la vida sin este medio. En la actualidad éste vive su apogeo, con las redes sociales como su máxima expresión, configurándose como un mundo propio, en el que los individuos pueden desarrollar de forma más amplia casi todos los aspectos de su vida, razón por la cual los mismos buscan construir la propia identidad dentro de estas plataformas, para así autodefinirse en este nuevo plano y poder ser reconocidos por los demás.

La autonomía que se le ofrece al usuario en el mundo virtual, ha permitido que éste pueda decidir entre múltiples opciones para representarse en el ciberespacio, ya sea extendiendo su propia identidad, creando una falsa, o bien, ocupando una ajena.

Respecto a este último punto se enfoca nuestro análisis, en cuanto el injusto de usurpación de identidad ha encontrado un nuevo nicho para

perpetrarse, creando nuevos desafíos que se ven exacerbados por el avance tecnológico que no hace más que moverse a pasos agigantados. En este sentido, el objetivo de esta investigación será responder si el Proyecto de Ley que "modifica el Código Penal, con el propósito de sancionar la suplantación de identidad realizada a través de Internet y redes sociales, ocasionando daños a terceros" es necesario, o si es suficiente el artículo 214 del mismo cuerpo normativo -donde se tipifica el delito de usurpación de nombre- para la protección de la identidad de aquellas personas que se ven afectadas por el uso indebido y no autorizado de la misma por terceros ajenos.

La Memoria que a continuación se desarrolla se esquematiza en seis capítulos, el primero de ellos pretende determinar qué entendemos por identidad -basado principalmente en el concepto de persona y su tratamiento en la legislación nacional-, e instituir un concepto de Derecho a la identidad personal –el que se construye desde la perspectiva de los derechos de la personalidad-.

El segundo capítulo hace referencia a la noción de identidad digital, cómo ésta se construye en Internet, y la correspondencia que tiene con los conceptos de “reputación” y “anonimato”, tan comunes en la Web. Además, comprende una relación expositiva del origen y funcionamiento de las redes sociales, más específicamente de Facebook y Twitter, y el análisis de la naturaleza jurídica que éstas detentan.

El tercer capítulo trata de la conceptualización, clasificación y caracterización de los delitos informáticos en general, y el tratamiento legal que se da a aquellos en el Derecho Comparado.

En el cuarto capítulo, y en virtud del examen de la figura penal clásica de la usurpación de nombre, se intentará explicar cómo se daría el delito estudiado en el contexto de las redes sociales, a través de la disección de los elementos para su configuración, y estableciendo cuál sería el bien jurídico a proteger por esta pretendida extensión del artículo 214 del Código Penal. Asimismo, se describirá el panorama internacional respecto al tratamiento legal del delito de usurpación de identidad y se analizará el Proyecto de Ley que “modifica el Código Penal, con el propósito de sancionar la

suplantación de identidad realizada a través de Internet y redes sociales, ocasionando daños a terceros", junto con el impacto que produce este injusto tanto en el mundo físico como en el virtual.

El quinto capítulo contiene una exposición de las políticas que Facebook y Twitter tienen para enfrentarse a la usurpación de identidad, y variadas propuestas para que el usuario pueda proteger la misma en la Red.

Y por último, el sexto capítulo comprende una revisión de diversos fallos emitidos por Tribunales chilenos que tratan sobre el ilícito de usurpación de nombre, cuando este delito de desarrolla en alguna red social.

CAPÍTULO I: IDENTIDAD: ASPECTOS GENERALES.

Con el fin de encauzar nuestro estudio sobre la usurpación de identidad en el contexto de las redes sociales, en el presente capítulo desarrollaremos las ideas de identidad personal y persona. Todo para establecer un soporte de conceptos claros que nos permitan el análisis de este delito en la era del Internet.

1. Qué es la Identidad

La identidad es un rompecabezas en el cual confluyen una gama diversa de cuestiones -filosóficas, psicológicas, socioculturales, entre otras- que se han tratado de resolver a lo largo de la Historia[1].

[1] Desde tiempos remotos, el hombre se ha cuestionado sobre el Sí Mismo, tratando de encontrar respuestas dentro de la religión, la filosofía, la psicología, entre otras ciencias, todo a través de diversas teorías sobre el yo, la interioridad, la conciencia de la persona humana, etc. El desarrollo de la idea de la identidad personal es un proceso que -según Giampiero Arciero en su libro "Estudios y diálogos sobre la identidad personal"- comienza con la aparición de la escritura, donde se abandona el sentido de conciencia colectiva, para repartirse ésta en cada uno de los que forman la generalidad

En la actualidad, la incógnita sobre la identidad personal se renueva, siendo su principal problema -determinado por las nuevas prácticas del mundo moderno- "la fragmentación del sentido de unidad personal, acompañada de la creciente velocidad y multiplicidad de las interacciones humanas"[2]. Lo cual, se evidencia con aún más claridad en el ámbito del Internet, en el que las plataformas de interacción que se han creado en el último tiempo -las famosas "redes sociales"- otorgan a las personas una clase extraña de libertad, donde cada uno puede crearse una identidad con el fin de identificarse en las mismas.

Para lograr el objetivo de esclarecer la noción de identidad, debemos simplificar de manera considerable todas estas perspectivas y enfocarnos en dar una aproximación del concepto de identidad personal que nos sirva a

---

como una interioridad individual. Este concepto evoluciona desde la antigua Grecia, pasando por la Edad Media y el Humanismo, hasta los tiempos contemporáneos, los cuales traen consigo nuevos desafíos e interrogantes que buscan respuesta sobre lo que es el Sí Mismo y la identidad personal.

[2] ARCIERO., G. 2005. Estudios y diálogos sobre la identidad personal: reflexiones sobre la experiencia humana. Buenos Aires, Amorrortu. p. 21.

futuro para lograr determinar si es posible que exista una usurpación de identidad en las redes sociales o no.

1.1. Concepto de identidad

Siendo la idea de identidad personal tan amplia como el espectro de doctrinas que la tratan de abarcar, y siendo aún un concepto en proceso de formación, debemos intentar construir una noción concisa que defina la esencia del ser humano, o sea, su identidad.

Como concepto universal, el diccionario de la Real Academia Española define la identidad como la cualidad de lo idéntico, el conjunto de rasgos propios de un individuo o de una colectividad que los caracterizan frente a los demás, o la conciencia que una persona tiene de ser ella misma y distinta de los otros[3].

[3] Diccionario de la real academia Española, concepto de identidad.

La identidad personal, entonces, la definimos como el conjunto de características de la persona que sirven para su individualización en la sociedad, su identificación como única y diferente de los demás.

Es importante destacar que la identidad personal, como conjunto de atributos únicos de la persona, estaría compuesta por dos factores determinantes; uno estático y uno dinámico.

La faceta estática de la identidad estaría definida por el aspecto genético de la persona, es decir, por las características biológicas propias y únicas de cada uno, sumado a ciertos elementos que contribuyen a la identificación del individuo, como lo es su nombre, su fecha y lugar de nacimiento, la filiación, entre otros, los cuales generalmente serían de carácter inmutable[4].

La dimensión estática, entonces, responde a la naturaleza humana de las personas, la cual sería una estructura fija, determinada y estable, común a

[4] COLLANTES S., C. y GONZÁLEZ G., C. 2001. Identidad personal, identificación e identidad genética. Memoria para optar a la licenciatura en ciencias jurídicas y sociales. Santiago, Universidad de Chile, Facultad de Derecho. Pp. 55-57.

todos los hombres, mas con la particularidad de ser única e irrepetible para cada ser humano, definiendo en parte nuestra identidad personal[5].

Por otro lado, la identidad en su dimensión dinámica responde a la construcción social del "yo", que es formada por las creencias, la cultura, la ideología, las peculiaridades de la personalidad, las experiencias de vida, entre otros elementos que confluyen para la constitución del individuo adulto perteneciente a un sistema social específico en una época determinada. Todos, factores que detentan una esencia variable[6]. Esto, en virtud, de que toda persona está "ordenada y capacitada a alcanzar mediante su obrar una mayor perfección"[7], lo cual revela que las personas no sólo se determinan por su estructura fija, sino también por el dinamismo del cual está dotada la vida. Presentando así al hombre como potencialidad en sí mismo, potencial de convertirse en quién quiere ser, siempre considerando que lo hará "en respuesta a los hechos exteriores de uno mismo"[8].

---

[5] HOYOS, C., I, M. 1990. La dimensión jurídica de la persona Humana. Bogotá. D.E., Colombia, Universidad de la Sabana. p.21.
[6] COLLANTES y GONZÁLEZ. Ob. Cit. pp. 55-57.
[7] HOYOS. Ob. Cit. p.22.
[8] APPIAH., A. 2007. La ética de la identidad. Traducido por Lilia Mosconi. Buenos Aires, Katz. p. 49.

El dinamismo del cual se encuentra dotada la naturaleza humana y, por tanto, la persona, presupone entonces la sociabilidad, que "es la vez tan natural, tan necesaria y tan habitual para el hombre (...), que de no ser por los lazos sociales que formamos (...) no podríamos llegar a ser un yo en absoluto"[9]. Lo que se suma al hecho de que "parte del material al que respondemos al dar forma a nuestro yo no está dentro de nosotros, sino en el exterior, inmerso en el entorno social"[10].

Es importante destacar que el aspecto social que influye en la construcción de la propia identidad, encauza a las personas a edificar el Sí mismo en los parámetros de ciertas categorías, como nacionales de determinado país, como heterosexuales u homosexuales, como profesionales, como padres o madres, etc., "todos ellos aspectos de nuestra identidad que, aunque sociales en un sentido, son peculiares para el individuo que somos y, como consecuencia, representan una dimensión

[9] Ibídem. pp. 51-52.
[10] Ibídem. p. 54.

personal de nuestra individualidad”[11]. Lo que, si bien son aspectos que se comparten, son propios de cada uno, que nos definen de forma particular y única, otorgándole al factor social en la construcción del yo el carácter de íntimo, de propio a uno mismo. Delimitando, por tanto, a todas las personas como seres en sí mismos, con identidades exclusivas a ellas, únicas e irrepetibles.

La identidad, entonces, es la convergencia del ámbito biológico de la persona con la expresión de ésta en la sociedad, lo cual dota de indeterminación a la misma, representándose como un “momento identificatorio en un trayecto nunca concluido, donde está en juego tanto la mutación de la temporalidad como la ‘otredad del sí mismo’ ”[12].

La insuficiencia inherente de la identidad personal se ve agudizada en el mundo actual, donde es el sujeto “quien se haga con la exclusiva de su identidad, asumiendo titánicamente todo el peso de justificar su ser-así-y-

[11] Ídem.
[12] IDENTIDADES, SUJETOS y subjetividades. 2005. Leonor Arfuch “et al”. 2ª edición. Prometeo, Buenos Aires, Argentina. p. 14.

no-de-otro-modo"[13], porque no sólo forma parte de la sociedad en el plano físico, sino que también habita en el universo abstracto que es Internet, donde los parámetros constructivos que da la naturaleza humana para moldear la propia identidad son difusos o incluso inexistentes.

Sin embargo, aún teniendo la identidad personal tal disposición -de incompleta-, dentro de ésta podemos reconocer ciertos elementos objetivos, que permiten la individualización de la persona de forma más concreta, lo que da un marco sostenible para establecer la identidad como objeto de usurpación.

1.1.1. Elementos de identificación

Siguiendo con lo expuesto anteriormente, la identidad personal es una "fórmula sintética para distinguir al sujeto desde un punto de vista global en la multiplicidad de sus características y manifestaciones", lo que

[13] NAVAL., C. 1995. Identidad personal, hábito y educación. [en línea] Concepción Naval. Universidad de Navarra. Revista Tópicos. Universidad Panamericana, México. <http://topicos.up.edu.mx/topicos/wp-content/uploads/2012/12/1995_TOP09_A_Naval.pdf> p. 33.

corresponde a todo el conjunto que es la persona; la exteriorización de su fuero interno, la posición ideológica y moral que adopta, su influencia cultural, entre otros. Elementos "que denotan la cabal personalidad del sujeto en su proyección social"[14], pero que no pueden ceñirse a una conceptualización muy rígida de identidad personal, debido a la amplitud de lo que abarca.

Existen signos distintivos con los que podemos individualizar a la persona, como son el nombre, el lugar y fecha de nacimiento, la imagen, la cédula de identidad, entre otros.[15] Los cuales, sirven para identificar a la persona "en el plano de la existencia material y de su condición civil"[16], manifestando con esto su calidad de único, irrepetible e idéntico sólo a sí mismo.

---

[14] Sentencia comentada en la obra de FERNANDEZ CESSAREGO, CARLOS. "Nuevas tendencias en el Derecho de las Personas" En: COLLANTES y GONZÁLEZ. Ob. Cit. pp. 114-115.

[15] Todos elementos de la identidad personal que coinciden con el ámbito estático de la misma, los que también pueden estar sujetos a modificaciones, pero que por lo general se caracterizan por su carácter inamovible. Más aún, estos elementos también son concordantes con los atributos de la personalidad, que serán explicados más adelante en el análisis.

[16] COLLANTES y GONZÁLEZ. Ob. Cit. pp. 113-115.

A continuación, explicaremos someramente en qué consisten cada uno de los elementos que sirven para el proceso de identificación.

1.1.1.1. El nombre

El nombre, según el diccionario de la Real Academia Española, es "la palabra que designa o identifica seres animados o inanimados, (...) tradicionalmente, una categoría de palabras que comprende el nombre sustantivo y el nombre adjetivo"[17], ya sea para reconocer a una persona -tanto natural como jurídica-, a un animal o una cosa.

En el presente estudio, sólo nos referiremos al nombre de las personas naturales, en cuanto son el objeto principal de nuestro análisis.

[17] Diccionario de la Real Academia Española, concepto de nombre.

Existen diversos autores[18] que intentan definir el nombre, mirándole desde diferentes perspectivas:

Colín y Capitant estiman que el nombre es la "señal distintiva de la filiación".

Para Bonnecase, el nombre es un "término técnico que responde a una noción legal, y que sirve para designar a las personas, el cual es un elemento esencial y necesario del estado de las propias personas".

Por su parte, Ferrara establece que el "nombre civil es el signo estable de individualización, que sirve para designar al sujeto como unidad en la vida jurídica", coincidiendo con la definición hecha por Rafael de Pina, quien estima que el nombre "es el signo que distingue a una persona de las demás en sus relaciones jurídicas y sociales".

El nombre, entonces, es el signo distintivo que tiene cada persona para diferenciarse e identificarse del resto de los individuos, y que tiene suma

[18] TREVIÑO G., R. 2002. La persona y sus atributos. Universidad Autónoma de Nueva León. Facultad de Derecho y Criminología. 1ª. ed. [en línea] <http://www.corteidh.or.cr/tablas/23961.pdf> pp. 45 y 46.

relevancia a la hora de establecer relaciones con los mismos, ya sean éstas meramente sociales o que comprendan algún componente jurídico.

Es evidente que más allá de las diferencias visibles que nos separan del resto –ya sean de carácter corporal o psicológico-, la vida en sociedad exige que las personas se distingan unas de otras a través de distintos medios, para identificarnos en el plano civil y jurídico. Una forma de determinarnos son los nombres, que nos singularizan respecto de los demás, dándonos un "lugar fijo dentro de la sociedad (…) y que nos permite materializar nuestros derechos y obligaciones en la organización jurídica (…)"[19].

Josserand, quien creemos que define perfectamente el objetivo del nombre para el propósito de este análisis, establece que "cada individuo representa una suma de derechos y obligaciones, un valor jurídico, moral, económico y social; importa que este valor aparezca al sólo enunciado de un nombre, sin equívocos, sin confusión posible; es necesario evitar que un individuo pueda aprovecharse falsamente de las cualidades (…); es

[19] COLLANTES y GONZÁLEZ. Ob. Cit. pp. 139-140.

indispensable que la personalidad de cada uno se distinga claramente de las otras; es gracias al nombre que este objeto se realiza"[20].

Esto, manifiesta que los nombres envuelven un interés jurídico, inmaterial, moral y social respecto de las personas, ya que el nombre representa el lugar y el valor de cada uno como individuo en la sociedad y en el campo del derecho.

El nombre tiene una funcionalidad multilateral, en virtud de su utilización como medio de individualización, identificación, indicación de filiación y del sexo, y como signo de la personalidad de los individuos.

Como instrumento de individualización, el proveer a los sujetos de un nombre los convierte en "individuos determinados personalizados", quienes pueden ser portadores de cualidades y a los que es posible imputarles conductas. Lo que hace que adquieran relevancia jurídica y se forme el orden mínimo necesario para el buen funcionamiento de la vida en

[20] JOSSERAND, L. Cours de droit civil positif francais. Tomo I. París. 1930. P. 207. En: COLLANTES y GONZALEZ. Ob. Cit. p.141.

comunidad. Además, tal individualidad permite a los hombres desarrollar su personalidad, dándoles la posibilidad de ser reconocidos como un "yo" propio y único[21]. A su vez, es medio de identificación, que no sólo cumple con distinguir unos de otros, sino que reconoce a cada sujeto como quién se supone o busca.

Y por último el nombre es indicativo de la filiación y del sexo de la persona, en cuanto la determina como parte de una línea familiar y manifiesta el sexo que detenta, lo que sirve para una identificación del individuo más acabada[22].

Debemos aclarar que es el nombre completo –el nombre propio o individual sumado al nombre patronímico o apellido- el que forma un todo indivisible con un valor identificatorio y jurídico, que permite nuestra

[21] Lo que va estrechamente ligado a ser el nombre signo de la personalidad, en cuanto otorga a las personas un sentido de posesión plena de sí mismos, dotados de voluntad y, por consiguiente, de responsabilidad. Tal conciencia de ser quien uno es, da a los hombres el ímpetu de desarrollarse tanto a nivel individual como familiar y social, y de lograr una vida que transcienda más allá de su existencia.

[22] PLINER, A. 1989. El nombre de las personas: legislación, doctrina, jurisprudencia, derecho comparado. Buenos Aires: Astrea, 2a. ed. pp. 49-57.

individualización -tanto en el ámbito filial, identificándonos como parte de una determinada familia, como particular-distinguiéndonos como individuos peculiares en la vida jurídica[23]-.

El nombre de las personas es necesario, imprescriptible, indisponible, absoluto e innato[24], siendo un derecho inherente a la persona y de carácter extrapatrimonial, con lo que lo consideramos un derecho de la personalidad, por proteger la esencia de la misma y sus más importantes atributos.

El derecho del nombre se funda, a nuestro juicio, en el derecho a la identidad, que propone proteger la individualidad de las personas para no ser confundidos con otros, lo que eventualmente podría traducirse en una situación perjudicial para el afectado[25].

---

[23] COLLANTES y GONZALEZ. Ob. Cit. pp.143-145.

[24] Esto significa que, toda persona debe tener un nombre, que no se puede adquirir o perder por el paso del tiempo y tampoco puede ser transferido ni transmitido por voluntad privada. Además de ser exclusivo de cada uno –a pesar de que hay nombres que se repiten- y oponible al resto de las personas, y de adquirirse al nacer sin necesidad de un título para adquirirlo.

[25] Esto se suma al interés del Estado y de terceros para determinar la identidad de las personas con las que generan y mantienen vínculos principalmente jurídicos, puesto que el perjuicio que aflija a una persona puede tener consecuencias respecto de otros.

El nombre, entones, es en sí una institución social, que tiene por finalidad la individualización de las personas, presentándose como "un centro alrededor del cual se entrecruzan derechos y deberes, impedido el sujeto de disponer por su sola voluntad de él, cuenta sin embargo con prerrogativas y facultades que le permiten ejercitarlo y defenderlo, impidiendo así que los terceros invadan la esfera del que utiliza legítimamente el nombre que le es atribuido"[26]. Pudiendo, no sólo usarlo, sino que defenderlo de un uso ilegítimo por otra persona.

La protección legal del nombre, parte de la base de este debe ser reconocido y respetado por los terceros, pudiendo ser utilizado por estos de forma adecuada, sin la intención de perjudicar a otros. Esto responde principalmente a una función social, lo que obliga al Estado a organizar y tutelar su ejercicio, y a proporcionar tutela judicial para los casos que se

[26] PLINER, A. 1951. El nombre de las personas: legislación, doctrina, jurisprudencia, derecho comparado. Argentina, Editorial Buenos Aires. p. 101. En COLLANTES y GONZALEZ. Ob. Cit. p. 162.

reclamen derechos o acciones relacionados con el nombre, ya sea su reclamación, su usurpación o la indemnización de daños y perjuicios[27].

Todo lo anterior, en virtud de la "suprema necesidad de orden público de que el nombre cumpla los fines jurídicos que le están asignados en satisfacción del señalado doble juego de intereses que, en definitiva, constituyen una sola y perentoria exigencia social regulada y sancionada por el derecho"[28].

Finalizado el análisis de la institución del nombre, cabe referirse resumidamente a las situaciones específicas del sobrenombre y el seudónimo, con el fin de establecer si éstos también son objeto de protección por parte del derecho.

Los elementos accidentales del nombre, como son el apodo y el seudónimo, si bien no son componentes esenciales del nombre "oficial" de las personas, se utilizan para complementar su individualización o sirven de

[27] COLLANTES y GONZALEZ. Ob. Cit. pp. 165 y 166.
[28] PLINER. Ob. Cit. p. 349.

forma especial a los sujetos para identificarse en órdenes de actividades específicos, mas –en palabras de Pliner- su validez es restringida y carecen de la jerarquía jurídica del nombre.

El sobrenombre es un modo de designación espontáneo que, por lo general, nace en el entorno familiar o social donde se desenvuelve la persona, el cual no tiene consecuencia jurídica en nuestro derecho. Sin embargo, puede darse que el alias sea ocupado con fines similares al nombre, caso en que dejaría de ser indiferente para el derecho.

El seudónimo, por otro lado, es un nombre escogido por la persona para ser representado por éste en el plano artístico, el cual viene a reemplazar al verdadero nombre en la actividad pretendida. Esto no significa que se sustituya al nombre real en su labor de individualizador en el ámbito jurídico, sino que es sólo una marca profesional con la que se decide trabajar. Lo importante es que su protección legal se basa en la patrimonialidad que se tiene sobre éste, aunque a veces, dada su íntima relación con la identidad de la persona, puede dársele un tratamiento como

bien moral jurídicamente protegido[29]. En nuestro país, el seudónimo es reconocido como derecho intelectual, por lo cual encuentra protección en la Ley sobre Propiedad Intelectual[30].

Entonces, podemos establecer que estas formas de designación que utilizan las personas en ámbitos específicos de su vida, pueden considerarse similares al nombre -tener la misma relevancia jurídica- en ciertos casos, siempre y cuando tengan una estrecha relación con la identidad del sujeto en cuestión. Es decir, que su personalidad se vea reflejada en el sobrenombre o el seudónimo, y que se identifique por esto a la persona de la que se trata.

1.1.1.2. La imagen

La imagen, es la proyección externa del ser personal del individuo, siendo la representación material de los aspectos inmateriales de su personalidad, convirtiéndose en una verdadera comunicación con el resto de

[29] Ibídem. p. 47 y 48.
[30] CHILE. Ministerio de LEY Nº 17.366, Apéndice Código Civil, publicada en el Diario Oficial Nº 27.761, del 2 de octubre del año 1970.

las personas[31]. Ésta puede definirse entonces como el "conjunto de rasgos que caracterizan ante la sociedad a una persona"[32], donde se plasma la individualidad del ser humano, siendo con esto su principal herramienta de comunicación, y uno de los focos donde se exterioriza su identidad[33].

Este elemento del proceso de identificación detenta dos aspectos, uno material y uno inmaterial. El ámbito material de la imagen se encuentra en el plano físico, siendo la apariencia o representación corporal de la persona su móvil principal para comunicarse con los demás, el que se caracteriza por ser tangible, es decir, que puede percibirse por los sentidos. Mientras que la inmaterialidad de la imagen se integra por un conjunto de funciones de significación, con las que ésta –la imagen- adquiere el poder de identificación de la persona.

---

[31] COLLANTES y GONZALEZ. Ob. Cit. p. 173.

[32] Diccionario de la Real Academia Española. Concepto de imagen.

[33] "La imagen humana en lo que tiene de presencia externa del hombre, le individualiza – le separa y le distingue de los demás hombres- y, a la vez, le comunica con ellos. Esa capacidad manifiesta de la imagen de individualizar y comunicar procede del sujeto personal". En: ROVIRA SUERIO, MARÍA E. El derecho a la propia imagen. Especialidades de la responsabilidad civil en ese ámbito, Colección de estudios de responsabilidad civil. Madrid, editorial Comares. 2000. p. 70. En: COLLANTES y GONZALEZ. Ob. Cit. p.173 y 174.

Las funciones de significación que convierten a la imagen en uno de los elementos de la identidad personal son; la de individualidad, de recognoscibilidad e identidad[34].

La primera función da cuenta que con la imagen, cada uno se percibe como alguien concreto, único, distinto y diferenciable de todos los demás, lo que se traduce en que la imagen detenta un rol importante dentro de la identificación de la persona.

En un segundo término, la función de recognoscibilidad se realiza al reconocerse o ser reconocida la persona por los demás, en cuanto conjunto de rasgos particulares que le son propios a un sujeto determinado. Función que le otorga a la imagen la condición de objeto de derecho, puesto que su reconocimiento como parte inherente de la persona da cabida a que sea considerado digno de ser protegido.

[34] COLLANTES y GONZALEZ. Ob. Cit. pp. 175 y 176.

Y por último, la función de significación de identidad nos permite determinar a quién corresponde tal representación visible y específica, es decir, podemos establecer que la imagen de una persona pertenece sólo a ella por su calidad de ser sí misma y no otra.

Es importante destacar que la imagen sólo tiene sentido cuando se incluye en un proceso comunicativo con otros, en cuanto abarca tanto el ámbito físico corporal de la persona humana como la representación que hace la misma de su modo de ser, de su personalidad, usándola como proyector de su identidad[35].

La imagen, como parte esencial de la identidad, es también un de derecho de la personalidad, en virtud de que la primera se encuentra al servicio de la segunda, para permitir su libre desarrollo. Convirtiéndose la imagen en el medio primordial para la exteriorización de la identidad, lo que determina que sobre ella se tenga su dominio absoluto, una especie de propiedad, ya que el derecho a la imagen, como representación o

[35] Ibídem.p p. 174-177.

proyección que es, sería consecuencia del derecho que se tiene sobre el propio cuerpo[36].

Al implicar, el concepto de imagen, la representación de alguna cosa, en este caso del ser humano, el derecho a la propia imagen integraría la personalidad del individuo y como tal debe ser protegido jurídicamente[37].

Al igual que el nombre, la imagen debe ser reconocida y respetada por los demás y, por lo tanto, cabe dentro de la esfera de protección del derecho[38], siendo deber del Estado proveer a las personas de tutela judicial para los casos en que su imagen se vea afectada.

Legislativamente, este derecho abarca tanto la imagen del sujeto, y se extiende al nombre, la voz y otras cualidades personales posibles de exteriorización, todos "rasgos que constituyen las señas de identidad más

---

[36] Ibídem. pp. 178-179.
[37] BORGARELLO, SUSANA E. Derecho a la imagen. Córdoba, Argentina: Marcos Lerner Editora, 1996. p. 31.
[38] Es habitual, que el derecho a la imagen tenga relación con la utilización de ésta para fines comerciales, publicitarios o de naturaleza similar, ya sea que una persona decida ocuparla de forma pública o bien opte por abstenerse de cualquiera de estas actividades.

indiscutibles”[39], el que se protege del uso indebido –sin permiso- para fines publicitarios o comerciales a los que no se haya consentido.

1.1.1.3. La nacionalidad

La nacionalidad es el vínculo que una persona tiene con una nación determinada, ya sea por pertenecer a una comunidad nacional por vía de nacimiento en un territorio específico, o bien por un “sentimiento suficientemente intenso para ligarlo a él”[40].

Por nación, entendemos el “conjunto de los habitantes de un país -delimitado en un territorio específico- regido por el mismo gobierno, que generalmente detentan un mismo origen, y que a su vez comparten un mismo idioma y tradición en común”[41].

La nacionalidad es inherente a la persona humana –hoy es imposible la existencia de personas sin patria-, siendo uno de los atributos de la

[39] COLLANTES y GONZALEZ. Ob. Cit. pp. 180-182.
[40] Ibídem. p. 188.
[41] Diccionario de la Real Academia Española. Concepto de nación.

personalidad más importantes, ya que es expresión inmediata de la sociabilidad que envuelve la vida de los hombres.

La abstracción que se hace del territorio, del idioma, de las costumbres, de la historia nacional, conduce a las personas a ser de cierta manera, a construir una identidad personal que se encuentre en relación a la identidad país. Lo que se traduce en una orientación al pensamiento, al sentimiento, a la forma de obrar de las personas que integran un pueblo determinado[42].

La nacionalidad, al igual que los demás atributos de la personalidad, también detenta una expresión jurídica, lo que se determina como "el conjunto de derechos y deberes individuales que, en medida plena, le reconoce el Estado, el cual en ejercicio de su soberanía, según su régimen y las concepciones generales de su época, se caracteriza por una relación de mutua defensa y de sometimiento del individuo a su Estado"[43].

[42] COLLANTES y GONZALEZ. Ob. Cit. pp. 189-194.
[43] ROMERO, NÉLIDA. Nacionalidad, concepto y principios fundamentales. Memoria de licenciado en Ciencias Jurídicas y Sociales. Santiago, Universidad de Chile. 1953. En: COLLANTES y GONZALEZ. Ob. Cit. pp. 188-189.

Esta manifestación jurídica, por lo general, se encuentra regulada en la Carta Política Fundamental de los diversos países alrededor del mundo, así como en el caso chileno donde la Constitución Política de la República es la encargada de establecer los parámetros de la nacionalidad.

Debemos recordar que, en nuestro país existen cuatro fuentes de nacionalidad; “Ius solis” y “Ius sanguinis”-donde la nacionalidad es originaria, adquiriéndola el sujeto al nacer- y, la nacionalización y la nacionalidad por gracia –en las cuales la nacionalidad es adquirida posteriormente y sustituyendo a la primera-.

Resumiendo, la nacionalidad -ya sea ésta originaria o adquirida-, es la relación que tenemos las personas con una nación determinada, lo que implica ser perteneciente a un territorio físico y compartir con los demás connacionales el idioma, la cultura, las tradiciones y la historia país. Lo que influye directamente en la construcción de la propia identidad y se convierte en parte fundamental de lo que somos.

1.1.1.4. Cédula de Identidad y Rol Único Nacional

La Cédula de Identidad y el Rol Único Nacional son instrumentos que tiene por utilidad comprobar la identidad de una persona en caso de que así sea requerido.

La Cédula de Identidad, por una parte, es un documento que contiene el nombre de la persona, su fecha y lugar de nacimiento, su Rol Único Nacional, su foto –que da cuenta de su aspecto físico-, su firma y la huella digital, todo esto con el fin de reconocer a la persona quien la porta. Dicha documentación se convierte en la representación legal completa de la persona, siendo un medio inequívoco para establecer y certificar la identidad del individuo.

En la actualidad es una herramienta utilizada por la gran mayoría de las naciones, en cuanto es efectiva en la tarea de individualizar íntegramente y de forma segura a las personas, sumado a la practicidad que otorga su uso en distintos ámbitos de la vida en sociedad[44].

[44] En un comienzo, este tipo de documentación se ocupaba principalmente en el ámbito criminal, con el fin de tener un registro de los delincuentes

Con la cédula de identidad "no sólo se quiere definir y fijar legalmente la personalidad, sino además facilitar la identificación de las personas, a fin de que cualquiera pueda efectuarla sencilla y rápidamente"[45]. Por lo que, "establecer el lazo de unión entre la persona y el documento, será poner los cimientos de la identidad personal"[46].

Por otro lado, el Rol Único Nacional o RUN es el número único e irrepetible con el que se identifica legalmente una persona en nuestro país. Éste se otorga al momento de la inscripción del nacimiento en el Registro Civil, y forma parte de nosotros a lo largo de nuestras vidas.

1.1.1.5. Firma

---

para que estos no fueran confundidos con gente respetable, pidiéndose principalmente en los empleos y a los inmigrantes.

[45] VUCETICH, JUAN. Proyecto de Ley de Registro General de las personas. Escrito en el período de 20 de enero y 17 de mayo de 1915. En: COLLANTES y GONZALEZ. Ob. Cit. pp. 219-220.

[46] Ídem.

La firma es principalmente la extensión de la voluntad de la persona, entendiéndose como el medio para materializarla[47]. Ésta, es una invención de la persona que la utiliza, siendo por lo general el nombre y apellido del sujeto.

La importancia de la firma, ya sea escrita en papel o utilizada en medios electrónicos- recae en que "establece la identidad del suscriptor de un determinado documento y/o se realiza una determinada transacción. Por medio de la firma se sabe que la persona que está emitiendo un documento es quien dice ser, quedando además un respaldo de ello"[48], el cual es muy difícil de desvirtuar.

Si bien no es relevante si la firma es legible o ilegible, completa o parcial, que se escriba acorde a las reglas ortográficas o en otro idioma, es necesario que sea auténtica y represente de forma verdadera la identidad de la persona, y sea emanada por la misma.

[47] Etimológicamente la palabra firma deriva del verbo latino firmo-are que significa afirmar o confirmar.
[48] COLLANTES y GONZALEZ. Ob. Cit. p. 223.

Existen otros sistemas de identificación, que nos permiten individualizar a las personas como sujetos irrepetibles, como la voz, el estado civil, la huella dactilar, entre otros. Mas, no los trataremos al considerarlos que no son mayormente útiles para el objetivo encomendado en el presente trabajo.

En resumen, podemos establecer que la identidad es la fusión del ámbito biológico de la persona con la expresión de ésta en la sociedad, siendo el conjunto de rasgos propios de un individuo que lo caracteriza frente a los demás, determinándolo como un sujeto único e irrepetible, sumado a la conciencia de ser uno mismo y no otro.

La identidad y sus elementos son análogos al ser humano, no entendiéndose uno sin el otro. Dicho esto, es imprescindible ilustrar el concepto de persona, para determinar qué es lo que el derecho protege al tipificar la usurpación de identidad como delito.

1.2. Concepto de persona

El concepto que desarrollaremos en esta parte del trabajo corresponde únicamente al de persona natural, en cuanto la identidad es propia y exclusiva de los seres humanos, siendo el objeto principal de nuestro análisis.

En la actualidad, la acepción de persona que existe en el lenguaje común es "todo individuo de la especie humana"[49], con lo que se considera una sola palabra para hombres y mujeres, sin hacer distinciones de ningún tipo[50].

[49] Diccionario de la Real Academia Española, concepto de persona.

[50] Según el Profesor Ángel Rodríguez Guerro, en su artículo "La persona humana", la historia de la palabra persona tiene su preámbulo en Grecia y Roma, donde este concepto se ligaba al de dignidad, la cual no era una cualidad de todos los hombres, lo que dependía de diversos factores como si se era libre o esclavo, de la clase social, la raza, etc., mas no existía aún como concepto definido. Recién con la llegada del cristianismo nace el término "persona", el cual dotaba a todos los individuos de igual dignidad, y los determinaba como únicos e irrepetibles.
Si bien en un comienzo se pensaba que el vocablo persona sugería la máscara que se usaba en el teatro -en cuanto servía para apersonarse-, pronto con los estoicos se le da un significado más concreto a esta palabra, refiriéndose al "sujeto responsable de sus acciones, capaz de dominio, con una interioridad, dignidad y autonomía, en la cual se implica una participación en el logos; y por ello la inteligencia de la realidad". Concepto que sufre distintas modificaciones en el seno de importantes filósofos como Descartes, Kant, Hegel y Sartre, entre muchos otros. Evolucionando hasta el

Sin embargo, la persona no sólo se define por su calidad de ser humano, sino también por el rol social que adquiere al vivir en sociedad, lo que alcanza características determinadas según el tiempo y la cultura a la que pertenece[51].

Esto se expresa de forma manifiesta en F. Rielo, para quien "la respuesta a 'qué es persona' es otra persona: una persona se define por otra persona (…) No existe persona única en soledad absoluta: la metafísica del 'quién' es un 'alguien' que da razón a otro 'alguien'"[52].

Sin embargo, y a pesar de estimar que las personas no se entienden de forma absoluta y en solitario y que es inherente a los seres humanos el vivir

día de hoy, donde se toma conciencia a nivel universal de que todos los seres humanos son personas, y que detentan igual dignidad.

[51] Cabe recordar que dicha sociabilidad es natural e inherente al ser humano -ya lo planteaba Aristóteles al referirse al hombre como el animal social ("zoon politikon")-, por lo que es parte fundamental en el proceso de construcción de la identidad personal, como se analizó anteriormente.

[52] J.M. LÓPEZ SEVILLANO. La nueva metafísica de F. Rielo, en Aportaciones de filósofos españoles contemporáneos. Colección de Filosofía 3, Fundación Fernando Rielo. Constantina (Sevilla) 1191, p. 87. En: Ángel Rodríguez Guerro. La persona humana.

en sociedad y verse representados en los otros, debemos tener claro que cada persona singular y concreta, es "realidad una, única e irrepetible que tiene capacidad para hacer suyas las cosas que adquiere fácticamente, intelectivamente y voluntariamente". La persona "es subsistente a todos los demás entes, en tanto que es diferente, se da en él cierta clausura. (…) El ser subsistente es indiviso, y no puede desintegrarse porque él mismo es una unidad"[53].

Según Hoyos Castañeda, se llama persona al ser que se domina a sí mismo, y en consecuencia domina sus actos. La persona, entonces, es portadora de cosas; ya sea su nombre, su vida, su libertad, etc., "y en cuanto tal puede (…) autogobernarse, poseerse, conocerse" [54] y relacionarse con otros. Determinando el señorío que tiene sobre sí misma y sobre sus actos[55].

[53] HOYOS. Ob. Cit. p.19.
[54] Ibídem. pp. 20-21.
[55] Hoyos Castañeda también se refiere a la persona como la integración de una faceta estática y una dinámica, en cuanto la naturaleza humana detenta una estructura fija, determinada y estable que es común a todos los hombres, y a su vez reside en ella la potencialidad de moldearse a través de sus actos, todo en relación con los sucesos accidentales que sean parte de la propia vida.

Si bien el ser humano es un ser individual y concreto -que cierra su existencia en sí mismo-, también detenta una naturaleza social, de la cual nace la juricidad que detentan las personas, la cual conduce a los individuos a relacionarse jurídicamente entre sí, convirtiéndolos a cada uno de ellos –como personas que son- en el núcleo del ordenamiento jurídico[56].

El ser humano, por tanto, detenta una doble función respecto del derecho[57], en cuanto éste último existe por la persona y para la persona, siendo el hombre quien lo crea y el bien supremo principal en el ámbito de su protección.

Jurídicamente, esta conceptualización de persona natural adquiere una extensión aún más acabada, definiéndose como "sujeto de derecho"[58], que

[56] HOYOS. Ob. Cit. p. 25.
[57] La persona es el elemento más importante para el derecho, tanto en su aspecto público como en el privado, siendo el eje principal de la juridicidad en todas sus ramas.
[58] Según el profesor Alejandro Guzmán, en su libro "Los orígenes de la noción de sujeto de derecho", el concepto de 'sujeto de derecho' no nace en la ciencia jurídica, ya que para los juristas romanos y medievales sólo existen las 'personas'. Sino que la expresión 'subiectum iuris' aparece con los escolásticos españoles del siglo XVI, pero no como término técnico propio del derecho, introduciéndose más adelante a él como una noción

si bien son conceptos que se relacionan, no deben confundirse. El sujeto de derecho, en términos generales, lo definimos como un centro de imputación ideal de derechos y deberes. Expresión máxima de esto se refleja en los atributos de la personalidad, que son aquellos elementos necesariamente vinculados a toda persona natural e imprescindible para su desarrollo como sujetos de derecho, los cuales se reducen a los siguientes: el nombre; la nacionalidad, la capacidad de goce, el estado civil, el domicilio y el patrimonio[59].

Los atributos de la personalidad, "son las más elementales prerrogativas de que pueden gozar las personas, y son atributos de los cuales no pueden

---

filosófica que plantea la pregunta de "quién puede ser titular del dominio en especial y de derechos (subjetivos) en general". Este concepto nunca es confundido, ni en la escolástica ni en el humanismo con el vocablo persona, aún pudiendo las personas ser designadas como sujetos. Ya con Leibniz, Wolf y Kant se hace una identificación de sujeto y persona bajo la expresión de sujeto de derecho. Mas luego, se define como un supraconcepto relacionado con quienes pueden ser titulares de derechos y obligaciones y ya no con las personas específicamente.

[59] Algunos de los atributos de la personalidad fueron vistos en el punto precedente, como elementos de identificación de la persona, o bien de su esencia o identidad, mientras que los demás sólo serán nombrados, ya que no cabe su análisis para el propósito del trabajo.

ser privados, que no pueden ser alterados y que no pueden sufrir menoscabo alguno"[60].

Como ya lo hemos planteado, la persona es el objeto central del derecho y, por tanto, los atributos que le son inherentes también estarían bajo el alero de su protección.

1.2.1. Legislación Chilena

En la cúspide de nuestra legislación tenemos la Constitución Política de la República, la que no establece el concepto de persona, mas sí determina una serie de derechos y deberes que ésta detenta.

Aún así, se entiende que la Carta Fundamental está erigida alrededor de la persona, en cuanto establece en su artículo primero inciso primero lo siguiente:

[60] Fallo de la CORTE DE APELACIONES DE SANTIAGO. En: Revista Chilena de Derecho y Jurisprudencia. 1961. Segunda Parte, secc. 2ª. 107. En: COLLANTES y GONZALEZ. Ob. Cit. p. 160.

"Las personas nacen libres e iguales en dignidad y derechos."

Y continúa en el inciso cuarto del mismo artículo:

"El Estado está al servicio de la persona humana y su finalidad es promover el bien común, para lo cual debe contribuir a crear la condiciones sociales que permitan a todos y a cada uno de los integrantes de la comunidad nacional su mayor realización espiritual y material posible, con pleno respeto a los derechos y garantías que esta Constitución establece"[61].

Ahora bien, al no definirse a la persona en nuestra Constitución, se le encomienda dicha tarea al derecho privado, siendo el Código Civil el que establece quiénes son parte de esta categoría en su artículo 55 inciso primero:

"Son personas todos los individuos de la especie humana, cualquiera que sea su edad, sexo, estirpe o condición."

[61] Es importante destacar que la Ley 19.611 reemplaza la palabra 'hombre' por la palabra 'persona', con la finalidad de igualar a hombres y mujeres frente a la ley, utilizando una palabra neutra que incluyera ambos sexos.

La mencionada disposición claramente no es una definición, sino un mero señalamiento de que 'persona' será todo individuo de la especie humana, sin especificar las características esenciales de la persona, por lo que falta el contenido fundamental para establecer "si un ser determinado puede o no ser incluido en el concepto de persona"[62].

Mas, este artículo detenta la gran virtud de determinar la igualdad y el principio de no discriminación respecto de las personas naturales, debiendo la ley darles a todas el mismo trato, sin hacer distinción de ningún tipo.

Según el profesor Fernando Fueyo, visto desde la perspectiva del profesor Gonzalo Figueroa, son tres los aspectos que deben considerarse al tratar el concepto de persona en el Derecho Civil.

En primer lugar, es relevante tener claro la generalidad de individuos que el concepto abarca, con lo cual su tratamiento tenderá a la

[62] FIGUEROA Y., G. 2000-2001. El derecho de la persona como rama autónoma del derecho civil. Revista de Derecho y Humanidades. P. 61.

estructuración de un estatuto general, "que los aborde tan sólo como individuos de la especie humana, sin considerar sus actividades o características específicas, buscando una esencia común e invariable"[63].

Segundo, se debe exceder la concepción puramente patrimonial de la persona, y tratar también los derechos extrapatrimoniales. Puesto que la persona se define más por "sus intereses y características vitales, espirituales y morales, que por sus rasgos económicos y patrimoniales"[64].

Y por último, al conceptualizarse la persona natural debe tomarse en cuenta el lugar central que debe tener en el sistema, en virtud de que "no hay nada más privado que la persona misma", debiendo ser su individualidad el fundamento del derecho civil[65].

Para este fin -de conceptualizar a la persona de forma más íntegra-, la línea civilística tradicional estableció su contenido a través de los 'atributos de la personalidad', sosteniendo que las personas se caracterizan por éstos.

[63] Ibídem. p.59
[64] Ídem.
[65] Ídem.

Sin embargo, en la actualidad, se estima estos son insuficientes para caracterizar a las personas, en cuanto ellas no son ni un nombre, un estado civil ni un patrimonio determinado. Pudiendo éstos poseerse por las personas, pero siendo incapaces de definirlas como tal.

Frente a esta situación, la civilística agrega los 'derechos de la personalidad'; como es el derecho a la vida, a la integridad física y psíquica, al honor, libertad, privacidad, etc., para complementar el concepto de persona[66]. Creemos, al igual que el profesor Gonzalo Figueroa, que "una persona natural debe caracterizarse siempre por los derechos humanos, los derechos constitucionales especialmente reglamentados, los derechos protegidos por el ordenamiento penal, los derechos y los atributos de la personalidad civil. Y tal caracterización debe ser válida para todas las ramas del Derecho, sin distinción, sin perjuicio de que cada una profundice el aspecto específico que le corresponde"[67].

1.3. Identidad personal como Derecho de la personalidad.

[66] Ibídem. p. 62.
[67] Ibídem. pp. 62-63.

1.3.1. Los derechos de la personalidad

Como ya hemos establecido en los puntos anteriores, todo ser humano, por el solo hecho de serlo, es persona para el Derecho, limitándose este último a reconocer tal condición, sin hacer distinciones de ningún tipo.

Actualmente se le reconoce a la persona un conjunto de derechos que se encuentran recogidos en las diversas constituciones alrededor del mundo, los que se conocen comúnmente como derechos fundamentales[68].

Debemos enfatizar que "será la distinta consideración jurídica de la persona frente al Derecho lo que determina el 'estado de la

[68] Según Clemente Crevillén, en su libro "Derechos de la personalidad.", ya en el Derecho Romano se le daba una cierta protección a algunos de estos derechos -como la vida, el honor y la libertad-, con el fin de reprimir actos que despreciaran a terceras personas. Lo que se acentúa en la Edad Media – más que nada respecto del derecho al honor-, y que alcanza su máxima expresión con las primeras constituciones en Europa y América en el siglo XVIII.

personalidad'"[69], en tanto, más protagonismo se le dé a la persona en los distintos sistemas jurídicos, mayor será la relevancia que los derechos de la personalidad adquieran en cada uno de ellos.

Es indudable que personalidad y derechos de la personalidad son conceptos inseparables, por lo que cabe elaborar una idea clara del primero con el fin de entender el segundo.

La personalidad es una cualidad jurídica, que existe dentro del ordenamiento jurídico y gracias a él, puesto que es el derecho el que imputa a las personas una serie de derechos y deberes que requieren de la existencia previa de la personalidad para ser adquiridos[70].

Los derechos de la personalidad, por su parte, son aquellos "derechos subjetivos privados, absolutos y extrapatrimoniales que posee todo ser humano (…) y que protegen la esencia de la personalidad y sus más

[69] CREVILLÉN., C. 1995. Derechos de la personalidad. Honor, intimidad personal y familiar y propia imagen en la jurisprudencia. Actualidad, Madrid. p.20.
[70] COLLANTES y GONZALEZ. Ob. Cit. pp. 35 y 36.

importantes elementos o atributos, tales como la vida, el honor, el nombre, la imagen, etc."[7172] Y, por tanto, en ellos convergen "las ideas del hombre, de libertades, de derechos ajenos, de esencialidad, y, su producto, individualidad"[73].

Ferrara, según lo señalado por Crevillén, establece que los derechos de la personalidad detentan el "carácter de derechos supremos del hombre que garantizan en él el goce de sus bienes personales debiendo distinguirse entre los bienes exteriores a la persona de los bienes 'in corporis' (…) o sea los

[71] GIERKE, citado por ORGAZ.,A. Personas individuales. 1961. Córdoba. Editorial Assandri. Derecho Civil Argentino. p.108. En: COLLANTES y GONZALEZ. Ob. Cit. p. 36.

[72] Si bien, a primera vista, se piensa que el objeto de los derechos de la personalidad es la persona misma -lo que no ha estado exento de controversia, en tanto, diversos autores estiman que habría una especie de 'cosificación de la persona, o bien debiera este objeto ser susceptible de apropiación, con lo que los derechos de la personalidad estarían más cercanos a los derechos reales-, estimamos que éstos recaen sobre alguna de las cualidades de la persona, como lo plantea Manuel de Cosio, en palabras de Adriano de Cupis, en su libro I diritti della personalitá, ya que la personalidad actúa como un recipiente vacío susceptible de ser rellenado con los derechos subjetivos y que son los de la personalidad que constituyen el mínimo necesario imprescindible de su contenido

[73] VODANOVIC S., N. 1981. Los derechos de la personalidad en las legislaciones positivas extranjeras. Memoria para optar a la licenciatura en ciencias jurídicas y sociales. Santiago, Universidad de Chile, Facultad de Derecho. p.6.

derechos de la personalidad que garantizan el goce de nosotros mismos y aseguran al hombre el dominio sobre su propia persona"[74].

1.3.2. Derecho a la Identidad personal

La identidad personal, como ya lo planteamos anteriormente, es la convergencia de los aspectos estático y dinámico, en cuanto responde a la estructura corporal fija propia de cada uno sumado a la construcción social que hacemos de nosotros mismos.

Esto supone que la identidad personal está conformada por la identidad biológica y la identidad cultural, siendo la primera la estructura genética única que le corresponde a cada ser humano, y la segunda la edificación del yo en sociedad en tanto somos individuos que comparten con otros[75].

[74] CREVILLÉN. Ob. Cit. p.20.
[75] COLLANTES y GONZALEZ. Ob. Cit. pp. 61 y 62.

Este último punto -la proyección social que tiene la identidad- es lo que le concede la calidad de bien jurídico, en virtud de la susceptibilidad de ser ofendida por otros, por lo cual precisa protección jurídica[76].

La identidad personal es el conjunto de rasgos que nos determina como seres únicos, diferentes e irrepetibles dentro de la especie humana, lo que significa –en palabras de Adriano de Cupis- nuestra "verdad personal".

Con lo anterior, queremos establecer que la identidad personal es en sí una cualidad propia de la persona, más precisamente una cualidad moral, que afirma la propia individualidad en el ámbito social, ya que todos buscamos diferenciarnos del resto, en virtud de las propias cualidades y acciones, interés que en la realidad requiere de una tutela jurídica que implica la obligación de respeto de la verdad personal.

Entonces, el bien jurídicamente protegido en el derecho a la identidad personal es la "verdad de la persona"[77]. Tal derecho haría referencia a una

[76] DE CUPIS, A. 1961. I diritti della personalitá. Dott. Antonino Giuffrè. Milano. Tomo II. p. 3.

cualidad, a una forma de ser, lo que para los demás determina que uno es igual a sí mismo, aspecto que se ajustaría inevitablemente a la realidad de la personalidad individual, que es un atributo de la persona[78].

Esto significa que cualquier alteración a la verdad personal, por insignificante que sea, puede considerarse como una ofensa a la identidad personal, puesto que la persona afectada deja de ser idéntico a sí mismo. Mas, tal extensión del concepto de identidad personal implica que el derecho que lo tutela abarque cualquier infidelidad en contra de la verdad personal, incluso las que no afectan en absoluto a la persona.

No creemos, sin embargo, que la protección jurídica del derecho a la identidad personal deba tener tal amplitud, puesto que tal escenario sólo conllevaría a un orgullo exagerado de la propia individualidad, lo cual aumentaría la intervención de la ley, convirtiéndola en represiva y

[77] COLLANTES y GONZALEZ. Ob. Cit. p. 61.
[78] DE CUPIS. Ob. Cit. pp. 6y 7.

desproporcionada en relación a las posibles lesiones que la identidad personal pudiera sufrir[79].

Ahora bien, en virtud de la vastedad del concepto de identidad personal, y del amplio espectro que abarca el derecho que la contempla, debemos especificar qué debe incluirse en este derecho.

Mientras, algunos autores –como De Cupis- consideran la identidad personal como un derecho de la personalidad, incluyendo en éste sólo los derechos que se tienen respecto al nombre y al seudónimo, otros prefieren hablar de derechos a la individualidad, dentro de los que se comprenderían los atributos de la personalidad como el "nombre, el domicilio, el estado civil y raza, patrimonio y profesión".

Pese al sentir de estos autores, es relevante mencionar que en gran parte de los códigos modernos sólo se incluyen algunos de estos elementos como parte de los derechos de la personalidad; "otros son dejados de lado, sea porque no se consideran así, sea porque aún calificándose de esa manera no

[79] DE CUPIS. Ob. Cit. p. 12.

se tratan porque tienen desarrollos latos y se norman fuera del cuadro de los derechos de la personalidad"[80].

En nuestra opinión, el derecho a la identidad personal tutela la verdad de la persona, es decir, la cualidad de ser idéntico a sí mismo, la individualidad del sujeto que lo hace único e inconfundible para el resto de los individuos. Protege entonces, en términos generales, el aspecto de la personalidad que mezcla el ámbito biológico con el cultural, que se proyecta en la vida en sociedad a través de ciertos elementos distintivos –como es el nombre, la imagen, la firma, entre otros- que nos identifican como seres propios y diferentes de los otros.

Esta conceptualización del derecho a la identidad es bastante amplia, por lo abstracto de su terminología, lo cual traduciéndose en una magnificación del sentimiento que tenemos respecto de la propia identidad, conlleva a su protección extralimitada, hasta el punto donde la más mínima alteración de

[80] LONG P., J. 1986. Tratamiento de los derechos de la personalidad en códigos civiles modernos. Memoria para optar a la licenciatura en ciencias jurídicas y sociales. Santiago, Universidad de Chile, Facultad de Derecho. p.64.

ella sería digna de una sanción por parte del ordenamiento jurídico. Por esta razón, estimamos que el derecho de la identidad personal debiera abarcar sólo los elementos que se consideran importantes para la representación adecuada de la persona, para su identificación en el ámbito social, o que estén estrechamente vinculados con la personalidad individual, y que en su afectación se logre una verdadera tergiversación de la identidad de la persona, sin que esto signifique un exceso de contenido para la identidad y su derecho.

Sin embargo, consideramos que cuando existan derechos especiales que protejan ciertos elementos de identificación -como es el caso del derecho a la imagen-, o que tutelen algún otro derecho de la personalidad que se relaciona directamente con la identidad, mas no sea exactamente éste, se prefieran y ocupen aquellos dotados de especialidad.

Por último, es importante destacar que el derecho a la identidad personal tiene como fundamentación principal el interés humano de precisar su identidad en el conocimiento de los otros, para así velar por que la personalidad individual no se deforme en la propia percepción ni en la

ajena, ya que es indudable el afán de todos de conocer al otro de acuerdo a la verdad[81].

1.4. Relación con otros derechos de la personalidad.

Son varios los derechos de la personalidad que han constituido un gran desafío para la doctrina comparada, en cuanto están erigidos sobre conceptos difusos y todos tienen el mismo objetivo; la protección de la persona humana. Más aún, es especialmente difícil relacionarlos con el derecho a la identidad personal, debido al escaso acuerdo que existe sobre su contenido y los pocos exponentes que ven la identidad como un derecho de la personalidad.

Cosa que sí podemos establecer de forma cierta, es que todos los derechos de la personalidad son inherentes a la persona y se relacionan directamente con la dignidad humana, en cuanto son éstos los que representan el ámbito más íntimo del ser humano, los que protegen el círculo más personal de la interioridad de los individuos, y por tanto,

[81] DE CUPIS. Ob. Cit. p. 17.

creemos que ésta -la dignidad de las personas- es el contenido mínimo de los derechos que se conceden para proteger la vida.

El carácter etéreo que rodea a los derechos de la personalidad puede conducir a una confusión entre ellos, o bien una mezcla de sus cometidos, creando el problema de que en una situación concreta de afectación a la personalidad se deba determinar cuál es el derecho que prevalece entre varios que coexisten.

Por estas razones, estimamos necesario delimitar algunos de los derechos que se relacionan de forma más directa con el derecho a la identidad personal, todo en miras de responder el conflicto que se suscita con el delito de usurpación de identidad en el ámbito de las redes sociales, más específicamente cuando ocurre en Facebook y Twitter.

1.4.1. Derecho a la intimidad o privacidad

La intimidad, según el Diccionario de la Lengua Española, es la esfera espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia[82]. Es el espacio más propio y personal de la persona.

El derecho a la privacidad surge como una libertad, ya que se entiende que el hombre es libre cuando es dueño de su persona y de sus actos, los cuales son exclusivos y reservados a él. El sujeto es propietario por sobre todas las cosas de su conciencia, pues tal recinto espiritual le otorga la mayor de las libertades, y no admite intromisión alguna[83].

En relación a su esfera privada, las personas tienen "derecho a guardar secreta la intimidad de su existencia (…) o algún aspecto de su vida, eliminando toda intrusión por parte de terceros". Razón por la cual, "este derecho (…) consistiría más bien en una libertad, que garantiza la tranquilidad de la persona y el aspecto privado de la misma"[84].

[82] Diccionario de la Real Academia Española, concepto de intimidad.
[83] BEJAR., Helena. El ámbito íntimo. Privacidad, individualismo y modernidad. Madrid, Editorial Alianza S.A., 1980. P.27. En: COLLANTES y GONZALEZ. Ob. Cit. p. 68.
[84] VODANOVIC. Ob. Cit. p. 21

Según Georgina Batlle –en palabras de Clemente Crevillén- “en el concepto de intimidad palpita una idea de exclusión de la comunicación total, de la publicidad, del conocimiento e intervención de los demás (…)”, salvo que permitamos la participación de otros en nuestras vidas privadas. Siendo esta relación social la que dota de sentido al derecho a la intimidad.

Este derecho protege, entonces, la esfera privada de la vida propia, su círculo más íntimo, respecto de intromisiones, publicaciones, captación de datos personales, entre otras intervenciones -no autorizadas- por parte de terceros.[85] Asentando, además, la capacidad de las personas para actuar con libertad respecto de cómo desean participar en la vida social.

Estimamos que la privacidad se asocia principalmente con el control sobre la propia persona, lo que se manifiesta en la facultad de poder excluir a terceros del ámbito más íntimo de nosotros mismos, porque ésta “supone

[85] CREVILLÉN. Ob. Cit. pp. 75-77.

sustraer del control público un ámbito de vida que no presente importancia directa en nuestra relación genérica con los demás"[86].

El derecho a la intimidad se encuentra inmediatamente relacionado con la identidad personal, en tanto sería una "garantía a la autonomía personal", ya que cualquier interrupción sustancial de nuestra privacidad atentaría contra nuestra individualidad, puesto que nuestra identidad se vería seriamente disminuida o, incluso –yendo más lejos- utilizada por otro sujeto[87].

La identidad personal y la privacidad tienen como elemento común la dimensión social del ser humano, ya que mientras "en el derecho a la intimidad se facilitan al individuo los instrumentos jurídicos para que delimite las fronteras en sus relaciones sociales", en el derecho a la identidad personal se garantiza al sujeto "el reconocimiento social de un ser

[86] BARROS B., Enrique. La privacidad como exclusión y secreto ante el derecho civil. Versión aún inédita de conferencia dictada en la Facultad de Derecho de la Universidad de Chile, 1997. p. 2. En: COLLANTES y GONZALEZ. Ob. Cit. p. 77.
[87] Ibídem. pp. 77 y 78.

único, con sus cualidades que lo identifican y distinguen de todo otro ser dentro de la sociedad"[88].

Si bien ambas convergen en el terreno de lo social, la identidad personal no puede reducirse a la esfera íntima de la persona, ya que en parte es la proyección que nosotros exteriorizamos en "lo público", es representación de nuestra personalidad, lo que nos hace únicos, irrepetibles e inconfundibles para el resto. Y, aunque la intimida pueda coincidir con ciertos rasgos que forman nuestra identidad, mas su protección hace alusión a la libertad que tiene la persona de reservar para sí determinada información personal y no compartirla con terceros, sin importar si ésta guarda o no directa relación con su identidad.

1.4.2. Derecho al honor

El honor está vinculado con el aspecto más profundo de la persona, en cuanto considera la propia estima que se tiene sumado a la valoración que hacen los demás de uno.

[88] COLLANTES y GONZALEZ. Ob. Cit. p. 82.

Según Adriano de Cupis, “el honor es la dignidad personal reflejada en la consideración de los demás y en el sentimiento de la propia persona.” Esto denota una doble perspectiva, una individual y una social, pudiendo determinarse que el honor es una especie de valoración social de la personalidad. Concepto bastante etéreo que bien podría traducirse como el derecho a ser respetado[89].

En virtud de lo mencionado, el derecho al honor implicaría que “toda persona tiene derecho a la protección de su personalidad ‘moral’, (…) de su reputación”. Ya que, “el honor se identifica con el sentimiento que cada uno tiene de su propia dignidad moral, y designa aquella suma de valores (…) que el individuo se atribuye a sí mismo” (…). Y “la opinión que los demás tienen de nosotros; lo que constituye el patrimonio moral que deriva de la consideración ajena”[90].

[89] CREVILLÉN. Ob. Cit. p. 29.
[90] VODANOVIC. Ob. Cit. pp. 20 y 21.

Al igual que los derechos ya analizados, el derecho al honor se basa en su aspecto social, en cuanto éste adquiere real sentido cuando se instituye respecto de otros, que deben reconocer y respetar la estima de la persona indicada.

Sin embargo, existen casos especiales –que creemos importante mencionar- en que este derecho puede sufrir intromisiones legítimas, pero que por ningún motivo significan que tal derecho pierda la calidad de indisponible.

El primero es el caso en que el interesado diera su consentimiento, lo que se debe entender como una autorización individualizada respecto del tercero, que corresponderá a una mera tolerancia[91].

Y el segundo, es el caso de los personajes público en que, si bien, "el honor en cuanto derecho de la personalidad es atribuido por igual a cada persona, (…) el honor de las personas que tienen un interés para el resto de las demás a causa de una mayor popularidad, se debilita en el sentido de

[91] CREVILLÉN. Ob. Cit. pp. 42 y 43.

que las críticas e informaciones sobre las mismas se ven reforzadas por el derecho de información en aras de un interés general" [92]. Lo cual establecería que, en una situación concreta donde estuvieran estos derechos en conflicto –el derecho al honor y la libertad de expresión o el derecho a información en favor del público- es posible que el derecho al honor pueda transgredirse sin considerarse por ello delito.

El honor y la identidad personal, puede decirse, detentan una relación estrecha, en tanto ambos se proyectan en el exterior de la vida humana, vinculado especialmente con la personalidad de los humanos.

No obstante, el derecho al honor por su parte, apunta más a la protección de la reputación o dignidad de la persona –mirado desde la subjetividad que yace en la valoración que aquellas hacen sobre sí mismas- frente a los menoscabos que pueda sufrir por aseveraciones falsas o negativas que emitan terceros.

[92] CREVILLÉN. Ob. Cit. pp. 57 y 58.

Mientras que, la identidad personal detenta un carácter más objetivo, puesto que en su mayoría se edifica sobre la percepción que los otros individuos tienen respecto de nuestra persona, ya que representa la individualidad de los sujetos en el plano social.[93]

1.4.3. Derecho a la propia imagen.

Como ya lo hemos señalado, la imagen –signo distintivo de la personalidad- es el principal medio de expresión que tiene la persona, en cuanto a través de ésta logra exteriorizar su yo, desplegando su individualidad con el fin de comunicarse con otros.

Actualmente, no hay duda alguna de la autonomía de este derecho, por lo que es lógica la exigencia de protección jurídica que reclama la imagen por sí misma.

Según el profesor Nogueira, "el derecho a la propia imagen tutela la proyección exterior y concreta de la persona en su figura física visible

[93] COLLANTES y GONZALEZ. Ob. Cit. pp. 89-91.

independientemente de la afectación de su honra, de su vida privada y del eventual derecho de propiedad, dotando a la persona de la facultad de decidir sobre el uso de su imagen sin intromisiones ilegítimas, en la medida que expresan cualidades morales de la persona y emanaciones concretas de su dignidad de ser humano, configurando su ámbito personal e instrumento básico de su identificación, proyección exterior y reconocimiento como ser humano"[94].

Podemos deducir que, así como toda persona tiene el derecho a exponerse cuando y donde quiera, se le debe reconocer también, el derecho a prohibir la circulación de su propia imagen de forma pública.

Este derecho sería correlativo, entonces, a la capacidad o facultad de la persona para "controlar lo que ésta desea que sea público, al permitir la captación, reproducción o publicación de su imagen y tiene la capacidad de

[94] NOGUEIRA A., H. 2007. El derecho a la propia imagen como derecho fundamental implícito. Fundamentación y caracterización. [en línea] Revista Ius et Praxis, Vol. 13, Nº. 2, 2007. <http://www.scielo.cl/pdf/iusetp/v13n2/art11.pdf> p. 261.

controlar lo que desea que sea privado, al prohibir o restringir lo que no desea que se difunda", lo que constituiría más bien una libertad.[95] [96]

Mas, de la misma manera que el derecho al honor, estimamos que existen excepciones admisibles al derecho a la imagen, que "solo pueden comprender la justificación de la propia notoriedad del sujeto cuya imagen se ampara, el cargo que desempeña –especialmente los de índole pública-, exigencias de justicia o policía, finalidades científicas, didácticas, culturales, o cuando la imagen es obtenida en lugares públicos, o en acontecimientos de interés público o que han acaecido públicamente. No obstante, un retrato o imagen no puede ser reproducido, ni aún a pretexto de

[95] GONZALEZ K., C. D. 2012. Derecho a la propia imagen: esfera constitucional y legal del derecho a la propia imagen en Chile y en el derecho comparado. Memoria para optar a la licenciatura en ciencias jurídicas y sociales. Santiago, Universidad de Chile, Facultad de Derecho. p. 17.

[96] También debemos agregar que, el derecho a la propia imagen tendría un ámbito patrimonial, en virtud de que la imagen personal es susceptible de adquirir un valor de mercado al ser utilizada comercialmente. Es tal la relevancia de la imagen, que este derecho se encuentra especialmente protegido en algunas legislaciones. Por ejemplo, en Estados Unidos se tutela bajo la forma del "Right of Publicity" –derivado del "Right of Privacy"- con el cual se protege el uso comercial de la propia imagen por terceros sin el consentimiento del respectivo titular. Se entiende que su objeto es la identidad personal, en cuanto no sólo comprende la imagen, sino que incluye además el nombre, la voz o una representación escénica.

las excepciones vistas, si del hecho resulta perjuicio para la honra, reputación o simple decoro de la persona retratada."[97]

En cuanto a su relación con el derecho a la identidad personal, la imagen es signo de identificación, siendo la representación externa más directa de la persona, por ser el principal instrumento de ésta para manifestar la propia personalidad y relacionarse con otros.

El derecho a la propia imagen, por tanto, protege consecuencialmente a la identidad personal, ya que es ésta la que se pone en peligro con la reproducción ilegítima de la imagen, por parte de terceros ajenos, sin la correspondiente autorización.

Empero, la imagen debe diferenciarse de la identidad personal, siendo la primera una proyección de la segunda, sólo un elemento de los que concurren para estructurar la noción de identidad. Pudiendo la imagen, además, ser reproducible a través de medios materiales como fotografías,

[97] VODANOVIC. Ob. Cit. pp.25 y 26.

dibujos o representaciones escénicas, entre otros, susceptibilidad que no detenta la identidad personal.

CAPÍTULO II: IDENTIDAD DIGITAL Y REDES SOCIALES.

1. Identidad digital.

Internet ha generado nuevos patrones de interacción social, en donde existe un mayor esfuerzo, por parte de los usuarios, en determinar quiénes son y cuáles son las características que los identifican.

Actualmente, "la identidad en Internet no está definida con el grado de concreción que ya se tiene en la vida real"[98], es por esto, que analizado lo que entendemos por identidad en el plano físico, pasaremos a revisar qué es la identidad digital y sus principales elementos.

1.1. Qué es la identidad digital

[98] CONSEJO GENERAL del Poder Judicial. 2006. Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad? Madrid, España. p.87.

"El conjunto de características propias de un individuo o de un colectivo en un medio de transmisión digital se conoce como identidad digital"[99]. Teniendo esto en consideración, podemos identificar que la identidad formada en Internet, como por ejemplo en las redes sociales, respondería al concepto de construcción o invención de la identidad, y ya no a la identidad material que está predefinida por el cuerpo. Es así, como hoy existe la posibilidad de inventar una nueva identidad, muchas identidades, o bien, no revelar esta identidad digital.

Las reglas de generación de identidad definitivamente no son las mismas que en el mundo físico, sin embargo, cada día es más importante esta construcción, transformándose ya no en una opción, sino que "un acto de pura responsabilidad"[100], debido a que Internet es parte de nuestra vida cotidiana[101] y por tanto, se necesitará en algún momento tener un correo

[99] Ibídem. p.42

[100] EVOCA COMUNICACIÓN e imagen. [en línea] Cuadernos de comunicación evoca. Identidad digital y reputación online <http://www.evocaimagen.com/cuadernos/cuadernos5.pdf> p.6

[101] Como se ha mencionado en la introducción, Internet ha generado grandes cambios conjuntamente con la revolución tecnológica que se vive. Esta revolución gira en torno al acceso a la información y la comunicación. La que cada vez tiene mayor repercusiones en la vida cotidiana.

electrónico, una cuenta en alguna red social o bien, registrarse en más de un sitio Web para navegar en la red buscando cualquier tipo de información.

La creación de la identidad digital se define como "la habilidad de gestionar con éxito la propia visibilidad, reputación y privacidad en la red como un componente inseparable y fundamental del conjunto de habilidades informacionales y digitales, las cuales se han convertido en fundamentales para vivir en la sociedad informacional"[102]. De esta manera podemos desprender los elementos de visibilidad, reputación y privacidad que analizaremos más adelante.

La generación nacida a partir de los años noventa se les ha denominado "nativos digitales"[103], personas que no han conocido la vida sin Internet, la utilizan todos los días y de manera masiva. Tanto estos como quienes se han incorporado a este fenómeno, han tenido que representarse o identificarse

[102] GIONES V. Aina, SERRAT I B. Marta. 2010. La gestión de la identidad digital: una nueva habilidad informacional y digital. [en línea] BiD: textos universitaris de biblioteconomia i documentació, juny, núm. 24. <http://www.ub.edu/bid/24/giones2.htm> [consulta: 10 de octubre de 2013] p.2
[103] Ídem.

en la red de alguna forma, y esto ha llevado a que cada uno construya un "yo" virtual -en contraposición de la identidad física- que puede ser una identidad reflejo de la material, o bien una nueva, que sea distinta a ésta.

1.2. Construcción de la identidad en Internet.

La construcción de la identidad significa dedicación, tiempo y esfuerzo, mas con el uso habitual de Internet, muchos inconscientemente, dejando una huella[104], han avanzado en la edificación de su identidad digital, la cual "tiene su base en la actividad que ellas mismas desarrollan y el reflejo que ésta tiene en los medios electrónicos"[105]. Basta con realizar acciones en la red como publicar imágenes, comentarios o videos, configurar un perfil de usuario de alguna red social, crear un correo electrónico, tener un Currículum virtual o participar en un blog, entre otras actividades.

---

[104] GAMERO., R. 2009. La configuración de la identidad digital. [en línea] Nota eter. Universitat Politecnica de Valencia. España. 6p. <https://observatorio.iti.upv.es/media/managed_files/2009/06/03/11569.pdf > p. 1.

[105] FERNANDEZ B., P. 2012. Aspectos jurídicos de la identidad digital y la reputación online. [en línea] Revista Científica de Estrategias, Tendencias e Innovación en Comunicación. número 3. p. 125-142 <http://repositori.uji.es/xmlui/bitstream/handle/10234/43024/Pablo%20Fern%C3%A1ndez%20Burgue%C3%B1o.pdf?sequence=1> p.128

Internet se ha convertido en un espacio libre por definición, donde las personas pueden expresar lo que sienten, lo que quieren, sus intereses, lo que les molesta o en definitiva todo aquello que los hace ser ellos mismos y no otros. En un estudio realizado por Sherry Turkle, una de los entrevistados expresó que, gracias a Internet: "Puedo dividir mi mente. Cada vez se me da mejor. Puedo verme a mí mismo como dos, tres o más personas. Cuando voy de ventana en ventana, activo primero una parte de mi mente y, luego otra. La vida real no es más que otra ventana, y no necesariamente la mejor que tengo"[106], lo que reafirma la idea que la Web permite a todos los usuarios una libertad que en el mundo físico no existe.

"La construcción de la propia identidad digital pasa por definir qué, cómo y dónde se va a comunicar en Internet"[107], debiendo participar de forma activa, puesto que somos de la opinión que "la identidad digital se configura a partir de los contenidos accesibles a través de medios

[106] SIMPOSIO ARGENTINO de informática y derecho. Suplantación de identidad digital como delito informático en Argentina. 27 y 28 de agosto de 2004. Buenos Aires, Argentina. <http://www.41jaiio.org.ar/sites/default/files/7_SID_2012.pdf > p. 88.
[107] EVOCA COMUNICACIÓN. . Ob. Cit. p.8

electrónicos y, por tanto, empieza a crearse desde el primer rastro que se deja en Internet, que no tiene que haber sido dejado por la propia persona"[108]. Con esto, intentamos expresar que cualquier acción realizada en Internet quedará ligada a quien la realice y desde ese punto de partida se construye la posición digital[109].

El computador se ha convertido en una herramienta indispensable para miles de personas, aportando a su desarrollo personal y permitiendo la comunicación, tal como un espejo que puede ser atravesado para pasar a un mundo virtual[110], que -para Manuel Castells- "es una extensión de la vida tal como es, en todas sus dimensiones y modalidades"[111].

Sin embargo, la idea de que la vida a través de la pantalla es una prolongación del mundo real, no es para todos igual, ya que la libertad otorgada por Internet permite a los usuarios elegir quién ser en la red, todo de acuerdo al "autoestima o la consciencia que se tiene de ser uno mismo y

[108] FERNANDEZ . Ob. Cit. p. 127
[109] Concepto adoptado por Rosaura Alastruey en El networking
[110] TURKLE, S. 1997. La vida en la pantalla: la construcción de la identidad en la era de Internet. 1ª ed. Barcelona; Paidós. p.15
[111] CASTELLS., M. 2001. La Galaxia internet. Areté, España. p.137

distinto a los demás en comunidades virtuales o medios sociales online"[112] [113].

A modo de resumen, en Internet, las personas eligen su identidad en virtud de la imagen que se desee dar de sí mismo, siendo fieles a su realidad física o tomando en consideración la percepción que puedan tener los demás usuarios en la red.

1.3. Reputación en Internet

La identidad virtual se edifica a través de la imagen que se quiera proyectar de uno mismo, sumado a la interpretación de aquella identidad por parte de terceros. Tal percepción que tienen los demás usuarios de la identidad digital que construye cada uno la llamaremos reputación online.

[112] FERNANDEZ. Ob. Cit. p.127.

[113] Nancy Bayman afirma en su estudio sobre el comportamiento de las comunidades online que "la realidad parece indicar que muchos, probablemente la mayoría de los usuarios sociales de la comunicación mediante ordenador, crean sus propias identidades online coherentes con sus identidades offline" En: CASTELLS. Ob. Cit. p.139.

Con el fin de analizar esta idea, se debe tomar en consideración que la información que es publicada en Internet permanece allí de forma definitiva, y que generalmente, el medio que se utiliza para divulgar estos antecedentes es administrada por un tercero que no necesariamente va a estar de acuerdo con retirar de la red lo que la persona ha publicado si este lo solicita, ya que es común que la difusión de la información en Internet se haga por medio de la copia.[114]

La reputación es un concepto que existe mucho antes del desarrollo de Internet y que constituye tanto "un elemento esencial para la pertenencia a la comunidad como para establecer el rango dentro de la misma"[115]. El problema que se origina hoy, es que en Internet toda la información, imágenes, videos o cualquier documento circula a una velocidad inimaginable, lo que hace por una parte, más fácil su localización y por otra, dificulta que sea eliminada u olvidada por los usuarios. Es así, como la

[114] Se señala que desde que algo se publica en Internet, esto comienza a ser replicado de forma infinita, es decir, que no existe un límite de veces ni de formas. De esta manera, la facilidad de la copia, sumado al gran número de usuarios hace que las posibilidades de que el contenido sea fácilmente público. En: EVOCA COMUNICACIÓN. Ob. Cit. p.7

[115] CASTELLS. Ob. Cit. p.54

reputación digital ha tocado distintos sectores de la sociedad, generando una preocupación cada vez mayor respecto del ideal que cada persona forma en Internet, principalmente por el acceso sin limitaciones que se tiene a esta información.

En la propia reputación se invierte una cantidad considerable de tiempo y dedicación, todo lo cual termina careciendo de valor cuando cambia exterioriza la opinión que tienen de los demás de uno y ésta se exterioriza para que otros la conozcan. En el caso de la reputación virtual, este fenómeno es aún más drástico porque la misma puede ser arruinada más fácil y rápidamente.

Resumiendo, la reputación o percepción que terceros tengan de una persona se generará de forma natural, fuera del control humano, pero el uso que el usuario le dé a Internet o la interacción que tenga con otros, podrá ayudar a encauzarla[116].

1.3.1. La firma electrónica

[116] EVOCA COMUNICACIÓN. Ob. Cit. p.8

En respuesta a la modernización que han sufrido los sistemas de comunicación a causa del avance tecnológico, el hombre ha debido extrapolar las herramientas que utiliza en el día a día para desenvolverse, teniendo que crear un equivalente de la firma en el mundo electrónico. Es así como tanto a nivel nacional como internacional, con el fin de facilitar ciertas transacciones de variada índole y reducir determinadas amenazas, hoy es amplio el uso de la firma electrónica.

Como plantea Magán Perales, los mayores riesgos en los sistemas electrónicos son los siguientes: "a) Que el autor del mensaje haya sido suplantado (por ello, lo principal es garantizar la identidad); b) Que el mensaje sea alterado (integridad del mensaje); c) Que el emisor del mensaje niegue haberlo transmitido o el destinatario recibido (rechazo), al igual que ocurre con las notificaciones escritas, y d) Que el contenido del mensaje sea leído por una persona no autorizada (confidencialidad)"[117]. Con la firma electrónica se pretende resolver el primer problema, esto es confirmar la

[117] ADMINISTRACIONES PÚBLICAS y nuevas tecnologías. 2005. Josefa Cantero "et al". Lex Nova, España. pp. 94 y 95.

identidad del remitente del mensaje o documento, intentando cumplir el mismo objetivo que el de una firma manuscrita, "identificar a una persona, proporcionar certidumbre sobre su participación personal en el acto de la firma y vincular a esa persona con el contenido del documento."[118]

La tendencia internacional ha sido legislar sobre el tema[119] y Chile no quiso quedar fuera de este desarrollo, por lo que el año 2000 se presentó el

[118] UNCITRAL. 2001. Ley modelo de la CNUDMI sobre firmas electrónicas con la guía para su incorporación al derecho interno. [en línea] 91p. <http://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf> p.23

[119] La primera ley sobre firma electrónica se aprobó en 1995 en el Estado de Utah, Estados Unidos, en donde se regula la firma electrónica en base al sistema de criptografía, la que además de reconocer las consecuencias jurídicas de las firmas electrónicas, da a ésta el mismo valor que la manuscrita. Siguiendo con esta línea, otros Estados como Georgia, California, Washington entre otros, comenzaron a legislar por la eficacia que representa para el comercio electrónico.
Posteriormente, se desarrolló una ley modelo de UNCITRAL en 1996, que tuvo por objeto establecer ciertas recomendaciones para tener en consideración a la hora de que los distintos Estados legislaran sobre el tema. En este sentido, la ley modelo adopta el criterio de "equivalente funcional", que consiste en reconocer que los documentos otorgados por medios electrónicos pueden ofrecer un grado de seguridad equivalente a la del papel o incluso mayor.
Dentro del continente europeo, Alemania fue el primer país en pronunciarse sobre la firma electrónica en 1997 y la Unión Europea, el 24 de mayo de 1999 dictó la Directiva de la Unión Europea sobre un Sistema Común para Firmas Electrónicas, la que repite lo indicado por la ley modelo, en donde la

proyecto de ley que buscaba legislar respecto a la firma electrónica. Así, el 12 de noviembre de 2007 se promulgó la ley 19.799 "Sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firma".

Esta ley, en su artículo segundo, define dos conceptos fundamentales referentes a este tipo de firma.

Artículo segundo letra f) "Firma electrónica: cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar al menos formalmente a su autor;"

Artículo segundo letra g) "Firma electrónica avanzada: aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del

---

firma electrónica adjuntada a un documento electrónico tiene el mismo valor legal que la firma manuscrita.

titular e impidiendo que desconozca la integridad del documento y su autoría"[120]

[120]Cabe destacar lo señalado por el profesor de Derecho Comercial, señor Ricardo Sandoval López en el informe de la Facultad de Derecho de la Universidad de Concepción respecto del Proyecto de Ley sobre Firma Electrónica y Servicios de Certificación de Firma Electrónica en el contexto del primer informe de la Comisión de Constitución: "Recapitulando, digamos que la Firma electrónica satisface tres funciones, a saber: a) función de identificación y atribución del mensaje y de la información contenida en él, indicación del origen y de la voluntad del emisor; b) función de privacidad, cifrado del mensaje y del nombre del Firmante, y c) función de seguridad e integridad- prueba la apertura o la alteración del mensaje entre el momento de sus emisión firmada y el instante de su llegada a manos del destinatario.
El problema que se suscita al legislar sobre esta materia es la existencia de diversas tecnologías para firmar electrónicamente y en consecuencia la opción que ha de hacerse para que la tecnología elegida satisfaga las distintas funciones de la FE. De las opciones disponibles para estampar la FE, algunas son completas en cuanto a que cumplen las tres funciones indicadas y otras son incompletas porque no llegan a todos esos roles. Sin embargo, no es dable negar los efectos jurídicos de ninguna de ellas, aunque se limiten al efecto esencial de identificación y atribución.
El Proyecto de Ley distingue y define por separado, en el artículo 2°, letras f) y g), respectivamente, los conceptos de FEA y de FE. En otras palabras primero hace una definición completa o integral y luego una definición elemental de FE.
La FE simple, definida en el artículo 2° letra g), de la iniciativa legal en estudio, como "cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar, al menos formalmente, a su autor", sólo satisface la función de identificación del autor del mensaje de datos, con olvido deliberado de otras funciones significativas. Era necesario consagrar legislativamente este tipo de FE, como lo hace la iniciativa legal, en aplicación del principio de no discriminación y, en cierta medida, en observancia de la idea de neutralidad

Las definiciones incorporadas en el artículo precedente, en conjunto con lo establecido en el artículo 3º de la Ley[121], hacen un significativo aporte,

---

tecnológica. Desde luego, los alcances jurídicos de la FE simple no pueden ser los mismos que los de la FEA, pero es necesario dejar libertad de los operadores del CE para que suscriban electrónicamente sus mensajes de datos, atendiendo a la importancia económica y jurídica de los mismos. Así un mensaje de datos que contenga una simple oferta de celebrar un contrato será suscrito mediante una FE simple, en tanto que, un documento electrónico que contenga el envío de una importante suma de dinero, será suscrito con una FEA. (…)

La FEA, por ser un mecanismo más completo, satisface las funciones de identificación, atribución, privacidad, integridad y seguridad, toda vez que se apoya en la denominada Infraestructura de Clave Pública (ICP), expresión que proviene de su nombre en idioma inglés Public Key lnfrastructure (PKI). Ella es puede asegurar, en el estado actual de la técnica, incluso con mayores garantías que el papel y la firma autógrafa, la identificación del Firmante y la atribución de los mensajes de datos. Igualmente la ICP mantiene la seguridad y privacidad respecto de los mensajes de datos, durante todo el recorrido desde el momento de emisión hasta el de la recepción.

La definición del concepto de FEA que propone la iniciativa legal, contenida en el artículo 2° letra f), es acertada en la medida en que describe las tres funciones básicas que ella debe cumplir y concuerda con las exigencias propias de la tecnología en que se basa. La lectura de esta definición puede dejar al lector estupefacto en la medida en que no se le haya conducido por el terreno puramente técnico. En verdad, sin emplear en la redacción de la norma la expresión criptosistema asimétrico, que es lejana al mundo del Derecho, contempla las exigencias de doble clave para describir la FEA."

[121] Artículo 3º.- Los actos y contratos otorgados o celebrados por personas naturales o jurídicas, suscritos por medio de firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escrito y en soporte de papel. Dichos actos y contratos se reputarán como escritos, en los casos en que la ley exija que los mismos consten de ese

toda vez que equipara de manera amplia los actos y contratos suscritos por medio de firma electrónica. Esto significa que tendrán el mismo valor probatorio en juicio que aquellos documentos otorgados de forma manuscrita, ya sea como instrumento público o instrumento privado.

1.3.2. Documento nacional de identidad electrónico

El documento nacional electrónico o DNI electrónico es un instrumento público que contiene datos personales, otorgado por un funcionario público competente, que permiten la identificación personal de quien lo posee. De esta manera, por ser otorgado por el administrativo correspondiente, este documento permite a la persona que lo tiene en su poder identificarse de forma personal o virtual en todos los ámbitos de su vida, en especial en aquellos que revisten el carácter de solemne y público[122].

---

modo, y en todos aquellos casos en que la ley prevea consecuencias jurídicas cuando constan igualmente por escrito.

[122] Físicamente se trata de un artículo similar a una tarjeta de crédito que contiene un chip que permite que las personas naturales puedan firmar digitalmente documentos electrónicos.

A pesar de que este instrumento no se ha sido masificado a nivel mundial, podemos actualmente contar al menos cinco Estados en que hoy tiene vigencia. A modo de ejemplo, podemos identificar el caso de Alemania, en donde se emplea este documento desde noviembre de 2010 y se compone por un número de 6 dígitos que corresponden a un chip, una foto de la persona, la fecha de nacimiento, la firma y la huella digital, entre otras cosas. Bélgica por su parte, ha sido pionero en este ámbito, incorporando este sistema desde el año 2002, pero teniendo un mayor impacto en su utilización desde el 2004, año desde el cual todos los documentos de identidad emitidos son electrónicos. Seguidamente España e Italia también optan por legislar sobre el documento de identidad electrónico en el año 2006 y más recientemente es Rumania, quien se ha unido a esta tendencia en el año 2011.

1.4. Derecho a la intimidad y la privacidad en Internet.

El derecho a la privacidad e intimidad tiene su nacimiento a finales del siglo XIX, cuando “por primera vez se hablaba de un derecho a la vida sin

dependencia de la propiedad" [123] y como analizamos anteriormente, el derecho a la privacidad se asocia con la libertad que tiene el hombre con su persona y con los actos que realiza, ya que los consideramos como exclusivos y reservados para él.

En el ciberespacio ocurre algo similar, toda vez que este derecho es inherente a la persona, traspasando el mundo físico, tal como la Constitución Política de la República lo recoge en el artículo 19 número cuatro:

"La Constitución asegura a todas las personas: 4) El respeto y protección a la vida privada y a la honra de la persona y su familia".

Sin distinguir si esta protección debe darse en el ámbito físico o el virtual.

[123] DAFFAU G., F. 2008. Derecho a la privacidad, su contenido esencial, limitaciones y colisión con otros derechos fundamentales. Memoria para optar a la licenciatura en ciencias jurídicas y sociales. Santiago, Universidad de Chile, Facultad de Derecho. p.74

En Internet es posible, si el usuario se preocupa de hacerlo de ese modo, el mayor resguardo de aquellos aspectos privados de la vida de una persona, ya que el usuario tiene la libertad de difundir sus ideas y elementos reservados de su vida, como puede también elegir no exhibirlos. Es por este motivo que, no podemos excluir el derecho de ocultarse que tiene todo usuario de Internet como parte de su derecho a la intimidad o privacidad, por lo que a continuación analizaremos con mayor detención el derecho al anonimato.

1.5. Derecho al Anonimato en Internet.

Internet, como se ha mencionado es un instrumento que permite tener amplia libertad para transmitir ideas, pensamientos, imágenes, información, etc., lo que tiene su máxima expresión en el Derecho al Anonimato, que permite al usuario compartir información como emitir opinión adjudicándose tal contenido como si lo hubiese publicado cualquier persona en un universo infinito de ordenadores, siendo a su vez tan difícil de controlar que logra ser garantía de la privacidad. Tal como plantea Castells, en los inicios de Internet “la privacidad estaba protegida por el anonimato

de la comunicación en Internet, así como por la dificultad de rastrear las fuentes e identificar el contenido de los mensajes transmitidos por medio de los protocolos de Internet"[124], sin embargo, esto ha ido cambiando con el tiempo como lo veremos más adelante.

Es muy distinto el caso del anonimato en el "mundo real" al derecho que se tiene en Internet. En el mundo físico, "una buena parte de nuestra identidad queda develada independiente de nuestra voluntad"[125], es decir que las personas para pasar desapercibidas o anónimas en un lugar, como la calle por ejemplo, tendrían que intencionalmente disfrazarse u ocultarse, ya que resulta inevitable que al circular no sea identificada por los distintos aspectos corporales que forman su identidad, como son el color de pelo, la estatura, etc., y aquellos elementos que son acreditados por medio de documentos como cédula de identidad para reconocer el nombre, la nacionalidad, etc.

[124] CASTELLS. Ob. Cit. p.193
[125] LESSIG., L. 2001. El código y otras leyes del Ciberespacio. Editorial Grupo Santillana de Ediciones, Madrid. p. 68.

En el ciberespacio, ocurre algo muy distinto, por cuanto no existen elementos tan simples que permitan identificar a quien se encuentra del otro lado de la pantalla. “El sistema capta que hay entidades externas interactuando con él, pero no sabe nada acerca de ellas. Mientras que en el espacio real –y ésta es la cuestión fundamental- el anonimato ha de crearse, en el ciberespacio el anonimato viene dado por defecto”[126].

Según Castells, este paradigma de libertad estaba basado en dos fundamentos. El primero es tecnológico, toda vez que su arquitectura estaba construida sobre la base de la conexión informática en redes sin restricciones, mientras que el segundo es institucional, ya que Internet se desarrolló primeramente en Estados Unidos, quedando amparado bajo la protección de la libertad de expresión de ese país[127]. Así, sumando estos dos elementos, podemos identificar las razones del rápido y masivo desarrollo de Internet, que junto con la falta de control durante muchos años, trajo diversos problemas a los países que han intentado frustradamente regularlo mediante medios tradicionales de censura y represión.

[126] LESSIG. 2009. El código 2.0. Traficantes de sueños, Madrid, España. 563p.
[127] CASTELLS. Ob. Cit. p.193

No obstante la creencia de que es posible un anonimato absoluto en la Web, cada día se hace más fácil perseguir o rastrear a una persona siguiendo las estructuras de control que se han cimentado a lo largo de los años con el objeto de identificar a los sujetos, ya que "a medida que se construye una Capa de Identidad en Internet, aumenta la posibilidad de exigir alguna forma de identidad como condición para acceder a los recursos de la Red"[128].

Tal como plantea Castells, en un principio, el uso de Internet estaba marcado por la privacidad, manteniendo información en secreto, pero actualmente y en el futuro irá apuntado a la regulación de la red mediante el uso de tecnologías de control, de vigilancia y de investigación[129].

[128] LESSIG. El código 2.0. Ob. Cit. p.105.
[129] CASTELLS. Ob. Cit. pp.195-196

Así, se puede señalar que en el plano de la identidad lo único que se tiene es un número IP[130], mas debe tenerse en consideración que "un vínculo a una dirección IP, sin embargo, sólo facilita el rastreo y, de nuevo, incluso en ese caso se trata de una rastreabilidad imperfecta"[131] y que "la dirección IP en sí misma no revela nada acerca de quién es alguien, o de qué espacio físico procede, pero sí que permite un cierto grado de rastreo. Si (1) hemos accedido a la red a través de un proveedor de servicios de Internet que nos asigna una dirección IP mientras estamos conectados, y (2) ese PSI conserva los registros de dicha asignación"[132].

1.5.1. Concepto de derecho al anonimato en la red

El Derecho al Anonimato lo definimos como "la capacidad de realizar cualquier acceso, comunicación o publicación en la red sin que terceros

[130] "los operadores. no tienen manera de saber –al menos con la información que proporciona el protocolo TCP/IP- si la identidad que entra en su página es un niño o un adulto". En: LESSIG. El código 2.0. Ob. Cit. p.92
[131] LESSIG. El código 2.0. Ob. Cit. p.95.
[132] LESSIG. El código 2.0. Ob. Cit. p.93.

tengan la posibilidad de identificar o localizar al autor de dicha acción"[133] o en otras palabras, es el derecho que tiene cualquier usuario de Internet de mantener oculta su identidad ante terceros.

Actualmente, para gozar de anonimato se requiere un esfuerzo adicional, ya que el uso común de Internet se ha vuelto rastreable[134], por lo que sólo un experto lograría ser anónimo, ya que pudiendo borrar las huellas dejadas en la red es posible que su identidad permanezca libre de indagación.

Analizado esto desde el punto de vista de la protección del usuario, el derecho al anonimato, en el ámbito virtual, es aquel que permite la protección del usuario en su esfera privada, mientras que si decide renunciar a su anonimato, no por ello estará renunciando a la protección de su privacidad o intimidad[135].

---

[133] DE SALVADOR C., L. 2012. Redes de anonimización en internet: cómo funcionan y cuáles son sus límites. España. 13p. <http://www.ieee.es/Galerias/fichero/docs_opinion/2012/DIEEEO16-2012_RedesAnonimizacionInternet_LdeSalvador.pdf> p.2

[134] LESSIG. El código 2.0. Ob. Cit. p.93.

[135] CABEZAS L., P. y MOYA M., F. 2008. El derecho al anonimato del usuario de internet. Memoria para optar a la licenciatura en ciencias jurídicas y sociales. Santiago, Universidad de Chile, Facultad de Derecho. 189 h. p.21

1.5.2. Problemas que origina ser anónimo

La existencia del derecho al anonimato ha traído consigo una serie conflictos. En primer lugar, destaca el hecho de que ser anónimo significa una ventaja para la realización de actividades delictivas en Internet. Así, "el ciberespacio es diferente por el alcance que proporciona y también por el anonimato que permite" [136], o en otras palabras, este medio permite esconderse -a pesar de los distintos métodos de identificación que existen- más fácilmente que en el mundo físico y, por consiguiente, para poder identificar a los autores de estos delitos –así como los cómplices y encubridores- el anonimato hace más difícil esta tarea[137].

Otro problema es aquel relacionado con la libertad que otorga el anonimato para poder publicar contenidos difamatorios o injuriosos o fotografías de carácter íntimo que afecten a terceros. Por lo general los reclamos se hacen contra los Proveedores de Servicios de Internet por el contenido de esas declaraciones, pero esto no da la seguridad de encontrar

[136] LESSIG. El código 2.0. Ob. Cit. p.57.
[137] DE SALVADOR. Ob. Cit. p.2

al autor, ya que como mencionamos antes, la dirección IP ayuda a rastrear el equipo en donde se difundió el contenido, mas no la identidad de quien lo publica –como es el caso de quien hace una declaración de este tipo en un computador de un cibercafé-[138].

2. Las redes sociales: Nuevas plataformas de interacción

2.1. Origen y desarrollo de las redes sociales: la web 2.0

El desarrollo que ha tenido Internet ha sido un largo proceso, en donde se puede distinguir el cambio de la Web 1.0 a la Web 2.0.

La Web 1.0 en sus inicios tenía como característica principal ser muy estática, lo que implicaba que la participación e interactividad de los usuarios con las páginas era nula, ya que estos no podían comentar ni publicar absolutamente nada. Ésta nace en los años 60`s de una forma muy básica, conformándose como un lugar de lectura, con contenidos de textos como ELISA, lo que luego evolucionó hasta la utilización del formato HTML, que si bien lo hacía más agradable a la vista, todavía significaba

[138] CABEZAS y MOYA. Ob. Cit. p.38

tener documentos en las páginas que nunca se actualizaban, lo que impedía que la información fuera renovada[139].

Producto de los avances y el deseo de los usuarios de participar más activamente en Internet, la Web 1.0 -catalogada como estática- pasó a ser una Web 1.5, mucho más dinámica que la anterior, hasta llegar a la Web 2.0, colaborativa[140] y cuna de las redes sociales.

La Web 2.0 o Web social -concepto acuñado por Tim O`Reilly- surge el año 2004 debido a la necesidad de crear una Web que estuviera acorde con los cambios y avances en Internet, que permitiera la participación, interacción y creación de contenido por parte de los usuarios, la que se ha considerado como "el fenómeno socio-tecnológico más significativo de las últimas décadas"[141], distinguiéndose de la Web 1.0 principalmente porque los mismos eran vistos en ésta sólo como consumidores[142].

---

[139] GOOGLE.SITES. Web 1.0 historia. [en línea] <https://sites.google.com/site/web10historia/>

[140] GARCIA A., L. 2007. ¿Web 2.0 vs Web 1.0? [en línea] Editorial BENED. 8p. <http://ddd.uab.cat/pub/dim/16993748n10a4.pdf> p.4

[141] EVOCA COMUNICACIÓN. Ob. Cit. p.30

[142]GARCIA. Ob. Cit. p.3

Dentro de sus características más importantes, podemos encontrar que tiene mayor interactividad, lo que mejora la relación entre los usuarios, promueve un aprendizaje colaborativo, es multidireccional al existir facilidad de opiniones y respuestas de millones de destinatarios, y concede libertad de edición y difusión[143]. Además, podemos señalar que la Web 2.0 es una plataforma en donde la información y contenidos se almacenan no en lugares físicos, sino que en la misma web, lo que recibe el nombre de "Cloud Computing" o "La nube".

Gracias a esta evolución en la Web, ha cambiado la forma en que entendemos Internet, donde se "presenta como un factor acelerador y amplificador de la extraordinaria habilidad de las personas para comunicar sentido, significados e ideas abstractas de forma social y colectiva"[144], toda vez que "el ciberespacio evoca o engendra, maneras de interactuar que antes no eran posibles"[145] y uno de las modificaciones más relevantes es la evolución de las redes sociales, que si bien existían hace tiempo, muchas

[143] Ibídem. p.2
[144] EVOCA COMUNICACIÓN. Ob. Cit. p.31
[145] LESSIG. El código 2.0. Ob. Cit. p.147

otras nacieron y se han desarrollado en este contexto reuniendo a millones de personas.

2.1.1. Las redes sociales

Como dijimos, las comunidades han existido desde tiempos remotos como forma de vida, por lo que las redes sociales, no son algo nuevo. Sin embargo, el ciberespacio "no se limita a hacer la vida más fácil: la hace diferente, o quizás mejor, dando lugar a una vida distinta (una segunda vida)"[146], donde podemos encontrar una forma distinta de interactuar.

El concepto de red social, nace de un término teórico-sociológico propuesto inicialmente por Frigyes Karimthy con la teoría de los "seis grados de separación", que establece, que cualquier persona puede conocer, interactuar o relacionarse con otra en el mundo con sólo seis enlaces o conexiones[147]. Con esto, se puede entender, que entre cada persona, sin

[146] Ídem. p.147

[147] BARRIUSO R., C. 2010. Las Redes Sociales y la protección de datos hoy [en línea] Memorias. XIV Congreso Iberoamericano de Derecho e Informática. Tomo I "Revolución Informática con Independencia del Individuo", Nuevo León, México: Universidad Autónoma de Nuevo León.

importar su ubicación geográfica, podría conocer a otra "a través de una cadena de conocidos que no tiene más de cinco intermediaros, conectando a ambas personas en tan sólo seis clicks"[148]

Marta Rizo señala que las redes sociales son "formas de interacción social, espacios sociales de convivencia y conectividad"[149], en donde "el atributo fundamental es la construcción de interacción para la resolución de problemas y satisfacción de necesidades. Su lógica no es la de homogeneizar a los grupos sociales, sino la de organizar la sociedad en su diversidad, mediante la estructuración de vínculos entre grupos con intereses y preocupaciones comunes."[150]

---

pp. 81 – 104. <http://biblio.juridicas.unam.mx/libros/6/2940/7.pdf> [consulta:] p.81

[148] Ídem.

[149] RIZZO G., M. Redes. Una aproximación al concepto. [en línea] Barcelona, España. 7p. <http://www.cecaargentina.com.ar/documentosinteres/redes.pdf> [consulta:] p.1

[150] Ídem.

Las redes sociales son estructuras muy antiguas de la actividad humana[151], pero con el invento y desarrollo de la Web 2.0, han cobrado una nueva vida, dando paso a la creación de plataformas que aprovechan los beneficios que ofrece Internet, logrando mayor interacción de los usuarios, siendo ellos quienes eligen la información y contenido que fluye, creando puntos en común, donde puedan compartir sus intereses y problemáticas en un lugar que no es físico y que permite unir a personas de todo el mundo por las facilidades que entrega la conectividad.

El concepto de red puede analizarse desde dos puntos de vista. Por un lado, se considera redes "todos los conjuntos de interacción que se dan de forma espontánea"[152] y por otro, siendo el más importante, "las redes pretenden organizar esas interacciones espontáneas con un cierto grado de formalidad, en el sentido de establecer intereses, problemáticas, preguntas y fines comunes."[153] Esto último, se relaciona con lo que conocemos como redes sociales, siendo un espacio de interacción con ciertas formalidades, representadas generalmente por el contrato que el usuario acepta al

[151]CASTELLS. Ob. Cit. p.15
[152] RIZZO. Ob. Cit. p.1
[153] Ídem.

momento de inscribirse en ellas, el que regula lo que está permitido y las actividades en que este participa, lo que varía según el proveedor.

Las redes sociales “on line” son relativamente nuevas, tendiendo como características fundamentales; en primer lugar, el valor de la comunicación horizontal y libre, y en segundo lugar, la conectividad autodirigida, es decir, la capacidad de cualquier persona para encontrar su propio destino en la red[154].

Ante este nuevo fenómeno surgido a mediados de los años 90, existen distintas formas de clasificarlas atendiendo a su dimensión antropológica, evolutiva y tipológica.[155]

La dimensión antropológica mira a las redes sociales desde dos perspectivas, una en sentido amplio, que engloba tanto a las que se desenvuelven en el plano físico como en el virtual, considerando que son

[154] CASTELLS. Ob. Cit. pp.70-71

[155] DELPIAZZO., C. Enfoque jurídico de las redes sociales. [en línea] Revolución informática con independencia del individuo. XIV Congreso Iberoamericano de Derecho e Informática, Monterrey. pp. 277-291<http://biblio.juridicas.unam.mx/libros/6/2940/18.pdf> pp. 281-283

ante todo, una forma de interacción entre personas. Mientas que aquellas llamadas en sentido estricto sólo se refieren a las creadas en el mundo on line, las cuales permiten a los usuarios generar un perfil desde el cual hacer público datos de carácter personal y que proporcionan herramientas que permiten interactuar con otros usuarios y localizarlos[156].

La dimensión evolutiva, se refiere al proceso que han vivido las redes sociales como fenómeno relativamente nuevo, considerando que nacen a mediados de la década de los noventa, donde algunas plataformas virtuales abrieron la posibilidad de que los usuarios se crearan perfiles personales y agregar amigos, tales como AsianAve, BlackPlanet, MiGente, Ryze.com y Tribe.net[157].

Posteriormente, el crecimiento de este tipo de redes fue destinado a que los usuarios compartieran todo tipo de contenidos como; Flickr, donde se comparten fotos, LastFM, donde se comparten intereses musicales, Youtube, con videos, entre otras. Mas, con la llegada de otras plataformas

[156] Ibídem. p. 281
[157] Ídem.

más completas como Facebook y posteriormente Twitter[158], el fenómeno de las redes sociales ha alcanzado su máxima prosperidad.

Por último, la dimensión tipológica distingue las redes sociales en función del público al que se dirigen -las redes sociales generalistas o de ocio y las profesionales[159] [160]-, o de acuerdo al tipo de contenido que contemplan.

Las redes sociales generalistas o de ocio, tienen como objetivo "facilitar y potenciar las relaciones personales entre los usuarios que la componen"[161], siendo claro ejemplo de esto los casos de Facebook y Twitter, ya que ofrecen distintas aplicaciones y funcionalidades que permiten a los usuarios realizar su vida cotidiana en torno a estas plataformas.

---

[158] Ibídem. p. 282

[159] AGENCIA ESPAÑOLA de Protección de Datos., Instituto nacional de tecnologías de la comunicación. 2009. "Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales on line". España. 158 p. p.40 y siguientes.

[160] DELPIAZZO. Ob. Cit. p. 282

[161] AGENCIA ESPAÑOLA. Ob. Cit. p.40.

Dentro de esta clasificación -llamadas generalistas-, podemos identificar una subclasificación de acuerdo a la finalidad de las mismas[162], las primeras son aquellas plataformas de intercambio de contenidos e información –tales como YouTube, Flickr o LastFM- en donde se ponen a disposición de los usuarios herramientas para la publicación e intercambio de contenidos digitales. Un segundo tipo son aquellas basadas en perfiles –como las cuentas de Facebook, Tuenti, Orkut, etc.- que es el más representativo dentro de las redes sociales de ocio[163]. Y finalmente, podemos identificar las de microblogging o nanoblogging –como Twitter o Yammer- que "basan su servicio en la actualización constante de los perfiles de los usuarios mediante pequeños mensajes de texto"[164], las que son publicadas en el perfil del dueño de la cuenta y a la vez en la página de sus seguidores.

Por otro lado, las redes sociales de contenido profesional son aquellas que "están creadas y diseñadas con la finalidad de poner en contacto y mantener la relación a nivel profesional con diferentes sujetos que tengan

[162] Ibídem. p.41
[163] Ibídem. p.42
[164] Ídem.

interés para el usuario"[165], como LinkedIn, donde el usuario puede generar una especie de currículum virtual facilitando diversas oportunidades dentro del campo laboral.

Cabe destacar que toda la información personal que los usuarios entregan a estas redes sociales aunque sea sólo para configurar una cuenta, es más que suficiente para crear una identidad digital, ya que ésta se va formando automáticamente gracias a las actividades que se registren por parte de la personas, por este motivo, compartimos la opinión de Barriuso, quien señala que la persona "debe saber que su identidad digital y sus relaciones sociales en línea repercuten en la vida real, que a la vez retroalimenta su identidad digital" [166], toda vez, que el usuario va configurando esta identidad con todas las intervenciones que realiza.

2.1.1.1. Facebook

[165] Ibídem. p.43.
[166] BARRIUSO R. Ob. Cit. p.82

2.1.1.1.1. Origen y desarrollo de Facebook

Facebook nace de la mano de la web 2.0 el año 2004, cuando el entonces estudiante de la Universidad de Harvard, Mark Zuckeberg creó una plataforma destinada a las Universidades más prestigiosas de Estados Unidos llamada "TheFacebook" en alusión a los "Facebook" o libros que editan estas universidades a principio de cada año para que sus estudiantes puedan conocerse, ya que en ella aparece una fotografía y el nombre de los alumnos[167].

Zuckerberg llevó esta idea a Internet con el objetivo de que los alumnos de su casa de estudio pudieran conocerse virtualmente, lo que luego se extendió a otras universidades en Estados Unidos y posteriormente al resto del mundo[168].

[167] ROA N., M. A. 2013. Facebook frente al derecho a la vida privada y la protección de datos personales. Memoria para optar a la licenciatura en ciencias jurídicas y sociales. Santiago, Universidad de Chile, Facultad de Derecho. p. 68

[168] COMPUTACIÓN APLICADA al Desarrollo. "Historia de Facebook" (sin fecha), [en línea]: <http://www.cad.com.mx/historia_de_facebook.htm>

Una vez iniciada la plataforma, su uso se masificó rápidamente, considerando que en las primeras 24 horas contaba con 1.200 alumnos de la Universidad de Harvard[169] y al primer mes ya se habían suscrito más de la mitad de los estudiantes de la misma. Luego siguió la expansión a las universidades MIT, Boston University y Boston College, entre otras. Al año de su creación, con más de un millón de usuarios, recibió apoyo financiero[170] y se eliminó el "The", quedando el dominio facebook.com[171].

Posteriormente, Facebook siguió con la expansión que ya había iniciado, ahora, dirigida a escuelas y universidades extranjeras, logrando en 2006 que la plataforma se hiciera pública, permitiendo que cualquier persona teniendo un correo electrónico pudiera formar parte de esta comunidad[172] [173].

[169] CROFT., C. 2007 A brief history of The Facebook. [en línea] 18 de diciembre. <http://charlenegagnon.files.wordpress.com/2008/02/a-brief-history-of-the-facebook.pdf> p.1.
[170] COMPUTACIÓN APLICADA. Ob. Cit.
[171] GRUVIX FREEWARE. 2013. Historia 2.0: Cómo nació Facebook. [en línea] <http://gruvix.com/historia-2-0-como-nacio-facebook/> [consulta:]
[172] COMPUTACIÓN APLICADA. . Ob. Cit.
[173] CROFT. Ob. Cit. p. 2.

Ya en 2007, anunció su lanzamiento del sitio en español, francés y alemán, lo que amplió el espectro de usuarios, quienes ya no necesitaban ser parte de un grupo selecto de alguna universidad para participar de este fenómeno.

En marzo de 2013 Facebook registraba 1.11 billones de usuarios[174] y en la actualidad esta plataforma pretende aumentar tal cifra, ya que busca integrar a cualquier persona que tenga un correo electrónico, ampliando su a empresas, marcas comerciales, personajes famosos o cualquier persona que quiera publicar o compartir parte de su vida con sus contactos.

Es necesario destacar que la plataforma ha logrado una conexión mucho más compleja con sus usuarios, ya que el avance de la tecnología permite el constante vínculo con ella por el uso de dispositivos móviles tales como celulares inteligentes, tablets, computadores portátiles o cualquier aparato que pueda conectarse a Internet, lo que trae como consecuencia mayor participación de los usuarios. “En Facebook la información es filtrada por

[174] STATISTIC BRAIN. 2013. Faceboom statistic. [en línea] <http://www.statisticbrain.co,5m/facebook-statistics/> [consulta: 9 enero 2014]

los amigos y las redes. El modelo no descansa sobre un motor de búsqueda, sino sobre las redes sociales. Casi cualquier persona con conocimientos informáticos básicos puede tener acceso a todo este mundo de oportunidades virtuales"[175].

2.1.1.1.2. Perfil

Para ser parte de esta comunidad es necesario en primer lugar el registro y creación de un perfil de usuario. Esta configuración "corresponde a la identidad de la persona y cómo se presentará en el espacio virtual, siendo el cúmulo de informaciones que define su personalidad digital" [176] . La identidad digital entonces, tal como la analizamos anteriormente, se forma por cada acción que realiza del dueño de la cuenta, que él mismo relaciona con Facebook. Por este motivo, la plataforma exige una cantidad mínima de datos que se deben aportar para crear una cuenta, además de la aceptación de las Condiciones de Servicio que propone Facebook, contrato que define y regula las relaciones entre el participante y el sitio.

[175] COMPUTACIÓN APLICADA. . Ob. Cit.
[176] ROA. Ob. Cit. p. 72

La información básica que se exige es el nombre, el sexo, el correo electrónico[177] y la fecha de nacimiento, teniendo en cuenta que la edad mínima para poder crear una cuenta es de 14 años[178]. En relación al nombre del usuario, es importante destacar que Facebook no permite la creación de cuentas falsas e incluso propone a quienes conozcan alguna, la denuncien[179].

Luego de configurar la cuenta con estos datos básicos y obligatorios, la plataforma da la posibilidad de establecer una imagen como "foto de perfil" y otra como "foto de portada" que serán con las que el dueño de la cuenta y otros usuarios podrán identificarlo.

[177] El correo electrónico funcionará como herramienta de comunicación entre Facebook y el usuario, ya que se notificará por este medio cualquier actualización, modificación de clave, entre otros asuntos.
[178] FACEBOOK. 2013. Ayuda para ordenadores. Edad mínima. [en línea] <https://www.facebook.com/help/210644045634222?sr=1&query=%20edad%20maxima%20para%20tener%20facebook&sid=0CosIs0UT4nY9dkqI>
[179] Sin embargo, la realidad es muy distinta, ya que existen innumerables perfiles con antecedentes falsos o de personas que nunca han existido, que generalmente son creados para engañar o incluso perjudicar a terceros.

Además, existe la posibilidad de ingresar otros datos en la cuenta que no son obligatorios, pero que la plataforma recuerda completar y actualizar de forma insistente con el objetivo de obtener más información del usuario y que así, sus amigos y contactos puedan conocer más de él, o aquellos que lo buscan puedan encontrarlo con mayor facilidad[180]. Tal como plantea Barriuso "cuando describimos nuestro perfil de usuario en alguna red social, damos a conocer datos personales, en proporción directa, también, al tamaño de nuestra red social"[181].

En relación a la construcción de la identidad digital en esta red social, es importante destacar el protocolo Open Graph de Facebook, el que consiste en etiquetar páginas web con sólo presionar el botón "me gusta" o comentarlas, ya que permite navegar por Internet sin perder la identidad de Facebook. Lo trae como consecuencia que cualquier "me gusta" o comentario se asocie con el perfil del usuario y pueda ser visto por sus

[180] Dentro de este tipo de información, que no es obligatoria, pero que se incluye dentro de los campos de configuración podemos encontrar el nivel académico alcanzado, el lugar de trabajo actual o anterior, las relaciones familiares, ya sea el estado sentimental del usuario como la relación que tiene con otros contactos, el lugar de nacimiento, gustos personales de música o películas, religión, entre otros tópicos.
[181] BARRIUSO. Ob. Cit. p. 92.

contactos[182]. En palabras de Miguel Morachimo Rodríguez, este protocolo "convierte a la red social en un componente articulador de la Internet, semejante a un sistema centralizado de identidad"[183].

2.1.1.1.3. Lista de amigos

Facebook es una red compuesta por todos quienes poseen una cuenta en el sitio y la forma en la que se configura esta red es la "lista de amigos", conformada por los contactos que el usuario agrega –que también deben tener cuenta en Facebook- y son aceptados como amigo del otro, puesto que dicha comunidad busca principalmente mantener el contacto e interacción entre sus usuarios.

La lista de amigos es uno de los elementos fundamentales de Facebook porque permite que muchas personas se encuentren, ya que "se pueden

[182] Esto ocurre por ejemplo con videos de la página web de youtube.com, ya que al comentarlos o señalar "me gusta", automáticamente se relacionarán con el perfil y la bibliografía.

[183] MORRACHIMO R., M. 2011. La privacidad después de Facebook. [en línea] Lima, Perú. <http://www.blawyer.org/docs/morachimo_privacidad_facebook.pdf p.7.

localizar amigos con quienes se perdió el contacto o agregar otros nuevos con quienes intercambiar fotos o mensajes"[184].

El principal método de búsqueda consiste en el "Graph Search", que cambia el antiguo sistema, en donde se podía encontrar a alguien sólo con el nombre o correo electrónico. Ahora, la plataforma ha facilitado esta búsqueda, toda vez que permite llegar a perfiles en base a cualquier característica que el usuario haya entregado a la red[185], tal como el lugar de nacimiento, de residencia, empresa en que trabaja o ha trabajado, universidad o colegio en que estudió, entre otros. Por otro lado, Facebook hace el trabajo de sugerir contactos de acuerdo a intereses o amistades en común, las que aparecen en la página de inicio de Facebook de cada usuario.

---

[184] VÁZQUEZ., F. A lawbook para Facebook. [en línea] Revolución informática con independencia del individuo. XIV Congreso Iberoamericano de Derecho e Informática, Monterrey. pp. 781-793. <http://biblio.juridicas.unam.mx/libros/6/2941/20.pdf>

[185] BENDERBR. 2013. Facebook elimina la opción de que no puedan buscarte por tu nombre. [en línea] <http://www.laneros.com/temas/facebook-elimina-la-opci%C3%B3n-de-que-no-puedan-buscarte-por-tu-nombre.205049/>

2.1.1.1.4. Grupos y páginas

Como mencionamos anteriormente, Facebook posee herramientas para reunir a sus miembros tomando en cuenta sus intereses comunes, los que permite que quienes integran los grupos y páginas interactúen, compartan fotos o aporten respecto a tópicos específicos.

En primer lugar, encontramos los grupos, que son espacios para que "grupos pequeños de personas pueden comunicarse sobre los intereses que comparten"[186], los que pueden ser configurados de forma "abierta", en donde cualquier persona o perfil podrá acceder a él y ver su contenido, "privada" donde los administradores deben aprobar la solicitud de ingreso, y los grupos "cerrados y secretos", los que no aparecerán en la búsqueda ni en los perfiles de sus miembros, por lo que sólo podrán ser parte de él quienes hayan recibido una invitación de ingreso. Consecuencia de lo

[186] FACEBOOK. 2013. Ayuda para ordenadores. ¿Qué diferencia hay entre las páginas y los grupos? ¿Cuál debo crear? [en línea] <https://www.facebook.com/help/www/162866443847527>

anterior, las publicaciones sólo podrán ser advertidas por quienes integran tal grupo.

Para fundar un grupo no existen muchas exigencias[187]. Cualquier persona que posea una cuenta en Facebook puede crearlos y configurarlos con un nombre, una breve descripción, añadir fotos y gestionar a sus miembros, los que para tener el título de tal "deben ser aprobados o añadidos por otros miembros"[188]. Asimismo se pueden utilizar todas las herramientas que permite la plataforma como chat, álbumes compartidos, creación de eventos, etc., que realizadas por cualquiera de los integrantes en el grupo serán notificados en la página de inicio de los demás.

De acuerdo a los contenidos permitidos existe una amplia variedad de temas, sin restringirlos ni clasificarlos, aunque cabe destacar que hay una

[187] Cabe mencionar que la cantidad máxima de grupos a la que una persona puede pertenecer son 6.000 En: FACEBOOK. 2013. Ayuda para ordenadores. ¿A cuántos grupos puedo unirme? [en línea] <http://es-es.facebook.com/help/www/162866443847527>

[188] FACEBOOK. 2013. Ayuda para ordenadores. ¿Qué diferencia hay entre las páginas y los grupos? ¿Cuál debo crear? [en línea] <https://www.facebook.com/help/www/162866443847527>

normativa que "incluye la prohibición de grupos con temáticas discriminatorias o que inciten al odio y falten el respeto y la honra de las personas"[189].

En segundo lugar, existen las páginas, principalmente dirigidas a empresas, organizaciones, personas famosas o marcas –que sean reales-, las que pueden comunicarse con aquellos perfiles que están interesados en ellas. Por este motivo, la plataforma indica que deben ser creadas y administradas por representantes oficiales [190] y "no pueden utilizar el término genérico de la categoría de productos o servicios que ofrecen"[191], ni tampoco pueden incluir nombre que contengan términos ofensivos, uso incorrecto de las mayúsculas, símbolos, entre otros[192].

[189] VÁZQUEZ. Ob. Cit. p.784

[190]FACEBOOK. 2013. Ayuda para ordenadores. ¿Quién puede crear una página? [en línea] <http://es-es.facebook.com/help/www/364458366957655>

[191] ¿Quién puede crear una página? [en línea] <http://es-es.facebook.com/help/www/364458366957655>

[192] FACEBOOK. 2013. Ayuda para ordenadores. ¿Qué nombres de páginas están permitidos en Facebook? [en línea] <http://es-es.facebook.com/help/www/364458366957655>

En un principio las páginas fueron creadas “con fines específicos y, a diferencia de los grupos, no contenían foros de discusión”[193], pero esto ha cambiado con el tiempo y hoy los administradores pueden entregar todo tipo de información con relación a su página. Así, se han convertido en perfiles de las marcas que se promocionan con todas las herramientas que poseen, muy similares a las de los perfiles de los usuarios[194].

La información que proporcionan los administradores de las páginas siempre es de carácter pública y está disponible para cualquier cuenta de Facebook. De esta manera, para poder acceder a las páginas, la persona debe señalar que “le gusta” y automáticamente la página se vincula con el perfil y comienza a recibir las actualizaciones de noticias en su inicio.

2.1.1.1.5. El Muro y la biografía

Tradicionalmente el muro era el espacio del perfil que poseía cada usuario, donde los contactos podían publicar comentarios, fotografías,

[193] VÁZQUEZ. Ob. Cit.784
[194] ROA. Ob. Cit. p. 80

videos o enlaces a páginas web, etc., y que a su vez contenía la información que ven los amigos del usuario cuando presionan su nombre. Bien, las características antes señaladas no han dejado de existir, pero el muro, como se conocía, fue modificado por los creadores y tomó el nombre de "biografía".

Así, este concepto abarca no sólo lo que otros publiquen en el perfil del usuario, sino que engloba también la información que él mismo proporciona desde la creación de la cuenta. Es tanto así, que la plataforma se presenta como una línea de tiempo –es por esto se usa la tan acertada palabra "biografía"- que resume los contenidos de todos los años en que el usuario ha sido miembro de Facebook. En definición del mismo sitio es "una colección de las fotos, historias y experiencias que componen tu vida"[195].

Todas las publicaciones que se contengan en ella, en principio, podrán ser vista por todos los contactos que estén en la lista de amigos, pero esto puede ser configurado por el usuario para que esta información sea pública,

[195]FACEBOOK. 2013. Ayuda para ordenadores. ¿Qué es la biografía de Facebook? [en línea] <https://www.facebook.com/help/www/467610326601639>

de manera tal, que incluso aquellos que no se encuentren en la lista de contactos puedan acceder a ella, o bien, puede restringirla para que sólo alguno de sus contactos puedan apreciarla o incluso excluir a determinados contactos.

Por otro lado, existen los "mensajes privados" o "inbox", los que pueden ser enviados entre los usuarios y sólo podrán ser visto por ellos de forma privada, funcionando como una especie de correo electrónico y chat.

2.1.1.1.6. Fotos

Otro elemento esencial de Facebook es la posibilidad que tienen sus usuarios de compartir fotografías[196] con sus amigos, ya sea la foto de perfil, la foto de portada, álbumes que el mismo usuario añade a su biografía, o bien, álbumes de otras personas en las que el usuario ha sido etiquetado.

[196] Para poder realizar esto, el usuario puede importar imágenes o archivos desde un disco duro o algún dispositivo de almacenamiento o directamente tomar una foto desde una cámara conectada al computador o cualquier dispositivo móvil que permita el acceso a Internet –celulares inteligentes, Tablet, etc.- y como dijimos antes, existe la herramienta para crear álbumes de fotos para compartirlas de forma más ordenada. En: ROA. Ob. Cit. p. 82

Al etiquetar en las fotos que se suben, éstas se asocian al perfil de esa persona y según la configuración que tenga se podrán ver inmediatamente o deberá esperarse la aprobación del dueño de la cuenta. Igualmente, las etiquetas pueden ser eliminadas por el usuario, ya que en él recae la decisión de si éstas pueden ser vistas sólo por sus contactos o incluso por quienes que no se encuentran en la lista de amigos.

2.1.1.1.7. Aplicaciones

Las aplicaciones son diseñadas para mejorar la experiencia en la plataforma, creadas por desarrolladores externos que deben cumplir las normas impuestas por Facebook [197]. "Estos programadores pueden ser desarrolladores de software quienes intentan recabar datos de los mismos usuarios al éstos inscribirse en su Aplicación"[198].

[197] FACEBOOK. 2013. Ayuda para ordenadores. ¿Qué es una aplicación de Facebook? [en línea] <https://www.facebook.com/help/www/217453588274571>
[198] VÁZQUEZ. Ob. Cit. p.788

Al ser desarrolladas por terceros ajenos a Facebook, éstos pueden acceder a la información privada del usuario como la lista de amigos[199] o cualquier otro dato sensible, ya que este último lo ha aceptado. Así lo explica Vásquez: "si el usuario acepta a través de botón de aceptación sus datos tienen consentimiento cedido para que el Desarrollador pueda usarlo indiscriminadamente o el Tercero desarrollador requerirá un consentimiento posterior para poder hacer uso de los datos privados del Usuario"[200].

2.1.1.2. Twitter

2.1.1.2.1. Origen y desarrollo de Twitter

La red social conocida como "Twitter", nace el año 2006 gracias a la idea de Jack Dorsey, Evan Williams y Biz Stone, quienes trabajaban en ese entonces para la compañía Podscasts Odeo Inc., y buscaban inventar una plataforma que permitiera enviar mensajes de texto –o SMS- con el objetivo

[199] JARAMILLO., O. 2010. La desarticulación de lo público y lo privado en las redes sociales. [en línea] 15p. <http://oscarjaramillo.cl/wp-content/uploads/2011/04/PO-Oscar.pdf> p. 4
[200] VÁZQUEZ. Ob. Cit. p. 788

de indicarle a un grupo pequeño de amigos o contactos qué se estaba haciendo y mantenerlos informados[201].

En un principio, el nombre original de la plataforma era "Status" (Stat.us), pero éste no duró mucho tiempo, ya que los co-fundadores buscaban un nombre que proyectara la idea de estar siempre actualizándose; comunicando y recibiendo información de los contactos de forma inmediata[202].

Según lo expresado por Jack Dorsey en la entrevista para Los Angeles Times, los creadores querían "capturar eso en el nombre –esa sensación de capturar ese sentimiento: la sensación física de estar presente en el bolsillo de un amigo-. Es como estar presente en todo el mundo"[203].

---

[201] COMPUTACIÓN APLICADA al Desarrollo. "Historia de Twitter". [en línea]: <http://www.cad.com.mx/historia_de_twitter.htm>

[202] DOMISFERA. 2009. El origen de Twitter. [en línea] 25 de febrero. <http://www.domisfera.com/el-origen-de-twitter/>

[203] "We wanted to capture that in the name -- we wanted to capture that feeling: the physical sensation that you're buzzing your friend's pocket-. It's like buzzing all over the world.". En: LOS ANGELES TIMES. 2009. Twitter creator Jack Dorsey illuminates the site's founding document. Part I. [en línea] Los Angeles Times. 18 de febrero 2009.

Posteriormente, surgió el nombre “Twitch” –o contracción en español-, por las vibraciones de los teléfonos móviles, pero no transmitía lo que querían expresar los cofundadores de la plataforma, por lo que buscaron en el diccionario palabras que se relacionaran con este término y encontraron “Twitter”, que en palabras de Dorsey “fue perfecto. La definición era “una corta ráfaga de información intrascendente” y “emite un sonido de los pájaros”. Y eso era exactamente lo que buscábamos”[204].

Según el cofundador, el sonido de los pájaros no tiene ningún significado para los humanos, pero sí para los otros pájaros, teniendo el mismo efecto que Twitter, ya que los mensajes pueden no tener importancia para muchos, pero esto va a depender de los receptores[205] [206].

<http://latimesblogs.latimes.com/technology/2009/02/twitter-creator.html l>

[204] “So we looked in the dictionary for words around it, and we came across the word "twitter," and it was just perfect. The definition was "a short burst of inconsequential information," and "chirps from birds." And that’s exactly what the product was.” En: LOS ANGELES TIMES. Ob. Cit.

[205] “The whole bird thing: bird chirps sound meaningless to us, but meaning is applied by other birds. The same is true of Twitter: a lot of messages can be seen as completely useless and meaningless, but it’s entirely dependent on the recipient.” En: LOS ANGELES TIMES. Ob. Cit.

Así, el primer mensaje enviado por twitter fue emitido por Jack Dorsey el 21 de marzo del 2006 con la frase "just setting up my twttr"[207] – en español, sólo ajustando mi twttr-, lo que posteriormente se transformaría en un camino largo y sin retorno, considerando que hoy en día existen más de 554.750.000 perfiles registrados en Twitter[208].

2.1.1.2.2. Perfil

---

[206] Para operar en los mensajes de texto optaron por quedarse con el nombre "twttr" en alusión a "Flirck" y por ser un código corto de cinco dígitos, pero Teen People ya tenía ese mismo código (txttp), por lo que se mantuvo el nombre original, Twitter. En: LOS ANGELES TIMES. Ob. Cit. "But you needed that short code -– in order to operate SMS you need the short code to operate with this cellular administration. So we were trying to get "twttr" -- because we could just take out the vowels and get the 5-digit code. But unfortunately Teen People had that code -– it was 'txttp' [Text TP]. So we just decided to get an easy-to-remember short code [40404], and put the vowels back in."

[207] TWITTER. 2013. Cuenta personal de Jack Dorsey. Actualización de su estado el 21 de marzo de 2006. [en línea] <https://twitter.com/jack/status/20> [consulta:] Primer mensaje enviado por Twitter por Jack Dorsey

[208] STATISTIC BRAIN. 2013. Twitter Statistics. [en línea] <http://www.statisticbrain.com/twitter-statistics/> Fecha del registro 7 de mayo de 2013

Al igual que Facebook, el usuario debe crear una cuenta en Twitter para poder participar en la plataforma, en donde debe señalar su nombre, correo electrónico y un nombre de usuario -que puede coincidir con la realidad o ser un seudónimo[209]- que lo identificará dentro de Twitter y que no podrá repetirse, toda vez que cuando lo introduzca la red social comprobará su disponibilidad[210].

El usuario es libre de configurar su cuenta como más le acomode de acuerdo a sus intereses, su idioma, y su preferencia en cuanto a la privacidad de los Tweets o mensajes, pudiendo además añadir su ubicación cuando mande un mensaje para que sus contactos o seguidores lo puedan ver.

Asimismo, como otras redes sociales, se solicita al usuario que añada una foto de perfil que lo identificará dentro de Twitter, ya sea con quienes

[209] Este nombre puede ser su nombre real o ficticio, además de aceptar números y algunos símbolos.

[210] PSUV. MANUAL de usuario. Twitter. Configuración. Principales funcionalidades. [en línea] Venezuela. 17p. <http://desarrollo.psuv.org.ve/files/2010/07/Manual-de-Usuario-Twitter.pdf> p.4

posean o no una cuenta en el sitio, y tendrá a su vez la opción de elegir la apariencia física que tendrá el perfil utilizando una imagen como fondo a elección del mismo [211] . Otro aspecto relevante de éste es la breve descripción que debe ingresar el usuario ya sea de sí mismo o del objetivo de su cuenta, puesto que los elementos que comparta respecto de su vida además de hacerlos públicos, donde cualquier persona podrá acceder a ellos, configurarán de manera más específica su identidad digital.

Una vez establecida la cuenta, su dueño podrá acceder a su página principal en donde aparecerán tanto los mensajes que postee, como aquellas publicaciones que realicen a quienes sigue, todas por orden de publicación, lo que es llamado "Timeline"[212] o cronología[213]. Hay quienes plantean que la importancia del Timeline recae en la determinación de las personas que

[211] SAN MARTIN del Rey Aurelio. Twitter. [en línea] España. 17p. <http://www.smra.eu/files/Twitter.pdf> p.6

[212] Generalmente, en la red social se abrevia como TL.

[213] WALNUTERS. Manual de Twitter. [en línea] España. <http://www.redsaludandalucia.es/sites/default/files/null/Twitter%20manual_0.pdf> p.13-14

se relaciona con el usuario[214] y los intereses que éstos tienen en común, lo que influye a la hora de configurar la identidad digital.

Finalmente, la configuración de la cuenta en Twitter intenta ser un reflejo virtual de la vida del usuario al compartir comentarios, imágenes, publicaciones de periódicos entre otros puntos de interés para él.

2.1.1.2.3. Qué son los "Tweets"

Los mensajes que la plataforma permite escribir en la página principal reciben el nombre de "tweets", los que tienen una cantidad máxima de 140 caracteres, pero que no limitan su contenido, puesto que se pueden también incluir enlaces de páginas web, fotos o videos entre otros[215].

Estos mensajes son por regla general de carácter público, lo que significa que cualquier persona, sin que necesariamente tenga una cuenta, lo pueda

[214] TWITTER: 5 años. Un recorrido por la herramienta que se convirtió en plataforma. Miguel Jorge "et al". [en línea] 107p. <http://www.antonioconstantino.com/pdf/twitter.pdf> p. 27

[215]RFG. Desarrollo web. Twitter. Qué es y cómo utilizarlo. [en línea] 20p. <http://www.rfg84.com/twitter/El_ABC_de_Twitter.pdf> p.3

ver. Sin embargo, la plataforma permite configurarlo, para que sólo algunas personas logren ver el contenido del mensaje.

También permite hacer menciones o referencias entre dos o más perfiles de Twitter[216], anteponiendo el signo "@", para que la persona aludida pueda ver el mensaje, el que se mostrará en el correspondiente perfil del usuario citado, el que a su vez podrá responder a las publicaciones hechas quedando su "Tweet" inmediatamente asociado a lo anterior. Asimismo, existe la opción de "Retwittear" o "RT", que da la posibilidad que el usuario pueda republicar en su perfil cualquier "Tweet" que haya sido compartido por otra, y marcar como favorito algún "Tweet" que le haya gustado al usuario, el quedará guardado en su perfil.

2.1.1.2.4. Seguidores y listas

A diferencia de Facebook, en Twitter no existe una lista de amigos propiamente tal, sino que cada usuario puede "seguir" a otros y ser "seguido", esto determinará qué publicaciones se verán en la página de

[216] SAN MARTIN. Ob. Cit. p.3

inicio del dueño de la cuenta. Sin embargo, "seguir" a alguien no es de carácter permanente, por lo que cada usuario puede dejar de hacerlo seleccionando la opción "dejar de seguir"[217].

En cuanto a las listas, éstas son útiles para quienes siguen a muchas personas y no quieren mezclar o confundir los distintos temas, pudiendo tener el carácter de públicas o privadas. Así, es posible que el usuario pueda organizar su Timeline, seguir eventos o concursos en Twitter, entre otros.

2.1.1.2.5. Hashtag y Trending Topic

Los usuarios de Twitter pueden agrupar mensajes sobre un mismo tema mediante el uso de almohadillas ("#"), o como se conoce comúnmente "Hashtag" que corresponde a su nombre en inglés.

Un "Hashtag" representa un tema o una forma de difundir un mensaje, que nació de la idea original de Chris Messina, activista e investigador, quien propuso la idea de usar un formato que se asimilara a los canales que

[217] PSUV. Ob. Cit. p.10.

se utilizaban en IRC [218] , para que en Twitter se pudieran crear conversaciones de temas específicos y así, los usuarios pudieran seguirlas de manera sencilla[219].

Rápidamente esta forma de agrupar mensajes fue adoptada y masificada [220] en todo el mundo, ya que desde julio de 2009, Twitter agregó un hipervínculo automático a todos los "Hashtag" que permite buscarlos en el sistema, lo que sumado al aporte de los "Trending Topics" en la página principal, hizo que se realzara mucho más su uso.

---

[218] IRC corresponde a un chat popular hace unos años atrás en el que se utilizaban "#channels", que correspondía un chat especial dentro de IRC, el que permitía agrupar a las personas que participaban en él por medio de intereses en común.

[219] El primer tweet en que se utilizó este método fue "how do yo feel aboutusing # (pound) for groups. As in #barcamp [msg]?" el 23 de agosto de 2007. En: BUENDÍA., A. El extraño origen del Hashtag en Twitter #historia. [en línea] <http://www.apolorama.com/2013/07/el-extrano-origen-del-hashtag-en-twitter-historia/>.

[220] El uso del Hashtag se ha masificado tanto, que incluso hoy se utiliza no solamente en Twitter, sino que otras redes sociales como Facebook, que lo incorporó en junio de 2013. En: FACEBOOK. 2013. Ayuda para ordenadores. ¿Cómo se usan los hashtag?. [en línea] <https://www.facebook.com/help/587836257914341?sr=2&sid=0164mb7pGcvLC3kkO>. En: STURM., C. 2013. Facebook ahora tiene Hashtag. [en línea] <http://www.fayerwayer.com/2013/06/facebook-ahora-tiene-hashtags/>

Un “Trending Topic” o “TT”, como se conoce comúnmente dentro de la red social, es “el tema del momento”, que tiene su origen y desarrollo en los “Hashtag”, ya que consiste en la publicación en la página de inicio de Twitter los 10 “Hashtag” más populares o más utilizados considerando los locales y mundiales[221].

En junio de 2012, Twitter lanzó un nuevo concepto buscando personalizar mucho más los “Trendig Topics”, el que recibe el nombre de “Tailored Trends”, en donde la plataforma por defecto utiliza un algoritmo que analiza la ubicación del usuario dentro de las más de 150[222] locaciones que se encuentran registradas en la plataforma, y a quién o quienes sigue para indicar los “Trendig Topics” más adecuados y relevantes, lo que permite al usuario estar más al día con Twitter y el acontecer local[223].

---

[221] Desde enero de 2010, los Trending Topic ya no son únicamente mundiales, sino que existen de forma local, lo que significa un impulso a promover temas considerando los intereses de los usuarios, según el espacio geográfico especifico en donde se encuentran. En: PARR., B. Based Trending Topics. [en línea] <http://mashable.com/2010/01/22/twitter-local-trend/>

[222] MAUSKOPF., S. 2012. Tailored Trends bring you closer. [en línea] <https://blog.twitter.com/2012/tailored-trends-bring-you-closer>

[223] ROLLAN., F. 2012. Tailored Trend los “trending topics” según el usuario y su localización. [en línea]

2.1.2. Naturaleza de las redes sociales

Ya descrita la estructura de las redes sociales que son motivo de nuestro estudio, Facebook y Twitter, cabe preguntarnos ¿qué son las redes sociales?

Si bien es indiscutible que la naturaleza jurídica del acuerdo que nace entre el usuario y la plataforma virtual es un contrato de adhesión, no existe unanimidad en definir si las redes sociales son o no un medio de comunicación social.

La Ley 19.733 en su artículo segundo, inciso primero establece que: "Para todos los efectos legales, son medios de comunicación social aquellos aptos para transmitir, divulgar, difundir o propagar, en forma estable y periódica, textos, sonidos o imágenes destinados al público, cualesquiera sea el soporte o instrumento utilizado".

<http://www.semseo.es/blog/general/tailored-trends-los-%E2%80%98trending-topics%E2%80%99-segun-el-usuario-y-su-localizacion.php>

Tomando en consideración la definición que da la mencionada Ley sobre los medios de comunicación social, a nuestro parecer, Facebook y Twitter a primera vista cabrían dentro de ella, puesto que el objetivo de estas plataformas es justamente dar movimiento a la información que cada usuario desea compartir en la red.

Sin embargo, al ahondar en el mencionado artículo, cabe analizar el fin de la norma. Aun cuando estamos de acuerdo con que el objeto de las redes sociales es "transmitir divulgar, difundir o propagar" información en cualquier formato, debemos hacer hincapié en que esta información compartida debe ser "destinada al público" para que tales redes sociales sean consideradas como "medios de comunicación social".

A nuestro entender, la palabra "público" que utiliza la ley, hace alusión al grupo de personas que conforma toda la sociedad, sin discriminación ni segregación alguna basada en la edad, sexo, raza, condición, parentesco, amistad o cercanía. Lo cual, no coincide con la información que se reproduce en Facebook o Twitter, puesto que observando el funcionamiento de cada una de las plataformas, podemos decir que:

A. Facebook:

Como señalamos anteriormente, es un medio en el cual cada usuario proporciona la información que quiere y cuando quiere, destinado principalmente a quienes ha aceptado como amigo.

Así, concuerda el voto minoritario del Ministro de la Corte Suprema, señor Sergio Muñoz, al señalar en su visto tercero que: "cabe precisar que "Facebook" es un sitio web que permite a sus usuarios el poder comunicarse e intercambiar opiniones entre ellos, para lo cual el interesado debe solicitar autorización expresa a un tercero para incorporarlos en sus contactos y dicho tercero sólo se integrará a los mismos luego de consentir expresamente en ello, de lo que se desprende que sólo entre quienes así han consentido la información y sus comunicaciones es pública, no existiendo habilitación para que dicha información sea utilizada por otras personas"[224].

[224] CORTE SUPREMA, rol 5322-2012 de fecha treinta de agosto del año dos mil doce.

Por lo tanto, la comunidad destinataria de la información que se comparte, mientras la cuenta no esté abierta, se reduce a los contactos que el usuario ha decidido agregar o aceptar como “Amigos”, lo cual acota la palabra “público” a su expresión más íntima, que sólo considera a los conocidos de la persona y, por consiguiente, no se ajusta con la idea de la información que es entregada al público en general, sin hacer distinciones, que va directamente relacionada con lo que es un medio de comunicación social.

Incluso, es posible en esta plataforma discriminar aún más el acceso a la información que se divulga respecto de los contactos que se tienen, puesto que Facebook permite en cada publicación seleccionar si la comunicación va dirigida a cualquier usuario, o bien, a qué personas específicas se les admite o prohíbe visualizar el contenido de la misma.

Además debemos considerar la calidad del contenido que se transmite en Facebook para determinar su carácter de medio de comunicación social, el que tendrá que ser de matiz general o de interés público para lograr que la cuenta sea definida como tal, puesto que todo dato compartido de índole

personal al no tener un grado de importancia suficiente para interesarle al resto, no puede ser entendido como un mensaje dirigido “al público”. Esto se suma a la exigencia de que la información que se publica se haga de forma periódica, puesto que entradas aisladas no pueden considerarse como medio de comunicación social.

Por tanto, consideramos que la mayoría de las cuentas de Facebook -salvo aquellas que se encuentran abiertas al público, transmitan información de carácter general de forma periódica y sin ningún filtro- no constituyen un medio de comunicación social, porque cada vez que el usuario realiza una publicación determinando quiénes serán los que puedan verla, y delimitando la calidad de la información a una de índole personal, elimina completamente la idea de que la información “esté destinada al público”.

B. Twitter:

Esta plataforma, por su parte, si bien nace como un medio para compartir, en sólo 140 caracteres, qué es lo que se está haciendo en tiempo real con los seguidores de la cuenta particular, se ha convertido en una

plataforma de microblogging[225] que traspasa dicho límite, puesto que hoy es una red altamente ocupada como fuente de noticias de índole pública y foro de opinión en el que los usuarios emiten sus propios juicios respecto de diversos temas.

En cuanto al segmento de personas a las que se dirige la información exhibida en los "Tweets", podemos establecer que existen sólo dos modalidades en que se puede compartir. Por un lado teniendo el perfil público –abierto a todos los que deseen seguir la determinada cuenta o se encuentren fuera de esta comunidad- lo que significa que podrá ser visto por cualquier persona. Siendo la otra alternativa, un perfil privado -cerrado a quienes el usuario acepte como seguidores- y por tanto, sólo estos podrán ver el contenido de las publicaciones.

Como podemos observar, Twitter es bastante menos selectivo que Facebook en lo que respecta a los receptores de la información, puesto que

[225] BARROS., M. y QUIROGA., V. 2011. El periodismo en tiempos de Twitter. Nuevas formas y actores en el mundo de las comunicaciones ¿Pueden todos ejercer el oficio del periodista? Tesina para optar al grado de Licenciado en Comunicación Social. Santiago, Universidad Diego Portales, Facultad de Comunicación y Letras Escuela de Periodismo p.14

el primero permite compartir las publicaciones con todos los usuarios o sólo con algunos, sin hacer clasificaciones específicas o personalizadas en cada "Tweet" emitido.

Es indiscutible que las cuentas cerradas no constituyen un medio de comunicación social a la luz de la definición que hace el artículo segundo de la mencionada Ley, ya que las comunicaciones que se realizan a través de este tipo de cuentas no van dirigidas al público en general.

Sin embargo, las cuentas abiertas son objeto de duda, puesto que al estar en este estado, claramente la intención del usuario es que el contenido que comparte vaya dirigido a quien quiera y pueda verlo, mas no necesariamente este hecho hace que sea un medio de comunicación social. Esto, porque habría que determinar cuántos seguidores se considerarían suficientes para que el conglomerado de personas destinatarias de la información sea catalogado como "público general".

Una cuenta que tenga una cantidad menor de seguidores, a nuestro parecer, no puede considerarse como un medio donde la información esté

destinada al público, puesto que no habría un interés generalizado por el contenido de la misma.

Pero, ¿Qué ocurre con aquellas cuentas que tienen muchos seguidores? En este caso, el análisis ya no se dirige a un criterio cuantitativo –en relación al número de seguidores- sino, que hacia un criterio cualitativo –basado en la calidad del contenido publicado-.

Esto nos lleva a cuestionarnos qué clase de información es la que debe entregarse en una cuenta de Twitter para que sea considerada como un medio de comunicación social, haciendo distinción si la naturaleza de lo que se comunica puede ser de carácter privado o, necesariamente, debe tratarse de hechos de interés general y público.

Somos de la opinión de que aquellas publicaciones que contengan información personal, no serán catalogadas como medio de comunicación social, independiente del número de seguidores que se tengan, puesto que lo transmitido no es relevante para la sociedad toda. Asimismo, tampoco constituyen medios de comunicación social aquellas cuentas en que a pesar

de que el contenido publicado en los “tweets” sea de índole común, éstos no se hagan de forma periódica, como lo señala el artículo segundo de la Ley 19.733.

En consecuencia, en nuestra opinión, sólo serían medios de comunicación social aquellas cuentas de Twitter que:

1. se encuentren abiertas,
2. sean seguidas por una cantidad considerable de personas,
3. donde la información que se propaga sea de interés general o público, y
4. haya periodicidad en las publicaciones que se hacen a través de este medio.

Para finalizar, es menester establecer que las cuentas, tanto en Facebook como en Twitter, asociadas a los medios de comunicación social tradicional, como son los canales de televisión, las estaciones de radios y periódicos, responden a los mismos fines transmitir, divulgar, difundir o propagar, en forma estable y periódica, información de interés general

destinados al público, siendo una extensión de éstos y, por tanto, igualmente medios de comunicación social.

CAPÍTULO III: DELITOS INFORMÁTICOS: TRATAMIENTO LEGAL EN EL DERECHO COMPARADO.

Recapitulando, identidad surge del interés del ser humano a ser individualizado en la sociedad, pudiendo entonces definirse como el "conjunto de características, datos o informaciones que permiten individualizar o referenciar a una persona" de manera precisa u objetiva[226], sirviendo este conjunto de atributos al desarrollo, en gran parte, de las relaciones sociales y jurídicas, por dotar a las personas de reconocimiento y habilitando su participación en el ámbito social.

También ha de recordarse que persona es todo individuo de la especie humana, que constituye por sí un centro de imputación de derechos y

[226] De Salvador, Carrasco Luis. Casos de suplantación de identidad detectadas en denuncias tramitadas por la Agencia Española de Protección de Datos, citada por Mata y Martín, Ricardo en El robo de identidad: ¿una figura necesaria? Ed. Arazandi-Thompson Reuters-Agencia Española de Protección de Datos-Universidad de Castilla-La Mancha. Pamplona. 2010. P.200. En: ROMERO L., L. 2011. Jus informa TIC's. 1ª ed. México. p. 151.

obligaciones, en virtud del dominio que tiene sobre sí mismo y sus actos. Lo que se relaciona, además, con ser sujeto de imputación de acciones delictuales, en cuanto por ser dueño de los actos que se realizan, debe responsabilizarse de ellos.

En este mismo sentido, Kant -según el profesor Alex Van Weezel- expresa que "persona es el sujeto "cuyas acciones son susceptibles de una imputación", que puede considerarse como "autor" (en sentido amplio) de una determinada acción y su efecto"[227]. Por consiguiente, es posible afirmar que la atribución de una identidad –en cuanto ésta es una ficción jurídica que nace de una convención social- permite establecer las posibles consecuencias de una conducta para su autor.

La imputación, por tanto, consiste en atribuir un determinado hecho a una persona como su obra, afirmación que se encuentra más que arraigada en la dogmática jurídico-penal, y que ha sido abordada por distintas

[227] VAN WEEZEL., A. 2011. "Persona como sujeto de imputación y dignidad humana." Límites de la imputación penal. Estudios 2000-2010. Universidad Externado de Colombia. Bogotá, Colombia. 1a.ed. p. 16.

posiciones[228]. Siempre considerándose que la imputación jurídica es un rendimiento social de la persona y no una autoimputación, la cual se basa en el principio social de la identidad personal, idea ya establecida en el precedente capítulo.

En la actualidad, la calidad de "sujeto de imputación" que detenta la persona, se extiende a ámbitos que hace algunos años atrás se consideraban inimaginables; como es la tecnología y la red, así como también la posibilidad de que éstos sean medios u objetivos de la comisión de delitos –sean clásicos o informáticos-. Esto se ve directamente relacionado con la existencia de la identidad virtual, la cual se constituye por el conjunto de datos personales con los que las personas interactúan y operan en las redes informáticas, pudiendo ser susceptibles de apropiación no autorizada por su dueño, lo que constituiría delito.

[228] Dichas perspectivas filosóficas transitan entre las ideas de Locke -con su teoría de la identidad de la conciencia o conciencia de la identidad-, pasando por Kant –con la distinción entre los conceptos de *homo noumenon* y *homo phaenomenon*-, hasta Hume y Kelsen –con sus ideas de la identidad personal como ficción resultante de una convención y el concepto de causalidad-, sumado a las posiciones contrarias que toman el camino inverso estimando que la personalidad es presupuesto de la imputación.

Ahora bien, es innegable que "los problemas que estas nuevas tecnologías traen consigo son mucho menos visibles que las ventajas y promesas que conllevan", y es justo éste el problema real de las mismas: "la gente no nota la amenaza; la peligrosidad de estos productos desaparece detrás de las facilidades que prometen". Lo que permite que los perfiles que creamos en Internet sean objeto de inesperadas y bien disfrazadas intromisiones, que se traducen en injerencias en la personalidad de los individuos[229].

Hoy, los computadores ofrecen variadas y sofisticadas oportunidades para romper la ley, dando cabida a la ejecución de delitos a través de ellos, contravenciones tanto de naturaleza clásica como de índole informática, lo que expande el universo de posibilidades de ser víctimas, sobre todo en el mundo del Internet, donde las facilidades de comisión están a un "click" de distancia.

[229] MORALES G., O. 2002. Delincuencia informática: problemas de responsabilidad. Cuadernos de derecho judicial, Consejo General del Poder Judicial. Madrid, España. p.41.

Por esta razón, en el presente capítulo, con el fin de cimentar el estudio que haremos sobre el delito de usurpación de identidad en las redes sociales y su tratamiento en Chile, analizaremos la realidad en el Derecho Comparado de los delitos informáticos, en vista de que éstos se encuentra más desarrollados fuera de nuestro país.

1. Delito informático

Internet, el mayor exponente de los nuevos avances, "es un sistema de intercomunicación global, cuya tecnología permite vincular millones de computadoras entre sí, y acceder desde cualquier sitio del planeta a la información o servicios que se ofrezcan en ella (…)".[230] Éste, además, constituye un sistema de interconexión espacial que se caracteriza principalmente por no reconocer fronteras, lo cual crea un escenario novedoso y de vastas oportunidades para cometer delitos.

[230] ABOSO., G.E. y ZAPATA., M. F. 2006. Cibercriminalidad y derecho penal: la información y los sistemas informáticos como nuevo paradigma del derecho penal : análisis doctrinario, jurisprudencial y de derecho comparado sobre los denominados "delitos informáticos". B de F, Montevideo. p. 6.

Esta herramienta virtual, a su vez, es aquella sobre la cual se erigen las tan solicitadas redes sociales, que también forman una plataforma perfecta para la realización de ciertas infracciones, ya que ofrecen el lugar perfecto para conocer datos (personales) sensibles[231] que la gente comparte, muchas veces sin advertir el riesgo que conlleva.

1.1. Concepto

Gracias a la nueva realidad impuesta por las neo-tecnologías se ha acuñado el término "ciberespacio", que esquematiza la zona donde tiene lugar esta interconexión entre computadores y personas sin límites fronterizos ni temporales, y donde se ejecutan una serie de fenómenos de la comunicación que se asientan cada día más en nuestra vida diaria, lo que se relaciona directamente con el uso abusivo de estos sistemas por vía informática y la eventual procedencia del cibercrimen.

[231] Según el artículo 2º de la Directiva nº 46 (96), dictada por el Consejo Europeo y el Parlamento Europeo, se entiende por "datos personales": "toda información sobre una persona física identificada o identificable; se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social."

Esta nueva forma de criminalidad se relaciona directamente, "con el uso o la intermediación de un elemento o dato informatizado", la cual se asocia indiscutiblemente con la tecnología, lo que plantea un desafío ya en la conceptualización del delito informático como en la determinación del objeto que protege, sus características y la eventual posibilidad de ser tratado como cualquier otro delito en el código penal, debido al creciente interés social que se demanda en la realidad actual[232].

El término "delito informático"[233], según Gustavo Arocena, debiera tener tal amplitud que pueda abarcar tanto las modalidades criminales que utilizan un sistema informático como medio para la perpetración de distintos ilícitos, como también cuando este mismo sistema se convierte en

[232] ABOSO y ZAPATA. Ob. Cit. p. 15.

[233] Si bien existe un debate terminológico sobre este término y aún no hay una definición uniforme que conceptualice este fenómeno, estimamos que para lograr el objetivo de nuestro análisis se considerarán como sinónimos de éste los vocablos; "cybercrimen", "ciberdelito", delitos con el adjetivo "virtual", "online", "digital", "computer-related", "internet-related", "electrónicos" o "e-crimes".

el objeto del comportamiento delictual[234]. Por lo cual, debemos entender que este vocablo singular supone una pluralidad de modalidades delictivas –y no una sola de carácter general-, vinculadas por supuesto a los computadores y otras tecnologías relacionadas.

Una primera aproximación al concepto de delito informático –según lo planteado por Arocena- establece que es "el injusto determinado en sus elementos por el tipo de la ley penal, conminado con pena y por el que el autor merece un reproche de culpabilidad, que utilizando a los sistemas informáticos como medio comisivo o teniendo de aquéllos, en parte o en todo, como su objeto, se vinculan con el tratamiento automático de datos"[235]. Tal acercamiento a la noción de delitos digitales se convirtió en insuficiente respecto de la rápida evolución que ha sufrido la criminalidad informática, no siendo posible ya determinar este concepto en términos

[234] AROCENA., G. 1997. De los delitos informáticos. Revista de la Facultad de Derecho, Universidad Nacional de Córdoba. Vol. 5, nº 1. pp. 44 y ss.

[235] AROCENA., G. 2012. La Regulación de los delitos informáticos en el Código Penal Argentino. Introducción a la Ley Nacional Núm. 26.388. [en línea] Boletín de Derecho Comparado, vol. XLV, núm. 135, septiembre-diciembre. Universidad Nacional Autónoma de México. <http://www.redalyc.org/pdf/427/42724584002.pdf> p. 950.

simplistas y genéricos, lo que ha llevado a su debate y consiguiente cambio.

Una conceptualización clásica del e-crime –que ha sido utilizada como base para su actualización por la mayoría de la doctrina- determina que éste es "toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor, o que, por el contrario, produce un beneficio ilícito a su autor aún cuando no perjudique de forma directa o inmediata a la víctima, y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas"[236].

En base a lo anterior, y con el propósito de ampliar el concepto de "computer crime", en 1983 un grupo de expertos de la OCDE definieron dicho término como "cualquier conducta antijurídica, antiética, o no autorizada, relacionada con un procesamiento automático de datos y/o

[236] CAMACHO L., L. 1987. El delito informático. Gráficas Condor, S.A. Madrid. P.17. En: ROVIRA D., E. 2002. Delincuencia informática y fraudes informáticos. Editorial Comares. Granada. p. 63.

transmisión de datos"[237]. Desarrollo de la expresión que se consideró beneficiosa y que tuvo gran acogida por parte de la doctrina, pero que siguió transformándose durante la década de los noventa hasta lo que actualmente se entiende por "delito informático"[238].

De estos planteamientos se deriva principalmente que los delitos informáticos deben responder a ciertos elementos: primero, que la acción cometida se vincule al funcionamiento de alguna máquina telemática, ya sea ella su objeto o el medio utilizado para llevarla a cabo; segundo, que tal acción sea considerada delito por estar tipificado en la ley, y; tercero, que exista un elemento subjetivo, el dolo, más allá de la existencia de un beneficio para el autor o un perjuicio para la víctima.

En la actualidad se ha optado por liberar el contenido del concepto "delito informático", por considerársele restringido para la real naturaleza de la criminología informática, en virtud de la pluralidad de ilícitos que abarca, los cuales tienen como elemento común su vinculación con los

[237] ROVIRA D., E. 2002. Delincuencia informática y fraudes informáticos. Editorial Comares. Granada. p. 62.
[238] Ídem.

computadores u otros equipos de orden telemático. Razón por la cual hoy se mira al delito de índole virtual –en sentido amplio- como el conjunto de comportamientos ilícitos informáticos que generan un riesgo de tal envergadura que es posible que "constituyan ataques serios a intereses jurídicamente protegidos y protegibles, tradicionales y nuevos, que deben ser contrarrestados con medidas que superen los meros ámbitos de la autorregulación, del derecho administrativo y derecho civil, requiriendo la intervención del derecho penal", pudiendo entonces denominarlos como "delitos informáticos"[239].

En el caso de Chile, con la Ley Nº 19.223 de fecha 7 de junio de 1993, se tipifican una serie de figuras penales relativas a la informática, mas no se define el "delito informático". Esta normativa aborda la delincuencia informática desde la perspectiva más originaria de los delitos virtuales, que los mira como delitos clásicos en los cuales intervienen sistemas computacionales, ya como instrumentos para su comisión o como objeto de los ilícitos, lo cual debe adaptarse a la realidad actual, en la que el valor de

[239] ROVIRA. . Ob. Cit. pp. 65-68.

la información que se protege exige que estas acciones ilícitas sean reprochables por sí mismas.

Si bien es loable el carácter pionero de esta legislación en el panorama latinoamericano, debemos esclarecer que esta Ley es deficiente en cuanto al alcance de sus normas, ya que aún con la introducción del concepto de "sistema de tratamiento de información", sólo se preocupa de la protección del soporte lógico o programas y los datos contenidos en ellos, dejando cualquier otro elemento que se encuentre fuera de lo dispuesto por este cuerpo legal al amparo de la normativa clásica[240]. Lo que además, se suma al insuficiente desarrollo del término "delito informático", que conlleva a la dificultad de extender esta ley a conductas delictivas asociadas, e igual de relevantes, lo cual restringe aún más el ámbito de su aplicación.

Todo por lo cual, estimamos que la conceptualización del delito informático debe estar determinada principalmente por la multiplicidad de

[240] DURAN B., M. A. 2010. Tratamiento del delito informático en Chile. Memoria para optar a la licenciatura en ciencias jurídicas y sociales. Santiago, Universidad de Chile, Facultad de Derecho. pp. 58-59.

comportamientos ilícitos de carácter informático que acoge -lo que tiene estrecha relación con su naturaleza pluriofensiva-, que tienen como elemento común la utilización de computadores u otros equipos de orden telemático, los cuales deben generar un riesgo importante que constituya un ataque real y grave a algún interés jurídicamente protegido o protegible, sea éste tradicional o moderno.

1.2. Clasificaciones del delito informático

El ciberdelito, en la gran variedad de conductas delictivas que abarca, es clasificado inicialmente según dos criterios iniciales: el primero como medio o instrumento y el segundo como objeto o fin[241].

Al igual que la mayoría de los juristas, utilizaremos esta distinción para enumerar los diferentes comportamientos ilícitos –considerados más relevantes- que se valen de computadoras para realizar su cometido o bien

[241] TELLEZ VALDÉS., J. 2004. Derecho Informático. McGraw-Hill Interamericana, México D.F., 3a.ed. p.165-170. En: CHINCHILLA S., C. 2004. Delitos Informáticos. Elementos básicos para identificarlos y su aplicación. Farben Grupo Editorial Norma. San José, Costa Rica. 1a. ed. pp. 28-30.

los consideran –a éstos o la información o datos que contengan- su objetivo. Enunciando, además, otras clasificaciones de delitos informáticos que guardan relación con la utilización de Internet como medio para la ejecución de tales actos delictuales[242].

1.2.1. Delitos informáticos como instrumento

- Planeación o simulación de delitos clásicos: como el hurto, el fraude, entre otros.

- Falsificación de documentos –carné de identidad, tarjetas de crédito, cheques, etc.- vía computarizada.

- Alteración de activos y pasivos en la situación contable de la empresa.

- Lectura, sustracción o copia de información confidencial.

[242] CHINCHILLA. Ob. Cit. pp. 28-32.

- Modificación de datos de acceso a sistemas informáticos.}

- Aprovechamiento indebido o violación de un código para penetrar un sistema de información determinado.

- Uso no autorizado de programas de cómputo.

- Alteración en el funcionamiento de un sistema informático, a través de virus de la misma índole.

- Acceso no autorizado a áreas informatizadas.

- Intervención de las líneas de comunicación de datos o teleproceso.

- Violación de correspondencia, mediante la intervención de correo electrónico.

- Fraude electrónico relacionado con las compras en la red.

- Transferencia de fondos, mediante engaño en la realización de dichas transacciones –por lo general por medio de sistemas informáticos ficticios-.

1.2.2. Delitos informáticos como objeto

- Programación de instrucciones que produzcan bloqueo total a un sistema informático.

- Spamming o bloqueo de sistema informático mediante el envío masivo de correos electrónicos de forma deliberada.

- Destrucción de programas por cualquier método.

- Lesión física contra la máquina o sus accesorios.

- Sabotaje político o terrorismo que destruya o produzca apoderamiento de los centros neurálgicos computarizados.

- Secuestro de soportes magnéticos que contengan información valiosa con fines de chantaje.

- Acceso no autorizado a un sistema informático, mediante el uso ilegítimo de contraseñas.

- Infracción de derechos de autor de determinadas bases de datos, mediante la utilización de la información sin autorización contenida en las mismas.

1.2.3. Otros delitos informáticos permitidos por el uso de Internet

- Espionaje, mediante el acceso no autorizado a sistemas informáticos de gobierno o empresariales, o a sus correos electrónicos.

- Ciberterrorismo.

- Otro tipo de delitos reprochables, como el narcotráfico; trafico de armas; pornografía infantil; provocación o instigación de discriminación (por sexo, religión, etnia, etc.), así como cualquier otro delito que posibilite el traslado de la vida real al ciberespacio y viceversa.

1.3. Características del delito informático

Los delitos informáticos se identifican primordialmente con la rápida y vertiginosa evolución de las tecnologías, por lo cual es de esperarse que las particularidades de este tipo de delitos estén en constante cambio. Por este motivo, a continuación, desarrollaremos las características esenciales de este tipo de delitos y las que detentan un perfil variable, éstas últimas en relación con las medidas legales que existen o debieran existir para enfrentar este fenómeno.

En un primer plano cabe analizar –en base a la postura de Rovira[243], que consideramos la más adecuada- las características básicas y sustantivas de los ciberdelitos en su generalidad.

1.3.1. Permanencia del delito por repetición y automatismo del hecho

Los delitos informáticos se caracterizan, principalmente, por la viabilidad de repetición del hecho delictivo, que configura estos ilícitos como comportamientos de carácter continuo, en cuanto es posible y habitual que una vez que el sujeto que intervenga en él -encontrando una forma fácil de llevarlo a cabo y con resultados exitosos-, lo realice de nuevo.

Además, de tal reincidencia en el comportamiento delictivo, dichos ilícitos pueden adquirir automatismo, en tanto, la utilización de un programa de funcionamiento informático puede –a través de su programación- posibilitar que la conducta se repita automáticamente, independiente de la intervención o autorización del sujeto que

[243] ROVIRA. Ob. Cit. pp. 77 y ss.

primeramente participó, dándose con esto, delitos de comisión instantánea con efectos permanentes[244].

1.3.2. Extensa y alta lesividad

Es propio de este tipo de delitos detentar una amplia y alta lesividad, en cuanto pueden menoscabar una variada suma de intereses, incluso simultáneamente, teniendo muchas veces –no siempre- un resultado perjudicial, sobre todo en el ámbito de la intimidad y en el económico.

1.3.3. Distanciamiento de tiempo y espacio

Con las nuevas tecnologías y el asentamiento del Internet como su principal exponente, en la actualidad existe la posibilidad de cometer la acción ilícita con un desfase de tiempo, relativo al momento en que se ejecuta el hecho y la materialización del mismo, la obtención de un resultado o la producción de un daño, sumado a la falta de fronteras que aporta este tipo de métodos, lo cual permite que un sujeto se encuentre

[244] DURAN. Ob. Cit. p. 33.

físicamente en un lugar y cometa un delito en otro. Caracterización de espacio/tiempo que viene dada por "las facilidades que el tratamiento, almacenamiento, procesamiento y transferencia de la información y de los datos de los actuales sistemas informáticos y de comunicaciones lleva consigo y (…) la velocidad en su realización conjuntamente con la posibilidad de interrupción, paralización o suspensión temporal en la ejecución completa de la acción ilícita"[245] [246].

1.3.4. Mayor diversidad, frecuencia y peligrosidad e incremento en su proliferación

De acuerdo al concepto y a las primeras características del delito informático, podemos establecer que alrededor de éstos existe una diversidad de modalidades delictuales, que están en permanente desarrollo,

[245] DURAN. Ob. Cit. pp. 35-36.

[246] Sobre este punto, referente a la ocurrencia de que un delito sea cometido en un país distinto del cual donde se experimentan sus consecuencias, cabe mencionar que si bien rige el principio de soberanía nacional, la posición mayoritaria de la doctrina propone que exista una política de cooperación internacional, ya que defiende la idea de que la única manera de combatir al delincuente virtual es que éste tenga menos posibilidades de impunidad, lo que se lograría con el trabajo en conjunto de los distintos países que irremediablemente son parte del mundo globalizado. En: ABOSO y ZAPATA y ROVIRA.

tanto respecto de su cantidad como variedad, y que cada día, en parte por la facilidad creciente en su comisión, son más frecuentes. Además, tal diversidad y frecuencia tienen directa relación con el incesante cambio que caracteriza a las nuevas tecnologías, que puede verse principalmente en la creación de más novedosos y perfectos aparatos y servicios –como los celulares con Internet por ejemplo- que ofrecen otra vía para disfrutar de ellas en todo momento.

Todo esto ha ampliado las posibilidades de criminalidad informática, extendiendo la afectación que ellos pueden producir a casi todas las áreas de la vida cotidiana, con lo que se agrega otra cualidad a estos delitos; la gran peligrosidad que éstos conllevan.

1.3.5. Dificultad en su investigación, comprobación y persecución

Son delitos de especial complejidad en cuanto a su persecución, por una parte, debido a la rapidez de su comisión, la que puede tener lugar en cualquier parte del mundo, y por otra, a lo difícil que es determinar al autor del hecho –problemas que surgen del distanciamiento espacio/tiempo-, lo

que se suma a la facilidad para encubrir el ilícito y la posibilidad de borrar los rastros de las acciones cometidas a través de estos medios[247].

Esto, va unido a la peculiaridad de poder actuar de forma anónima en la red, la progresiva posibilidad de encriptación, codificación u ocultación de datos en los sistemas telemáticos, entre otras técnicas, lo que obstaculiza la determinación del autor de los hechos respectivos, disminuyendo la posibilidad de riesgo a ser descubierto. Lo que junto a la posibilidad de retracto –poder borrar la falta cometida y no dejar huellas- generan mayor conflicto a la hora de su averiguación.

Por otro lado, es de observar que los delitos digitales también detentan características más bien inmediatas -que se relacionan directamente con la naturaleza versátil y alterable de la delincuencia informática-, las cuales

[247] Bueno Arus., F. 1997. Els delictes relatius a la informática, en "El Codi Penal de 1995: Parte especial". Studia iurídica. Vol. 13. Centre d'Estudis Jurídics i Formació Especializada del Departament de Justícia de la Generalitat de Catalunya. Barcelona. p. 174. En: ROVIRA. Ob. Cit. p. 75.

hacen referencia a las medidas legislativas que existen o debiesen existir para este tipo de ilícitos[248] y que veremos a continuación.

1.3.6. Falta de reacción penal frente a delitos informáticos

Los delitos virtuales son una realidad innegable en nuestros días, respecto de los cuales ya no se puede retroceder, puesto que la criminalidad informática es un proceso en desarrollo que avanza por la vía de la tecnología. Escenario que no ha recibido respuesta inmediata por parte del derecho penal tanto en nuestro país como en el extranjero, a pesar de ser un fenómeno que instituye nuevas formas de lesión a bienes jurídicos, tanto clásicos como originales del último tiempo, lo que determina la posibilidad de que autores de tales acciones delictivas las ejecuten impunemente.

1.3.7. Desarrollo de nuevas modalidades delictivas

[248] DONOSO L., M. 2002. Bien Jurídico Protegido y Delincuencia Informática. Memoria para optar a la licenciatura en ciencias jurídicas y sociales. Santiago, Universidad Adolfo Ibáñez, Facultad de Derecho. pp. 81 y ss.

Así como la evolución de la tecnología es acelerada, también lo es el desarrollo de nuevas modalidades delictivas en torno a los sistemas informáticos, hecho que hace difícil la reacción pronta del derecho penal frente a la delincuencia virtual, debido a que existe gran dificultad para ir a la par con los cambios sociales que giran en torno a las nuevas tecnologías.

1.3.8. Dificultad en la determinación de Ley aplicable

En virtud del desfase espacio/tiempo, característico de los e-crimes, donde el autor puede cometer ilícitos a distancia o apartar el momento de comisión del hecho del de su materialización, se genera un problema al establecer la legislación aplicable en el caso concreto, que conlleva a conflictos jurisdiccionales entre los países en cuestión.

Si bien, existe un acuerdo entre la Doctrina comparada sobre la cooperación internacional en torno a la delincuencia informática, aún no se han creado normativas que hagan esto posible.

Es importante tener en cuenta que las características de este tipo de delitos están sujetas a modificación, en virtud de su peculiar naturaleza, cambio del que sólo sabremos pasados los años y que dependerá principalmente de los avances tecnológicos del futuro.

1.4. Bien o interés jurídico protegido

Vista la conceptualización de delito informático y sus respectivas características para constituirse como tal, es de suma importancia analizar cuál es el bien jurídico que protege este tipo de ilícito.

El bien jurídico es el interés individual o colectivo que por su significación social es digno de protección por parte del ordenamiento jurídico respectivo. Más aún, la existencia de numerosos y diversos intereses jurídicamente dignos de protección hace que se requieran diferentes vías para resguardarlos, siendo la jurídico-penal exclusiva de los que se consideran más relevantes para la sociedad, en virtud del carácter de ultima ratio del derecho penal.

Los delitos "computer-related", por lo general, se configuran sobre el bien jurídico tradicional de los delitos clásicos que se estiman cometidos a través de medios informáticos, sean éstos la vía o el objeto del comportamiento delictual. Sin embargo, hoy ya no es posible cubrir los nuevos intereses que nacen con la realidad actual -que afecta a la sociedad global- y que se basan principalmente en la importancia de la propia información, los datos en sí mismos y la seguridad de los sistemas y redes informáticas.

Se puede afirmar, entonces, que junto al interés jurídico tradicional se encuentra este nuevo bien protegido que se configura como "la información sobre la información", la que "permite acceder a la información y conocerla, atribuyéndole una consideración como valor o bien económico en si misma, y que da unidad sistemática a todas las modalidades delictuales vinculadas a la informática"[249], dándole esto la relevancia suficiente para que se requiera su cualificación jurídica y, la eventual y

[249] ROVIRA. Ob. Cit. pp. 70-71.

correspondiente sanción de ser –el bien jurídico "de la información"- lesionado[250].

Lo anterior está estrechamente ligado a la calidad de delito pluriofensivo del delito informático, en cuanto a que este bien jurídico "de la información", paralelo al interés protegido por el delito tradicional, se encontraría presente –sin afectar en lo absoluto la naturaleza jurídica del ilícito clásico en cuestión-, como cualidad relacionada y adicional, en diferentes tipos de ilícitos.

Estimamos que para determinar si un delito es electrónico, en cuanto al bien jurídico que protege, es necesario establecer si la información –que es objeto del ilícito- "en sí podría ser considerada como un valor socialmente aceptado, cuya protección demanda una respuesta sancionatoria de carácter penal" [251]. Ya que, el delito informático será –por ser llevado a cabo a través de medios telemáticos o que éstos sean el objeto del ilícito- el que se instituya en torno a la afectación de la información como bien jurídico

[250] Ibídem.pp. 69-71.
[251] ABOSO y ZAPATA. Ob. Cit. p. 210.

protegido esencial y básico, aunque no exclusivo, puesto que en virtud de estar relacionado por lo general a delitos clásicos, se debe tener presente que no será el único interés bajo protección.

Establecido que el bien jurídico fundamental protegido por la figura de los e-crimes es la información en sí misma, en tanto actualmente se considera un bien económico[252], es relevante analizar cuál debe ser el grado de afectación del mismo, para que se entienda necesaria una protección penal por parte del ordenamiento jurídico.

Como determinamos, en virtud del concepto de delito informático, bastaría con que el comportamiento delictual generara un riesgo, creara la potencialidad de afectar gravemente la información en sí misma que constituye el bien jurídico protegido esencial, y que a su vez se viera posiblemente lesionado el interés colectivo que nace de la seguridad de los sistemas y redes de almacenamiento, tratamiento, y transferencia de la

[252] En la actualidad la información se constituye como un nuevo bien económico, en cuanto se considera poderoso a quien la detenta, se abastece y dispone de ella. Idea –"la información es poder"- que ha sido acuñada por diversos autores, ya en las áreas de la ciencia, la filosofía y la economía.

información. Esto, independiente del requisito de existencia de un elemento subjetivo o incluso lesivo –como sería la presencia de dolo en algunos casos o daño en otros- de los delitos clásicos que concurrirían conjuntamente en el caso concreto[253].

Cabe destacar que el quebrantamiento del bien de la información debe tener tal envergadura que traiga consigo indiscutiblemente una peligrosidad de lesión respecto de otros bienes jurídicamente protegidos, generalmente tradicionales, para que se requiera una respuesta jurídico-penal, ya que de no ser así –cuando sólo se trata de una intromisión a la información o un leve quebranto de la misma sin consecuencias altamente riesgosas- sólo se necesitaría una sanción administrativa.

En el caso chileno, la Ley 19.223 crea un nuevo bien jurídico a proteger por esta normativa, el cual, determinado en la historia de esta Ley, es "la calidad, pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan". Entonces, podemos establecer que, siguiendo

[253] ROVIRA. Ob. Cit. pp. 72-74.

con lo expuesto anteriormente, en esta normativa también se abogaría por el bien jurídico de la información en sí misma, como bien o valor económico. Por esto, la creación de un nuevo bien jurídico basado en las cualidades de la información, abstraería al mismo de los intereses jurídicos tradicionales que protege la ley penal, como el referente a la intimidad, el patrimonio, entre otros, aún cuando pueden ser afectados de forma simultánea por la conducta sancionada[254].

1.5. Tratamiento legal en derecho comparado

Ya establecido que la cibercriminalidad, fenómeno inherente del último tiempo, se ha convertido en una amenaza a nivel mundial, es lógico que se requiera de un esfuerzo internacional para el enfrentamiento de este nuevo tipo de delincuencia. Y en virtud de la necesidad de una cooperación entre países, pasaremos a revisar el tratamiento que hacen de los delitos informáticos los organismos internacionales más importantes.

[254] DURAN. Ob. Cit. pp. 81 y ss.

Los delitos informáticos encuentran un anterior y más extenso estudio y, con ello, un tratamiento legislativo correspondiente, en la realidad Europea y Estadounidense, por lo que también merece sin lugar a dudas de un análisis por nuestra parte, con el fin de observar las políticas de delitos informáticos que se desarrollan en países con el grado de influencia que este conglomerado detenta, y determinar aquellos puntos que pueden favorecer a la cooperación internacional en la materia.

Junto a esto, examinaremos asimismo la situación de Argentina y México, para así indicar -parcialmente claro- el camino que ha recorrido América Latina respecto de los ciberdelitos.

1.5.1. Directivas y recomendaciones de Organismos Internacionales

1.5.1.1. Organización para la Cooperación y Desarrollo Económico

Desde muy temprano, la O.C.D.E. propone armonizar las legislaciones nacionales sobre cibercrimen, con el objeto de poder mejorar la capacidad

para hacer cumplir la ley ante estos delitos[255]. En 1983 se crea la Comisión Internacional de Expertos en Derecho Informático de los países miembros con la intención de hacer una revisión de la legislación hasta la fecha, lo que se traduce en un informe emitido durante 1985, donde se busca impulsar propuestas para combatir el cibercrimen, analizando entre otras cosas las distintas formas de realización de estos delitos, la capacidad de las legislaciones nacionales y los instrumentos internacionales para combatir la delincuencia informática y estableciendo una lista mínima de delitos que los países podrían tipificar [256] en base al reconocimiento de cinco formas principales de abuso: el fraude informático, la falsificación informática, el sabotaje informático, la copia ilegal de programas informáticos y el acceso ilegal a sistemas informáticos[257].

[255] BRENNER., S. 2012. La Convención sobre Cibercrimen del Consejo de Europa. [en línea] Revista Chilena de Derecho y Tecnología. Centro de estudios de derecho informático. Vol.1 n°1. pp. 221-238. Universidad de Chile. <http://www.revistas.uchile.cl/index.php/RCHDT/article/viewFile/24030/25629> p.225

[256] UNIÓN INTERNACIONAL de telecomunicaciones. 2009. El coberdelito: Guía para los países en desarrollo. [en línea] recursos jurídicos contra el ciberdelito. 238p. <http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf> p.110

[257] ROVIRA. Ob. Cit.p. 284

La O.C.D.E. define de manera vaga e imprecisa el abuso informático como "todo comportamiento ilegal o contrario a la ética o no autorizado que concierne a un tratamiento automático de datos y/o de transmisión de datos"[258].

Con esto, podemos señalar que el esfuerzo realizado por la O.C.D.E. busca abarcar tanto conductas penales como extrapenales, dando pie al progresivo abandono en sede penal de los ciberdelitos[259] [260].

Con posterioridad a lo señalado, la O.C.D.E. ha seguido avanzando en el tema, y entre muchas otras intervenciones a nivel internacional, podemos encontrar que en el año 2005 se publica un análisis sobre el impacto del

[258] Ruiz, V. En: ROVIRA. Ob. Cit. p.285

[259] HERNANDEZ., L. 2009. El delito informático. [en línea] Eguzkilore n°23 pp.227-243. San Sebastián, España. <http://www.ivac.ehu.es/p278-content/es/contenidos/boletin_revista/eguzkilore_23_homenaje_ab/es_eguzki23/adjuntos/18-Hernandez.indd.pdf> p.232

[260] Podemos decir con esto que "se trata de una primera aproximación a un posible concepto, adoptada en un principio por varios autores con el argumento de que una definición de esa amplitud permitiría el tratamiento de las mismas hipótesis de trabajo para distintas disciplinas y podría así usarse una misma definición en análisis penales, económicos, sociológicos, etc." En: HERNANDEZ. Ob. Cit. p.232

correo basura en los países en desarrollo[261], y en 2007 emite un informe relativo al tratamiento del ciberterror por la petición de la Unidad de Planificación Estratégica de la Oficina Ejecutiva del Secretario General de las Naciones Unidas[262].

1.5.1.2. Organización de las Naciones Unidas

La O.N.U., debido al gran interés que detenta sobre el tema, ha puesto en la palestra la discusión respecto de los delitos informáticos, llevando a cabo varios Congresos sobre Prevención del Delito y Tratamiento del Delincuente, en donde nos parece relevante destacar el Octavo de ellos celebrado el año 1990 en La Havana, Cuba, con el objetivo principal de legislar contra el ciberdelito[263].

El resultado de esta instancia fue la publicación en 1994 de un Manual sobre la Prevención y Control del Delito Informático, en el que se considera a éste como "una forma nueva de crimen transnacional y que para tratarlo

[261] UNIÓN INTERNACIONAL. Ob. Cit. p.111
[262] Ibídem. p.112
[263] Ibídem. p.99

se requiere efectivamente de la cooperación internacional concertada"[264]. Asimismo, se puede decir que este Manual "recoge los puntos problemáticos fundamentales en el ámbito de la cooperación internacional en el área del ilícito informático y la ley penal, y si bien no fija una definición concreta del delito informático, utilizando de forma intercambiable los términos "computer crime" y "computer-related-crime", reconoce que los términos "computer misuse" (mal uso informático) y "computer abuse" (abuso informático) se usan asimismo frecuentemente de forma indistinta"[265].

Por otro lado, y dentro de las características más importante del Manual, se puede destacar la clasificación de las cinco modalidades más comunes de delito informático[266]:

[264] ROVIRA. Ob. Cit. p.308
[265] Ibídem. p.308-309
[266] CASSOU R., J. 2009. Delitos informáticos en México. [en línea] Revista del Instituto de la Judicatura Federal. Núm. 28. pp. 207-236. <http://www.ijf.cjf.gob.mx/publicaciones/revista/28/Delitos_informáticos.pdf> p.225

- Fraudes cometidos mediante manipulación de computadoras: como la manipulación de datos de entrada, de programas, de datos de salida y el fraude efectuado por manipulación informática.

- Falsificaciones informáticas: utilizando sistemas informáticos como objetos o como instrumentos.

- Daños o modificaciones de programas o datos computarizados: como el sabotaje informático, los virus, gusanos, bomba lógica o cronológica.

- Accesos no autorizados a servicios y sistemas informáticos: el acceso no autorizado a sistemas o servicios, piratas informáticos o hackers, la reproducción no autorizada de programas informáticos con protección legal[267].

[267] URETA A., L. 2009. Retos a superar en la administración de justicia ante los delitos informáticos en el Ecuador. [en línea] Tesis de grado para optar al título de magíster en sistemas de información gerencial. Facultad de ingeniería en electricidad y computación, Escuela Superior Politécnica del Litoral. Guayaquil, Ecuador. 113p. <http://www.dspace.espol.edu.ec/bitstream/123456789/5792/5/TESIS%20-%20DELITOS%20INFORMATICOS%20EN%20ECUADOR%20Y%20ADMINISTRACION%20DE%20JUSTICIA.pdf > p.9

Finalmente, se puede indicar que en relación a la prevención del delito informático en general, y con especial importancia respecto a la cooperación internacional, el Manual establece que "siendo la criminalidad informática no meramente un problema nacional, sino internacional, o por lo menos lograr conceptos comunes de lo que comprende, de aumentar la cooperación supranacional, y armonizar los procedimientos procesales para sancionarlo"[268].

1.5.1.3. Organización de los Estados Americanos

Finalmente, los Estados Miembros de la O.E.A. han intentado impulsar el crecimiento de sus países y de la economía global desde las distintas áreas de producción y comercialización, pero Internet se ha presentado como una amenaza que ostenta peligros para los usuarios por la creciente delincuencia que se genera en este medio y que puede perjudicar tanto los sistemas utilizados, como la información que se maneja en ellos.

[268] ROVIRA. Ob. Cit. p.312

Desde 1999 la O.E.A. ha manifestado su preocupación por el ciberdelito[269], dando mandato a la Reunión de Ministros de Justicia de las Américas (REMJA), quienes además de comprometerse a trabajar el tema y buscar soluciones, desarrollaron la Estrategia Interamericana para Combatir las Amenazas a la Seguridad Cibernética[270] [271], y en reflejo a ello, celebró el 2003 una Conferencia sobre Seguridad Cibernética, intentando demostrar la gravedad de las amenazas a la seguridad en la red.

Esta estrategia se basa en el apoyo constante del Comité Interamericano contra el Terrorismo (CICTE) y de la Comisión Interamericana de Telecomunicaciones, entre otros, puesto que con la experiencia y esfuerzos de estos grupos especializados se busca crear una cultura de seguridad cibernética. Además, reconocen que la fórmula para lograr este objetivo será proporcionando información a los usuarios y operadores de computadores, fomentando asociaciones públicas y privadas con

---

[269] UNIÓN INTERNACIONAL. Ob. Cit. p.114

[270] ACURIO D., S. Delitos Informáticos: Generalidades. [en línea] Cátedra de Derecho Informático, Pontificia Universidad Católica del Ecuador. 67p. <http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf> p.43
Esta estrategia ha sido reconocida en la Asamblea General de la resolución AG/RES. 1939 (XXXIII-0/03)

[271] UNIÓN INTERNACIONAL. Ob. Cit. p.114

intenciones de aumentar la educación respecto al tema y finalmente, promoviendo la adopción de políticas y legislación sobre los delitos informáticos[272].

1.5.2. Normativa en el Sistema Europeo

En vista de la creciente problemática que significó el uso de la tecnología y el Internet para actuar indebidamente y así cometer delitos, el Sistema Europeo decide edificar un conjunto de normativas relativas a los e-crimes, con el objeto de enfrentar dicho fenómeno con herramientas actuales y adecuadas a la nueva realidad.

La Unión Europea ha erigido su política legislativa respecto de la delincuencia virtual sobre la base de los Derechos Humanos, con el soporte principal del "Convenio Europeo para la protección de los Derechos Humanos y Libertades Fundamentales", de noviembre de 1950, con la finalidad de que las personas hallen protección de sus derechos más esenciales frente a las nuevas tecnologías con el potencial riesgo que éstas

[272] ACURIO. Ob. Cit. pp.43-45

conllevan. Consecuencia de esto, la primera iniciativa que se lleva a cabo por la Asamblea del Consejo de Europa es constatada en la Resolución 65/509/CE de 1968, normativa útil para el estudio de los nuevos logros científicos y técnicos, y su relación con los derechos humanos.

La delincuencia informática entró a formar parte de la Agenda europea a principios de los 80[273], en lo relativo a la criminalidad en los negocios, surgiendo consecuentemente la adopción de la Recomendación R (81) 12, de junio de 1981, en la cual la criminalidad informática quedó incluida dentro de la delincuencia económica como una "infracción no específica", que se ejemplificaba con el robo de datos informáticos, la violación de

[273] Si bien antes de la década de los 80 no se habla de los delitos informáticos propiamente tales, ya desde el año 1973 hasta 1987, el Sistema Europeo crea una serie de reglas que persiguen la seguridad de la vida privada de las personas físicas en los sistemas electrónicos, tanto en el sector público como en el privado, proceso afrontado directamente al progreso tecnológico de la región. El desarrollo de esta política fue enfocado principalmente en la protección de datos, información que se especifica es almacenada en bancos electrónicos y que puede ser compartida a través de la red, alcanzando la legislación a abarcar variados campos; como el financiero, el de salud, el laboral, entre otros. En: REVISTA INFORMÁTICA Jurídica. 2013. Legislación. Unión Europea, Consejo de Europa y Comité de Ministros del Consejo de Europa. [en línea] <http://www.informatica-juridica.com/legislacion/union_europea.asp>

secretos, la manipulación de datos, etc. Esta recomendación, si bien abogaba por una mínima intervención penal, alentaba a los países miembros de la Unión Europea a revisar sus legislaciones, para hacer de ellas un conjunto coherente y completo de normas, y a la vez flexible para enfrentar a este nuevo tipo de criminalidad que evolucionaba a pasos agigantados junto al cambio de la economía y la tecnología[274].

Ya en el año 1989, el Consejo de Europa convoca al comité de expertos para la redacción de la Recomendación R (89) 9 sobre criminalidad en relación con el ordenador, en la cual se reconoce la importancia de responder adecuada y rápidamente al nuevo reto que significan los delitos informáticos. En este documento, se aconsejaba a los Estados parte que al revisar su legislación o en la creación de la misma, consideraran lo prescrito acerca de los e-crimes de esta recomendación, y que reportaran consecuentemente los cambios que sufriera su legislatura, sus prácticas

[274] ROVIRA. Ob. Cit. pp. 287-291.

judiciales o las experiencias de cooperación internacional[275] en relación a los delitos virtuales [276].

Al comité, en esta oportunidad, se le dificultó la tarea de definir el "delito informático", por considerar que todos los intentos de delimitar este concepto detentaban mayormente desventajas, lo que no permitía reconciliar de forma precisa, y sin lugar a dudas, todos los elementos que el e-crime dispone para lograr una correcta acepción. Por dicha razón, se decidió dejar abierto el término de "delito informático", en el cual se contenían todos las ofensas enumeradas y definidas en las legislaciones

[275] Todas las cuestiones relacionadas con la cooperación internacional y procesal que no fueron tratadas con anterioridad, se consideraron en la Recomendación R (95) 13, de 1995, la cual, motivada por el riesgo de que los sistemas de información y la información electrónica fueran usados para cometer delitos, y por la falta de normas procesales de carácter internacional que apoyaran la investigación criminal entre los países, este documento incita a los Estados miembros a compatibilizar sus legislaciones en la materia, con el fin de implementar y cumplir con un plan de acción uniforme. En: ROVIRA. Ob. Cit. pp. 301-302.

[276] EUROPEAN COMMITTEE ON CRIME PROBLEMS. 1990. Computer-related crime. Recommendation No. R. (89) 9 on computer-related crime and final report of the European Committee on Crime Problems. Strasbourg. Council of Europe, Publishing and Documentation Service. p.7.

nacionales, presentando el comité sólo una lista mínima de los delitos que cada país miembro debía regular[277].

Si bien esta recomendación estableció los conceptos que debían definirse por las naciones dentro de los parámetros relacionados a ciertas formas de malos usos informáticos, ésta detentaba la calidad de sugerencia, por lo que fue insuficiente para asegurar una eficacia palpable en la lucha contra esta nueva amenaza, la cual sólo puede darse bajo la exigencia de un instrumento internacional de carácter obligatorio[278].

A fines de la década de los 90, la Comunicación "COM 1999/687" –no

[277] Ibídem. pp.12-14.

[278] Medida legislativa que además debía comprender los tópicos de cooperación internacional, derecho sustantivo y procesal para que la misma funcionara en un contexto donde las tecnologías de la información son protagonistas y actuales a nuestros tiempos. Durante la siguiente década, se siguió con el trabajo para construir una legislación que protegiera adecuadamente a las personas físicas respecto, principalmente, de sus datos personales que se vieran recolectados en sistemas electrónicos, y a la seguridad de los sistemas de información. A su vez, el Consejo de Europa también se preocupó de tratar los delitos computacionales a través del despliegue de normativas referentes al derecho de autor, el comercio electrónico, los documentos electrónicos, los derechos de menores frente a ilícitos cometidos en la red, la protección de la vida privada en Internet, el spam, etc. En: REVISTA INFORMÁTICA . Ob. Cit.

publicada en el Diario Oficial-, pone en marcha la iniciativa "eEurope" de la Comisión para el Consejo Europeo extraordinario de Lisboa de 23 y 24 de marzo del año 2000, que buscaba crear "una sociedad de la información para todos". Tal ambicioso programa perseguía difundir en la mayor medida posible las tecnologías de la información, consistiendo la estrategia en "orientar buena parte de los esfuerzos financieros, científicos, tecnológicos, empresariales y sociales hacia la creación de una sociedad europea del conocimiento (SEC)", con la pretensión de que la Unión Europea se convirtiera en líder mundial de la sociedad de la información y el conocimiento para el 2010[279].

Esta tendencia se continúa con el programa "eEurope 2002", el que tenía como principales objetivos; el llevar la era digital y de la comunicación al ciudadano común, a través de un mayor acceso a las tecnologías en los hogares, las escuelas y las empresas; crear una comunidad que domine el ámbito virtual a través del apoyo a las nuevas ideas por parte del Estado; y

[279] ECHEVERRÍA, J. 2007. Gobernanza de la sociedad europea de la información. [en línea] Rev. iberoam. cienc. tecnol. soc. v.3 n.8. Ciudad Autónoma de Buenos Aires, abr. 2007. <http://www.scielo.org.ar/scielo.php?pid=S1850-00132007000100006&script=sci_arttext>

reforzar un proceso de liberalización de las tecnologías socialmente integrador[280]. Junto a esto, se enfatiza la necesidad de que tal desarrollo se dé con un nivel idóneo de seguridad en las redes y con un debido embate a los ilícitos informáticos[281].

El sistema Europeo, ya con un ánimo indudable de querer hacerle frente a la ciberdelincuencia, dicta la "Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones: Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos" (COM 2000/890/final) - tampoco publicada en el Diario Oficial-. En ésta, se define ampliamente lo que es un delito informático, entendiendo por aquel; todo delito que implique la utilización de las tecnologías informáticas, donde exista una explotación de las redes

[280] POLITICA DE la sociedad de la información. Guía práctica de la Unión Europea. No. 27. [en línea] <http://www.madrid.org/cs/Satellite?blobcol=urldata&blobheader=application%2Fpdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1352807270520&ssbinary=true>

[281] EUROPA. Síntesis de la legislación de la UE. 2005. eEurope: Una sociedad de la información para todos. [en línea] <http://europa.eu/legislation_summaries/information_society/strategies/l24221_es.htm>

de información y comunicación sin ninguna dificultad geográfica, y haya circulación de datos intangibles y volátiles, siempre contando con un elemento subjetivo de intencionalidad.

Tal abstracta definición sólo era delimitada por los delitos que eran tratados hasta la fecha por la legislación europea común, en los cuales figuran; los delitos contra la intimidad relacionados principalmente con el almacenamiento y uso indebido de datos personales; la difusión de pornografía infantil vía Internet; los delitos económicos, los de acceso no autorizado y sabotaje; y los delitos relativos a la propiedad intelectual y derechos de autor[282].

Es en el año 2001 cuando la Unión Europea coincide en la creación del primer tratado internacional que versa sobre delitos cometidos a través de Internet y otras redes informáticas. El Convenio de Budapest sobre el Cibercrimen (desde ahora el Convenio) fue firmado por todos los estados miembros, además de Estados Unidos, Canadá, Japón y Sudáfrica –que no son parte del Consejo de Europa-, y que además ha sido adoptado por varios

[282] Ídem.

otros países que buscan normativas donde apoyarse para luchar contra la delincuencia informática[283].

El Convenio tiene el carácter de ser una política penal común que busca proteger a la sociedad frente a la ciberdelincuencia, a través de dos elementos principales que son: la adopción de una legislación adecuada y la mejora en la cooperación internacional. Si bien este tratado no define lo que es el delito informático, delimita un catálogo de ilícitos virtuales que abarcan variados bienes jurídicos. Además, determina qué medidas deberán tomarse a nivel nacional en el ámbito del derecho penal sustantivo y en el derecho procesal[284].

De acuerdo a los avances que se hicieron en la materia, el Sistema Europeo continúa con su esfuerzo de posicionarse como una comunidad tecnológica y actualizada, para lo que se sigue con el plan "eEurope 2005",

[283] PEÑA O., P. 2013. ¿Cómo funciona internet? Nodos críticos desde una perspectiva de los derechos. Guía para periodistas. Chile. ONG Derechos Digitales. p. 42.
[284] CONSEJO DE EUROPA. 2001. Convenio de Budapest. [en línea] <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_spanish.PDF>

en el contexto del sexto programa marco que se extiende del 2002 al 2006, fase del programa que muestra una mayor sensibilidad social, con el fin de disminuir la "brecha digital" –nueva modalidad de desigualdad social basada en el acceso a las nuevas tecnologías y al Internet-. A pesar de las mejoras, en 2005 se decide cambiar el programa "eEurope" por el "plan i2010" para los siguientes años[285] [286].

Con este último plan de acción se trata de regular la nueva revolución tecnológica que nace con Internet, donde se prioriza la lucha contra los delitos informáticos, persiguiendo principalmente la seguridad en la red –utilizándose para esto, por ejemplo, los programas "Safer Internet" y "Safer Internet Plus"-.

Es necesario recordar que la voluntad de hacerle frente a la ciberdelincuencia data -con mayor fuerza- desde inicio de los años 80, decidiendo el Sistema Europeo que su principal línea de acción consistiría

[285] ECHEVERRÍA. Ob. Cit.
[286] MOLINA., C. 2009. El derecho comunitario y la I+D+T: Hacia el diseño de un perfil para el futuro. Textos universitarios. Universidad de Alcalá, servicios de publicaciones. Dykinson. Madrid, España. 31 y ss.

en que las "propuestas legislativas se basaran fundamentalmente en la armonización de las leyes de cada país comunitario (…) en relación de los sistemas de derecho penal en lo referente a los delitos informáticos y la aplicación del reconocimiento mutuo en lo que respecta a las medidas cautelares dictadas en la investigaciones llevadas a cabo en este tipo de delitos". Junto a esto, también se instauran actuaciones como "la creación de unidades especializadas, la formación permanente de los cuerpos de seguridad del estado y la creación de un foro", que buscaban conseguir el incremento de la cooperación judicial en materia penal.[287]

1.5.3. Normativa en Estados Unidos

Cabe señalar primeramente que en Estados Unidos existe un sistema estatutario, en donde cada Estado proporciona sus propios estatutos penales, mientras que el Gobierno Federal se limita a promulgar ciertas normas de carácter nacional. Por esto, es menester hacer un breve análisis de ambas categorías.

[287] Ibídem. p. 126.

1.5.3.1. Nivel legislativo federal

El interés de este país por regular los cibercrímenes, nace en 1977, cuando el senador Ribicoff hace la primera propuesta para legislar sobre el tema[288]. Durante los años 1981 –con el Proyecto de la Ley Federal de Protección de Sistemas Informáticos-, 1982 –con la "Electronic Funds Transfer Act"-, 1984 –con la "Counterfeir Acces Device and Computer Fraud"- que se integró al "Federal Criminal Code" donde "se regularon y tuvieron ya cabida con carácter general los fraudes y conductas abusivas mediante procedimientos informáticos que afectaran a un ordenador de interés federal"[289], significó una demanda a nivel doctrinal, en donde la ley no sólo mostrara un interés federal, sino que debía proteger a cualquier persona en el país que se viera afectada por un delito de este tipo. Esto llevó a que en 1986 se hiciera una reforma denominada "Computer Fraud and

[288] RAMOS., J. Delitos informáticos. [en línea] 9p. <http://julioramos.bligoo.com.mx/media/users/23/1189400/files/338082/DELITOS_INFORMATICOS.pdf> p.1

[289] ROVIRA. Ob. Cit. p.365

Abuse Act", que amplió la antigua norma, incorporando aquellos delitos informáticos que se requerían[290].

En 1994 se adopta en Estados Unidos el Acta Federal de Abuso Computacional, que modifica el Acta de 1986. Esta reforma, consideramos, se hizo "con la finalidad de eliminar los argumentos híper-técnicos acerca de qué es y qué no es un virus, un gusano, un caballo de Troya y en qué difieren cada uno de ellos, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas (18 U.S.C.: Sec. 1030 (a) (5) (A)). La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus"[291],

[290] Se incorporaron tres figuras nuevas: "la primera de las cuales era precisamente el acceso informático, no sólo uso del ordenador con la intención de defraudar; y mediante el cual se obtiene cualquier cosa de valor; asimismo se modificó el concepto de "ordenador de interés federal" como afectado, pasando a ser únicamente aquellos pertenecientes o usados por el gobierno federal o institución financiera, siendo suficiente con que estén integrados en una red interestatal, es decir extendida por distintos estados federados". En: ROVIRA. Ob. Cit. p.366.

[291] GUERRA V., A. 2011. Delitos informáticos - Caso de estudio. [en línea] Tesis para obtener el grado de Maestro en Ingeniería en seguridad y tecnologías de la información. Instituto Politécnico Nacional, Escuela Superior de Ingeniería Mecánica y Eléctrica. México D.F. 124 p.

ya que no se limita a una clase de estos, sino que previene cualquier otra especie que se pueda crear y que afecte programas, bases de datos, etc.

Cabe destacar además que dicha Acta, hace una distinción en el tratamiento del delito entre aquellos que lancen ataques de virus de manera temeraria de aquellos que los realicen con la intención de causar perjuicios. Así, para quienes intencionalmente causan un daño, el castigo es mayor -10 años más una multa- en comparación a la sanción para aquellos que lo transmiten de manera imprudente y sin intención de causar estragos –la sanción en ese caso sería entre una multa y un año de prisión-[292] [293].

<http://www.repositoriodigital.ipn.mx/bitstream/handle/123456789/12653/TESIS.%20DELITOS%20INFORMÁTICOS-CASO%20DE%20ESTUDIO.pdf?sequence=1> pp.28-29

[292] RAMIREZ B., E. AGUILERA R., A. 2009. Los delitos informáticos. Tratamiento internacional. [en línea] Contribuciones a las ciencias sociales. 13p. <http://www.eumed.net/rev/cccss/04/rbar2.pdf> p.10-11

[293] Esta idea de que la reforma es un gran cambio en el concepto de virus, es respaldada por otros, quienes expresan que "la nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen. Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple qué se debe entender como acto delictivo". En: ESTRADA G., M. Delitos informáticos [en línea] 26 p.

Se puede además inferir que el objetivo al hacer estas modificaciones era aumentar la protección a las personas, los negocios, los estados y cualquier organismo que se vea perjudicado con la interferencia, el acceso no autorizado a programas, sistemas computarizados o bases de datos[294].

Existe además un "Departamento de Justicia de los Estados Unidos Sección de Delitos Informáticos y Propiedad Intelectual" encargado de implementar nuevas estrategias de acuerdo a las necesidades para combatir estos delitos, así como también previene, investiga y enjuicia los delitos informáticos[295].

1.5.3.2. Nivel legislativo estatal

<http://perso.unifr.ch/derechopenal/assets/files/articulos/a_20080526_32.pdf> p. 16

[294] Ibídem. p.11

[295] DEPARTAMENTO DE Justicia de los Estados Unidos. Sección de delitos informáticos y propiedad Intelectual. [en línea] 1p. <http://www.oas.org/juridico/english/cyb_mex_info.pdf>

Los Estados desde la década de los 80, han introducido en sus estatutos nuevos delitos relativos a la delincuencia vinculada a sistemas informáticos[296]. Siendo el más importante el delito de fraude informático –o computer fraud- que se encuentra regulado en casi todos los Estados, muy similar a la figura de la estafa llevada a cabo mediante la manipulación informática[297].

Así, es posible hacer una breve clasificación de acuerdo a la forma en que es tratada esta figura delictiva en los distintos Estados.

Aquellos Estados que han creado expresamente una figura de fraude informático en el ámbito patrimonial de forma más o menos escueta son por ejemplo: el Estado de Virginia, de Arkansas y Mississippi, entre otros[298]. Mientras que los que la han desarrollado de forma más completa son los Estados de Arizona, Dakota del Norte, Hawai e Illinois[299].

---

[296] ROVIRA. Ob. Cit. p.349
[297] Ídem.
[298] Podemos encontrar además estados como los de Virginia, Delaware y Louisiana. En: ROVIRA. Ob. Cit. pp.350-355
[299] Ídem.

También podemos encontrar Estados que, sin expresa mención a la figura del fraude informático, pero sancionándose el acceso o uso informático con inclusión de la finalidad defraudadora, no hacen distinción alguna entre los delitos informáticos y los delitos contra la propiedad, como son el caso del Estado de California, Montana, New Jersey y Pensilvania. Mientras que existen otros que hacen una previsión expresa y autónoma del delito informático, como Colorado, Oklahoma, Kansas y Dakota del Sur, entre otros[300].

Según Rovira, como "sistema peculiar es la consideración de la finalidad defraudadora como elemento agravatorio del tipo del mal uso o acceso indebido informático" como el caso de los Estados de Missouri, Nevada, Ohio, Wisconsin, Wyomin y Florida[301]. Mientras que otros estatutos han seguido el "sistema normativo de inclusión de las manipulaciones

[300] También se encuentran los estados de Idaho, Oregon, Utah, Carolina del Sur, Tennessee, Georgia, Kentucky, Nuevo México, Carolina del Norte y Rhode Island. En: ROVIRA. Ob. Cit. pp.355-360.
[301] ROVIRA. Ob. Cit. pp.360-362

informáticas defraudatorias patrimoniales en las figuras clásicas" como el Estado de Alaska[302].

Cabe mencionar a aquellos que "no regulan el fraude informático, ni concretamente las manipulaciones defraudatorias patrimoniales, con autonomía propia fuera de las figuras clásicas de los delitos contra la propiedad" como es el caso del Estado de Alabama, New York, Texas, Washington, ni tampoco New Hampshire, entre otros[303]. Y aquellos que ni siquiera tienen una regulación expresa de ilícitos informáticos son los estatutos de Estados de Maine y de Vermont[304].

1.5.4. Normativa de Argentina

En el caso de la República de Argentina, la nueva realidad jurídica de los delitos informáticos ha sido abordada desde dos perspectivas: una que ve la cibercriminalidad como una problemática que ha de ser tratada de forma

[302] Ibídem. p.362
[303] También se encuentran dentro de ellos los Estados de Conneticut, Indiana, Iowa, Maryland, Massachusetts, Michigan, Minnesota, Nebraska. En: ROVIRA. Ob. Cit. pp.363-364.
[304] ROVIRA. Ob. Cit. p.365

separada, teniendo en cuenta el bien jurídico novedoso a proteger, y otra que estima debe ser incluida en el Código penal, en virtud de que los diferentes e-crimes abarcan los objetos jurídicos ya establecidos en el mencionado cuerpo normativo.

En un principio, y en vista de la rápida evolución de los e-crimes, la Secretaría de Comunicaciones del Ministerio de Infraestructura y Vivienda de la Nación presenta el Anteproyecto de Ley de Delitos Informáticos, optando por la creación de una ley específica para este tipo de ilícitos. Esto, en razón de que los ciberdelitos detentan un objeto jurídico novedoso –la información- digno de una protección jurídico-penal especial, que requiere de la posibilidad de creación de nuevos tipos penales –principalmente el hacking, el cracking y el fraude informático, de tratamiento privilegiado-, sin poner en peligro la armonía del Código punitivo que podría conllevar a futuras modificaciones del mismo[305].

[305] AROCENA., G. 2012. La Regulación de los delitos informáticos en el Código Penal Argentino. Introducción a la Ley Nacional Núm. 26.388. [en línea] Boletín de Derecho Comparado, vol. XLV, núm. 135, septiembre-diciembre. Universidad Nacional Autónoma de México. <http://www.redalyc.org/pdf/427/42724584002.pdf> pp. 955-957.

Cuando Argentina decide abogar por una reforma de su Código Penal, con la Ley 26.388 del año 2008, introduce en él las modalidades delictivas relativas a la informática, procediendo el desarrollo de la nueva legislación penal concerniente a la cibercriminalidad –vigente hasta el día de hoy- de forma desconcentrada, incluyendo los distintos tipos legales en los diversos títulos del Código Penal, conforme a los diferentes bienes jurídicos tutelados por aquél[306].

Dentro de la reforma que se hace al Código Penal, en la cual no se define el delito informático como tal, sí se agregan ciertos elementos de la informática, principalmente el uso del Internet, en diversas figuras penales ya existentes, como la pornografía infantil y la violación de privacidad y secreto. Y se incluyen nuevas formas de delito, como el acceso no autorizado o ilegítimo de un sistema o dato informático restringido

[306] Es importante destacar que dicha ley se ha basado en el Convenio sobre Cibercriminalidad de Budapest, redactado en 2001 por el Consejo de Europa, el cual fue adherido por este país en 2010. En: AROCENA. Ob. Cit. p. 954.

(intruismo informático no autorizado o hacking) y el sabotaje informático (cracking)[307].

Para el tratadista Gabriel Cámpoli, respecto de los delitos informáticos, la legislación argentina se detuvo esencialmente en el debate conceptual entre los términos "por medio de" y "en contra de", cuestión que finalmente se determina por el hecho de que la mayoría de los ciberdelitos se consideraron como sólo nuevos medios para cometer ciertos ilícitos tradicionales[308], razón por la cual se agregan los mismos términos en distintos títulos del mencionado cuerpo normativo según el objeto jurídico que protegen, correspondientes consecuentemente a figuras penales clásicas.

Entendiendo que tal cambio en la legislación penal argentina, que fue ampliada al ámbito de la informática y las nuevas tecnologías, fue un progreso, es claro que era insuficiente para enfrentar el rápido crecimiento de la ciberdelincuencia. Por esto, Argentina también debió desplegar una

[307] AROCENA. Ob. Cit. pp. 958-985.
[308] NAVA., A. 2005. Análisis de los delitos informáticos. 1a.ed. Porrúa, México. pp. 87-88.

institucionalidad que fuera acorde a los cambios legales, y en donde se pudieran denunciar los delitos informáticos, lo que derivó en la creación de: la División Delitos Tecnológicos de la Policía Federal Argentina, las Áreas Especiales de Investigaciones Telemáticas de la Policía Metropolitana, la Dirección Nacional de Protección de Datos Personales, y el Instituto Nacional contra la Discriminación, la Xenofobia y el Racismo, entre otros[309].

Si bien esta reforma se realiza con unos 15 años de distancia del avance en la materia hecha por Chile, con la creación de esta Ley, Argentina armoniza su legislación con las del resto de Sudamérica, siendo un aporte indiscutible al enfrentamiento integral que debe hacerse en el bloque regional respecto de los delitos informáticos, con el fin de disminuir las posibilidades de impunidad en este tipo de ilícitos.

1.5.5. Normativa de México

[309] ARGENTINA Cibersegura. ¿Cómo realizar una denuncia ante un delito informático? [en línea] <https://www.argentinacibersegura.org/admin/resources/files/consejos/28/1308_-_Qué_hacer_ante_un_delito_informático.pdf>

Con la finalidad de observar y entender el tratamiento que hace México de los delitos informáticos, debemos recordar que la federalización del país consiguió que se imitara el modo legislativo de los Estados Unidos – forma diametralmente distante de la cultura legal que fue heredada por México-, lo que, con su Constitución de 1824 (manteniéndose esto en las siguientes constituciones), permitió a los estados que expidieran sus propias leyes en todas las funciones que no estuviesen expresamente concedidas a los funcionarios federales[310]. Consecuencia de esto, a lo largo del siglo XX se solidificó una multiplicidad de códigos penales en la República que perjudicó la uniformidad del escenario legislativo mexicano.

Dentro de esta composición de ordenamientos, son pocos los estados que consideran a los ciberdelitos dentro de su catálogo penal, menos los que hacen una división de tal categoría, e incluso, existen algunos estados en los

[310] NAVA. Ob. Cit. pp. 43-44.

que ni siquiera se ha considerado que la computación pueda ser el medio comisivo en la realización de este tipo de ilícitos[311].

La primera vez que se legisla en México sobre los delitos informáticos es en el estado de Sinaloa en 1992, donde se establecía en el Código Penal -artículo 217- que: "comete delito informático, la persona que dolosamente y sin derecho: I. Use o entre a una base de datos, sistemas de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar; ejecutar o alterar un esquema o artificio con el fin de defraudar; obtener dinero, bienes o información; o II. Intercepte, interfiera, reciba, use,

[311] Los estados que tratan los delitos informáticos en su Código penal son; Aguascalientes, Baja California, Chiapas, Colima, Distrito Federal, Morelos, Oaxaca, Puebla, Sinaloa, Querétaro, Tabasco, Tamaulipas, Zacatecas y en el federal. Y los cuales donde no se hace referencia alguna a los mismos en sus códigos estatales son; Baja California Sur, Campeche, Chihuahua, Coahuila, Durango, Estado de México, Guanajuato, Guerrero, Hidalgo, Jalisco, Michoacán, Nayarit, Nuevo León, Quintana Roo, San Luis Potosí, Sonora, Tlaxcala, Veracruz Llave, Yucatán.
Además, existen Códigos punitivos que no mencionan conductas relacionadas a instrumentos informáticos como medios en la comisión de delitos; como los de los estados de Campeche y Nayarit. En: GUERRA. Ob. Cit. pp. 39-80.

altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red"[312].

Es de suma relevancia destacar que Sinaloa no sólo fue el primer estado en tipificar los ciberdelitos, sino que también es el único estado en denominar esta clase de ilícitos como "delitos informáticos"[313].

Ya en 1999, se incorpora al Código Penal Federal un capítulo denominado "Acceso ilícito a sistemas y equipos de informática", en el cual se agregan una serie de artículos –del 211 bis 1 al 211 bis 7- que tratan sobre el delito de sabotaje informático, consistente en la modificación, destrucción o provocación de pérdida, o la copia o acceso ilegítimo, "sin autorización, de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad"[314]. Con esto, se perfeccionó considerablemente el tratamiento de los delitos informáticos en

[312] NAVA. Ob. Cit.pp. 76-78.
[313] PIÑA L., H. Los delitos informáticos previstos y sancionados en el Ordenamiento Jurídico Mexicano. [en línea] <http://www.ordenjuridico.gob.mx/Congreso/2doCongresoNac/pdf/PinaLibien.pdf> p.13.
[314] ABOSO y ZAPATA. . Ob. Cit. pp. 201 -202.

México, haciendo de aquel nuevo desafío un tema país, el cual debía afrontarse legislativamente a nivel nacional y ya no ser una tarea dejada sólo a los pocos estados interesados.

Otro de los ordenamientos importantes donde se protegen ciertos bienes jurídicos frente a la informática es la Ley Federal contra la Delincuencia Organizada (LFDO), en la cual se establece la existencia de una unidad especializada de la Procuraduría General de la República para la investigación y persecución de delitos que se organizan a través de la red.

Consecuentemente, debido a la realidad mexicana en relación al trato –bastante disperso- de los delitos informáticos, y a la dificultad probatoria que existe alrededor de los mismos, en este país se ha creado la "Coordinación Interinstitucional de combate a Delitos Cibernéticos"[315], institución que se encarga de controlar el uso y contenidos ilícitos en Internet, y la organización de delitos en la red, todo a través del monitoreo

[315] Esta institución está formada por; la Presidencia de la República, la Procuraduría General de la República, la Procuraduría General de Justicia del Distrito Federal, la Policía Penal Preventiva, el Centro de Investigación y Seguridad Nacional, la Secretaría de la Defensa Nacional, la Secretaría de Marina, la Secretaría de Seguridad Pública, entre otros.

de una Base de Datos Nacional en la que se observarán patrones, preferencias y modus operandi de las causas reportadas[316].

Vistas las medidas legales e institucionales tomadas por México para contrarrestar la comisión de delitos que se auxilien de las nuevas tecnologías, debemos comentar que sería necesario el despliegue de una política común respecto a los ciberdelitos, ya que el caos que se genera con la variedad de leyes que permite el régimen federal y la falta de uniformidad en el tratamiento de los e-crimes a nivel local permite que en la actualidad se aprovechen estas lagunas legislativas para incrementar la impunidad en el contexto de la delincuencia informática.

[316] NAVA. Ob. Cit. pp. 84-85.

<u>CAPÍTULO IV:</u> USURPACIÓN DE IDENTIDAD EN LAS REDES SOCIALES: TRATAMIENTO LEGAL EN CHILE Y EN EL DERECHO COMPARADO.

Como mencionamos anteriormente, el desarrollo tecnológico ha significado la necesidad de adaptarse a los nuevos tiempos a través de nuevas formas de comunicación, las cuales permiten tener absoluta libertad en la construcción del propio usuario, surgiendo con esto la incertidumbre de si la persona que se encuentra al otro lado de la pantalla es realmente quién dice ser y no otra.

En virtud de la autonomía que existe para crear un sinfín de perfiles en Internet, y más específicamente en las redes sociales, y de hacerlo en la forma que se estime conveniente, podemos clasificar las cuentas en dos categorías: aquellas que son legítimas, por ser reflejo de la persona que las administra o bien, aunque no representando fielmente a la misma cumplen con las políticas del sitio web en la que se erigen, y otras ilegítimas que se

crean con la finalidad de hacerse pasar por otra persona, pudiendo causarle algún daño a esta última, lo que sin lugar a dudas es una conducta indebida, que puede traer consecuencias jurídicas.

Es respecto de las cuentas que se crean para usurpar la identidad de otro, que cabe analizar una serie de cuestiones fundamentales, como la figura penal clásica de suplantación de identidad, por el hecho de que tal conducta sólo es sancionada en el ámbito físico de los individuos; la estructura que debe detentar este delito cuando se dé en el contexto de Internet y las redes sociales; y el Proyecto de Ley presentado en 2014 que persigue sancionar la usurpación de identidad en Internet, entre otras.

1. La usurpación de identidad como tipo penal

El delito de usurpación de identidad en Chile no ha tenido el reconocimiento que merece, encontrándose escasamente regulado en

nuestra legislación penal y no siendo desarrollado en absoluto por parte de la doctrina[317].

En el Código Penal, la suplantación de identidad está regulada en el artículo 214[318], que establece lo siguiente:

> Art. 214. El que usurpare el nombre de otro será castigado con presidio menor en su grado mínimo, sin perjuicio de la pena que pudiere corresponderle a consecuencia del daño que en su fama o intereses ocasionare a la persona cuyo nombre ha usurpado.

[317] Habiendo revisado los principales manuales de Derecho Penal, como son "Lecciones de Derecho Penal chileno, Parte Especial" del profesor Sergio Politoff y "Derecho Penal, Tomo III" del profesor Alfredo Etcheberry, no fue posible encontrar un tratamiento al respecto.

[318] Este precepto ha mantenido su redacción original desde el proyecto del Código Penal, presentándose bajo el artículo 216, el que al momento de la publicación del cuerpo normativo pasó a ocupar el artículo 215. Y que posteriormente, con la Ley 17.155, tomó el lugar del artículo 214 que conocemos en la actualidad. Cabe destacar que desde su inclusión en el Código, esta norma no ha sido discutida ni objetada en el Congreso, así consta en las actas de redacción del Código original de 1874, en las actas Parlamentarias donde se discute la promulgación del mismo, y en la modificación de éste mediante la Ley 17.155.

De la norma podemos establecer que para que exista suplantación de identidad basta que haya utilización por parte de un sujeto del nombre de otra persona sin consentimiento de ésta última, independiente de la comisión de otras conductas que también se consideren delictivas y sean consecuencia de este ilícito primigenio.

Estimamos que el término "el que usurpare el nombre de otro" no puede tomarse de manera literal, puesto que debe entenderse más ampliamente abarcando cualquiera de los elementos que conforman la identidad de la persona, ya sea sólo el nombre, la imagen, la firma, etc., o bien una suma de todos o algunos de ellos[319]. Tratándose entonces de una personificación, la

[319] El Informe realizado por la Biblioteca del Congreso Nacional establece que el artículo 214 del Código Penal sólo abarca la usurpación que se haga del nombre propio de otra persona para configurar el tipo penal aunque no se haga pasar por aquella, siendo el objeto sobre el cual recae el delito el mero nombre y no la identidad. Esto, porque "el "nombre" es mucho más concreto y definido que "identidad" (…) Por un lado, ello hace que la figura penal sea un poco más débil, al cubrir menos casos, pero al mismo tiempo la hace más segura, pues de lo contrario podría cubrir hipótesis demasiado difusas". A pesar de la restricción que se hace de la norma, a nuestro criterio ésta, a falta de otra más amplia o completa, debe comprender la hipótesis de la suplantación de identidad en uno o más de sus elementos, ya que dentro de nuestra legislación penal es el único remedio que existe para proteger las víctimas de este delito. En: BIBLIOTECA CONGRESO NACIONAL. 2012. Informe sobre Delitos por Internet:

que se lleva a cabo no sólo con el uso del nombre ajeno, sino que teniendo la intención de actuar en nombre de otro, apropiándose de tal identidad como si fuese la suya.

También cabe destacar que de la simple lectura del artículo se deduce que la usurpación de identidad se configura con la mera acción de suplantación, independiente del daño que se provoque con ésta a la víctima, ya que el delito se sanciona sin perjuicio de las consecuencias en la fama o intereses que se le ocasionare a la persona cuyo nombre se ha usurpado.

De esta idea podemos establecer que la usurpación de identidad puede conformarse por dos fases, una primera donde existe una utilización de la identidad de otro y que siempre está presente, puesto que el ilícito se configura con la acción de suplantación, y una segunda etapa que está relacionada con el daño que es consecuencia de otros delitos conexos que se hacen valer de la usurpación de identidad para su comisión. Dicho en otras palabras, basta la fase primitiva de suplantación para que se dé el delito,

---

Legislación Nacional elaborado por Juan Pablo Cavada Herrera, Asesor Técnico Parlamentario. Chile. 9p.

habiendo o no daño para la víctima –el cual puede ser de diversa índole-, mientras que la segunda fase es independiente y eventual respecto de la primera, puesto que existirá cuando el ilícito primigenio se utilice para la ejecución de otros delitos –como los de injuria, calumnia, estafa, entre otros- los que generen otro tipo de daño o uno más intenso.

En relación a este punto, y de acuerdo a lo planteado por el precepto, se entiende que de cometerse una usurpación de identidad y otros delitos que atenten contra la fama o intereses de la víctima y que estén conectados con el primero, habrá un concurso ideal de ilícitos, puesto que el sujeto activo se habrá servido de la suplantación para la comisión de los segundos.

1.1. Elementos para su configuración

Para un estudio acabado del injusto de usurpación de identidad cabe revisar los elementos que sirven a su configuración.

- Sujeto pasivo: La suplantación de identidad en su faceta clásica puede sólo afectar a las personas naturales, puesto que son estas las que

detentan una identidad propia y determinada, susceptible de apoderamiento por terceros en cualquiera de los elementos que la representan y conforman.

- Sujeto activo: Hacerse pasar por otro es una práctica que sólo pueden llevar a cabo las personas naturales, puesto que únicamente aquellas capaces de intervenir en la comisión del ilícito y ser responsables ante la ley penal. Además, es menester mencionar que no es requisito tener una calidad especial para ser sujeto activo, como detentar el cargo de funcionario público.

- Acción u omisión: La figura penal clásica de suplantación de identidad establece que se sancionará a aquel que usurpare el nombre de otro, sólo siendo procedente la acción –por tanto excluyéndose la usurpación por omisión- de apropiarse de cualquiera de los elementos de configuran la identidad de una persona.

En cuanto a la calidad de este delito, debemos preguntarnos si constituye un ilícito de carácter instantáneo o permanente. Por un lado, si la suplantación se consuma "en un solo instante, esto es, si el proceso de

ejecución que culmina al completarse todas las exigencias del tipo delictivo se cierra en un momento determinado y único, nos encontramos en presencia de un delito instantáneo"[320]. Como en el caso en que un individuo entregue una cédula de identidad de otra persona a la policía cuando esta ejecuta un control de identidad.

Por otro lado, estimamos que también es posible que exista una suplantación de nombre de carácter permanente, cuando "el momento consumativo perdura en el tiempo"[321] [322], como en todos aquellos casos en que una persona adopta la personalidad de otro y realiza diferentes actos en su nombre sin la autorización por parte de este último.

[320] NOVOA M., E. Curso de Derecho Penal Chileno. Editorial Jurídica de Chile, 1960, Págs. 259 a 261. En: CORTE SUPREMA DE CHILE. 11 de octubre de 2007. Rol N° 2.370-07.

[321] Ídem.

[322] A este respecto, según el profesor Novoa "la característica diferencial entre los delitos instantáneos y permanentes está en que los primeros quedan terminados cuando alcanzan la plenitud de los requisitos propios de la consumación, al paso que los segundos inician en ese momento una duración en el tiempo más o menos prolongada, en la cual la violación jurídica subsiste por la voluntad del sujeto activo". En: Ídem.

Es importante señalar que gracias a la usurpación de identidad el sujeto activo puede cometer un amplio abanico de conductas antijurídicas con la información personal de otro ilegalmente obtenida –siendo todos delitos diferentes pero conexos, en virtud de que se hacen valer de la suplantación de identidad para ejecutarse-, las que pueden provocar un gran espectro de daños a la víctima.

- Culpa o dolo: En cuanto al elemento subjetivo que debe presentarse en el ilícito en cuestión, el artículo 214 no establece si usurpar el nombre de otro requiere de una intensión específica por parte del perpetrador. A pesar de esta omisión en la norma y siguiendo lo planteado en la doctrina comparada creemos que únicamente es admisible el dolo directo en este injusto, en cuanto "la acción típica, «usurpar» supone necesariamente el uso de la identidad usurpada lo que sólo puede realizarse haciéndose pasar por otro"[323], con la intención de hacer uso de los derechos y acciones del suplantado.

[323] FARALDO C., P. 2010. Suplantación de identidad y uso de nombre supuesto en el comercio tradicional y electrónico. [en línea] Revista de Derecho Penal y Criminología. 3° Época, n°3. pp.73-134. <http://e-

- Daño: El precepto penal examinado estipula que la suplantación de identidad se configurará por el sólo hecho de "usurpar", lo que se traduce en el que la acción delictiva se sancionará independiente de que sufra daño o no el sujeto pasivo. Incluso, el afectado podrá demandar separadamente por el perjuicio que se le produzca en su fama o intereses cuando éste sea consecuencia de otros delitos cometidos por el delincuente aprovechándose de la usurpación de identidad ya ejecutada.

Podemos encontrar que en la relación que existe entre el delito de usurpación de identidad y el daño producido por éste, existen dos escenarios diametralmente opuestos. En un primer caso, puede ocurrir que la suplantación sea penada aun cuando no produzca ningún daño o cuando éste sea mínimo, mientras que en un segundo caso, la ejecución de la usurpación puede conllevar un perjuicio inmensurable a la víctima, ya sea porque la mera suplantación le afecta en su ámbito más personal, o bien, porque en virtud de delitos conexos a la misma se le provoca un daño en su

---

spacio.uned.es/fez/eserv/bibliuned:revistaDerechoPenalyCriminologia-2010-3-5030/Documento.pdf> p.87

honor o su patrimonio que exceden la magnitud del daño que se produciría sólo con el delito originario.

1.2. Bien jurídico protegido

El artículo 214 del Código Penal al decir "el que usurpare el nombre de otro" alude, a nuestro parecer, al derecho al nombre, el cual como mencionamos anteriormente, es un derecho inherente a la persona y de carácter extrapatrimonial que protege al individuo en su esfera social y la esencia de su personalidad.

Según lo planteado en el Capítulo I, el derecho al nombre se instituye en la identidad, por ser el primero elemento y expresión de la segunda –debemos recordar que el nombre completo forma un todo unitario con un valor identificatorio y jurídico que permite nuestra individualización en los distintos aspectos de la vida-, por lo que estimamos que el bien jurídico

protegido por el tipo penal en cuestión es el derecho a la identidad personal, que tiene por fundamento la "verdad de la persona"[324].

Asimismo, en palabras de Garrido Montt la norma protege "la vida en relación, pues en el tráfico jurídico la ocultación de la propia identidad mediante el empleo de un nombre que no corresponde al real, puede provocar serias confusiones en la sociedad"[325].

Por consiguiente, lo que persigue resguardar la norma es la autenticidad de los sujetos y el aspecto de la personalidad que se proyecta en la vida en sociedad, el que se manifiesta en los diferentes elementos identificativos de la misma –como por ejemplo el nombre o la imagen- los que nos individualizan como seres únicos e irrepetibles.

---

[324] Véase N° 1.3.2. Derecho a la Identidad personal del Capítulo I.

[325] GARRIDO M., M. 2005. Derecho Penal, Tomo IV, Parte Especial. Editorial Jurídica. Santiago, Chile. p.137. En: MUÑOZ L., F. 2013. ¿Es punible la parodia a través de Twitter? [en línea] Revista chilena de Derecho y Tecnología. Centro de estudios en Derecho Informático. Universidad de Chile. Vol.2. Núm. 1 (2013). p. 157-158. <http://www.revistas.uchile.cl/index.php/RCHDT/article/viewFile/27015/28938> [consulta: 4 de febrero de 2015]

2. La usurpación de identidad en las redes sociales

Teniendo en cuenta que la regulación del delito de usurpación de identidad en el artículo 214 del Código punitivo chileno sólo contempla la suplantación que se produce en el mundo físico entre personas naturales, actualmente dicho ilícito ha encontrado en las redes sociales un espacio novedoso para perpetrarse.

Tal nicho ha ayudado a la expansión de los límites en que puede darse una suplantación de identidad, en virtud del mundo sin barreras que es Internet, lo cual genera nuevos desafíos a la hora de proteger a la persona en su esfera más íntima, puesto que los frentes de ataques se multiplican infinitamente en este medio.

En consideración al inexistente tratamiento legal y doctrinario en nuestro país de este injusto en un contexto virtual, pasaremos a analizar el posible tipo penal que abarcaría tal conducta indebida siguiendo la estructura desarrollada en base a la figura clásica de la usurpación de identidad.

2.1. Elementos para su configuración

- Sujeto pasivo: Al igual que en el tipo penal clásico, cualquier persona natural podría ser víctima de una suplantación en todos o algunos de los elementos que conforman su propia identidad. Sin embargo, en el contexto de Internet y las redes sociales, estimamos que las personas jurídicas también podrían verse afectadas por este tipo de ilícito, puesto que el o los delincuentes podrían tomar control de las cuentas que tengan aquellas en los distintos sitios web que utilicen para darse a conocer al público, actuando en nombre de las mismas, y pudiendo causarles un daño en la identidad que tienen como marca.

- Sujeto activo: En principio se tiende a pensar que el sujeto activo -ya sea autor, cómplice o encubridor- sería el individuo que posee vastos conocimientos en materia informática, porque es requerimiento esencial para la ejecución del mismo delito la utilización de los medios telemáticos, no obstante, con las facilidades que proporcionan las nuevas Tecnologías de la Información y Comunicación ya no sería necesario ser experto en esta área para cometer ciberdelitos, y cualquier persona con acceso a un

computador e Internet podría convertirse en sujeto activo del ilícito de suplantación de identidad en las redes sociales[326].

- Acción u omisión: La usurpación de identidad en el contexto de las plataformas virtuales coincidiría en este aspecto con la figura penal clásica, sólo procediendo la acción de usurpar. En las redes sociales, la idea de una suplantación de identidad a través de la apropiación de cualquiera de los elementos que conforman a ésta se hace más patente, puesto que el perpetrador podría realizar actos en Internet utilizando –sin el consentimiento respectivo- no sólo el nombre de otro, sino también adoptando su imagen completa a través de sus fotografías como si fueran propias.

Compartiendo en parte lo expuesto por Romero Flores y Téllez Valdes[327], estimamos que la acción de usurpar la identidad digital estaría

[326] Así lo corrobora el Comisario Santiago David, de la Brigada del Cibercrimen de la Policía de Investigaciones en la entrevista que se adjunta en el punto III del anexo.

[327] Estos autores plantean que en el tipo penal de suplantación de identidad que existe en la legislación mexicana se distinguen tres elementos básico: a) la apropiación de datos personales por medios convencionales o

conformada por dos elementos: la apropiación de datos personales por medios convencionales o informáticos, obtenidos ya sea legal o ilegalmente[328], y "la facultad arrogada de manera ilícita para utilizar los datos personales con fines de suplantación de identidad, es decir, las calidades atributivas y relacionales con el ente de imputación jurídica, son derivadas a un nuevo ente para producir actos o consecuencias legales para ser atribuidas al ente jurídico original sobre del cual se obtuvieron datos personales"[329].

---

informáticos (inclusive telemáticos); b) la transferencia o sesión de los datos personales; y c) la facultad arrogada de manera indebida para utilizar dichos datos personales con fines de suplantación de identidad. En: ROMERO, F. R. y TÉLLEZ, V. J. 2011. La usurpación o suplantación de identidad: una aproximación conceptual y los posibles elementos constitutivos del tipo penal. p.149-170. En: ROMERO L., L. 2011. Jus informa TIC's. 1ª ed. México. 202p.

[328] Se entiende que la información sensible obtenida por medios legales alude al escenario en que el sujeto pasivo entrega voluntariamente sus datos, aunque sea de forma inconsciente, mientras que apropiación ilegítima de la información se dará cuando el sujeto activo la recaude a través de tácticas indebidas. Además es posible que la obtención ilegal de datos se dé mediante transferencia o sesión de información personal que ya fue adquirida de manera ilícita, ya que es innegable que dentro del tráfico informacional que existe en Internet, la comercialización previa de bases de datos automatizadas de personas físicas o jurídicas es recurrente.

[329] ROMERO L., L. 2011. Op. Cit. p. 150.

Otro punto a examinar en relación a la acción de usurpar la identidad es el carácter instantáneo o permanente del ilícito. En este caso, la suplantación se configuraría como un injusto continuado, en cuanto la apropiación de el o los elementos de la identidad de la otra persona se utilizan para abrir y mantener una cuenta en las redes sociales, perpetuando a través del tiempo la conducta delictiva.

Al igual que en la suplantación de identidad tradicional, aquella que se desenvuelve en la Red podría conllevar a la comisión de otros tantos y diversos delitos, por aprovecharse estos de la información sensible de la víctima. La diferencia con el injusto que se da en el mundo físico es que en Internet los límites de tiempo y espacio son difusos, y por tanto, las facilidades de ejecución de este ciberdelito son mayores, lo que aumenta considerablemente –incluso a un nivel inmensurable- el espectro de delitos que el sujeto activo podría cometer.

- Culpa o dolo: La faz subjetiva del delito en estudio, al igual que en su esfera clásica se satisfaría sólo con dolo directo, puesto que el sujeto activo debe estar dotado de un ánimo de apropiación de la identidad ajena, toda

vez que actuará en nombre de la víctima gozando de sus derechos e imputando las consecuencias de las acciones que realiza en el sujeto pasivo.

- Daño: Así como la modalidad tradicional de suplantación de identidad, aquella que se da en el contexto de las redes sociales, tampoco requeriría que la víctima sufra un perjuicio para que el delito de configure, bastando el hecho de la usurpación para ello. Esto, porque lo que buscaría proteger el posible tipo penal sería lo mismo que el artículo 214: la identidad.

De la misma manera, es posible este delito constituya la base para la ejecución de otros tantos ilícitos que podrían provocar innumerables daños, los que en el plano de las redes sociales tienden a multiplicarse más fácil y rápidamente por las condiciones que otorga la Red. La reparación de los perjuicios que nacen de los delitos conexos podrá exigirse de forma separada por la víctima de ellos.

2.2. Bien jurídico protegido

El bien jurídico a proteger por la potencial figura de usurpación de identidad en Internet y las redes sociales en principio debiera ser el mismo que se ampara bajo el artículo 214, siendo éste la identidad personal, la cual como mencionamos anteriormente, es aquella que se manifiesta a través de diferentes elementos identificatorios, como el nombre, la imagen, la firma, u otros.

Es necesario establecer que el delito de suplantación de identidad digital constituye el mismo ilícito de la esfera clásica, la diferencia radica en el medio de comisión -que es la Red-, por lo cual la protección debiera apuntar al mismo objetivo, que es el resguardo a la "verdad personal" y la "vida en relación".

El hecho de que la usurpación de identidad se dé en un plano virtual amplía el concepto que tenemos de identidad –por esto se agrega el adjetivo virtual o digital-, la cual abarca tanto los elementos convencionales de la misma como los "datos personales sensibles que pueden incluir claves de acceso a cuentas bancarias o redes mediante las cuales las personas se comunican u operan en redes informáticas o telemáticas y cuya circulación

transfronteriza es potencialmente peligrosa ante su posible apropiamiento no autorizado"[330]. Todo lo anterior, porque "la identidad digital que una persona desarrolla a través de Internet forma también parte de ese todo único e inseparable que es su identidad personal"[331].

2.3. Usurpación de identidad como ilícito civil extracontractual.

2.3.1. Derechos de la personalidad como objeto de protección civil

Los derechos de la personalidad son objeto de protección por parte del Derecho civil. Siguiendo a Barros, podemos afirmar que dicha protección se fundamenta en la dignidad de la persona, a quien se le reconoce un derecho a desarrollar libremente su personalidad y un espacio privado de acción exento de turbaciones externas. Resulta evidente que este orden de ideas es análogo a lo que se ha sostenido a lo largo de esta investigación en relación a la identidad de la persona, en el sentido de que el desenvolvimiento en un

[330] Ibídem. p.151 y 152.
[331] BORGHELLO, C. y TEMPERINI, M. Suplantación de Identidad Digital como delito informático en Argentina. [en línea] Simposio Argentino de Informática y Derecho. 16p. <http://www.elderechoinformatico.com/publicaciones/mtemperini/JAIIO_DI_Identidad_Camera%20Ready.pdf> [consulta: 14 de marzo de 2015] p.10

espacio autónomo, de manera sostenida, permite el desarrollo de la personalidad y configura lo que entendemos por aquélla.

El derecho a la honra y el derecho a la privacidad son especies de derechos de la personalidad. Como bien anota Barros, éstos pueden ser descompuestos en diversos intereses protegidos por el derecho civil y cuyos límites son precisados mediante la definición progresiva de ilícitos civiles de mayor especificidad[332]. Lo anterior cobra mayor relevancia cuando se considera que los derechos referidos se consagran a nivel constitucional; luego, el contenido axiológico de las normas constitucionales permea indefectiblemente en la legislación civil que debe ser interpretada a la luz de la Carta Fundamental.

El derecho a la honra y el derecho a la privacidad tienen notas distintivas. Como se señaló anteriormente, "la honra se muestra en la consideración de los demás, de la que depende la validación social del

[332] BARROS., E. 2007. Tratado de Responsabilidad Extracontractual. Editorial Jurídica de Chile, Santiago, Chile. p. 539

titular"[333], o en otras palabras, la infracción a la honra se caracteriza por ser una consecuencia de una imputación falsa, esto es, de un hecho falso que influye en la opinión que los demás tienen del individuo.

Por su parte, la privacidad se configura como un derecho de exclusión, donde el titular define qué aspectos de su vida revela ante la sociedad, atendiendo a los distintos tipos y grados de relaciones intersubjetivas y a los contextos en que éstas se verifican. Así, el actor asume una posición de control respecto de la información personal que revela ante terceros. En este orden de ideas, la infracción a la privacidad se caracteriza por una transgresión a los límites fijados por el titular[334]. Como se aprecia, las acciones concretas que conllevan una infracción a la honra y a la privacidad, respectivamente, son esencialmente distintas.

La privacidad presenta una serie de intereses que el derecho civil cautela distintamente atendiendo a sus particularidades. En lo que respecta al objeto de esta investigación, nos referimos al derecho moral, por un lado, y al

[333] Ibídem. p. 540
[334] Ibídem. p.541 y 542

patrimonial, por otro, derivados de los aspectos externos de la personalidad que Barros identifica como la imagen, la voz y el nombre.

En cuanto al derecho moral, podemos señalar que éste se traduce en la prohibición de actuar sin autorización sobre dichos aspectos externos, configurándose como una potestad de excluir a otros de un cierto ámbito personal. Y sobre el derecho patrimonial, podemos decir que los aspectos externos de la personalidad supone, en cambio, la prohibición de apropiación por un tercero de la imagen, la voz y el nombre, asegurando su goce económico exclusivo al titular, lo que es conexo a la exclusividad que otorga el derecho moral[335].

2.3.2. Acciones civiles que protegen los derechos de la personalidad

En materia de protección de los derechos a la honra y a la privacidad, se presenta una tipología de acciones que distingue entre: (1) acciones preventivas e interruptivas del daño eventual o del daño que se está produciendo actualmente y; (2) acciones correctivas del daño ya producido.

[335] Ibídem. p. 543 y 564

Estas últimas se clasifican en: (2.1) acciones dirigidas a la restitución en naturaleza del mal causado y; (2.2) acciones dirigidas a obtener indemnización de perjuicios.

La relevancia de la distinción radica en que, en esta materia, existe una primacía a las acciones dirigidas a la restitución en naturaleza por sobre la indemnización en dinero[336], lo que deriva de los distintos fundamentos de las acciones correctivas. Si bien ambos tipos de acciones disciplinarias suponen la ilicitud de la conducta del demandado -esto es, que ocasiona un daño antijurídico-, la diferencia radica en que las acciones de reparación en naturaleza surgen de un deber jurídico motivado en el error del demandado, el deber restitutorio, y no de un juicio de culpabilidad. Así, la acción de reparación en naturaleza busca restablecer moralmente a la víctima del error que ha causado un daño antijurídico sin entrar en consideraciones sobre la imputabilidad de tal perjuicio. Por lo tanto, en materia de acciones de reparación en naturaleza no cabe hablar de un juicio de responsabilidad civil extracontractual, sino de un deber de restitución basado en obtener el restablecimiento moral de la víctima. Resulta, en consecuencia, que los

[336] Ibídem. p.592 a 594

requisitos de procedencia de las acciones de reparación en naturaleza son menos estrictos que los de las acciones indemnizatorias, puesto que en las primeras basta la verificación del daño antijurídico, mientras que en las segundas se requiere, además, realizar un juicio de culpabilidad.

Esta diferencia en los fundamentos que motivan ambos tipos de acciones correctivas y que se traduce en diversos niveles de exigencia en los requisitos de procedencia, deriva entonces, en una primacía de las acciones de restitución en naturaleza. Sin embargo, cabe precisar que ello sólo será posible en la medida en que la restitución en naturaleza sea el remedio adecuado y exigible[337]. Por tanto, será adecuado cuando las acciones correctivas de restitución (réplica, corrección, retractación o publicación de la sentencia) sean aptas para eliminar o disminuir el daño causado; y, será exigible cuando resulte que de las circunstancias que la víctima debe aceptar, al menos una parte del menoscabo sea reparado por esta vía.

En síntesis, el principio rector en este punto se traduce en obtener la más completa reparación en naturaleza que resulte posible, quedando la

[337] BARROS. Ibídem. p.597

indemnización en dinero relegada a cubrir sólo el perjuicio remanente. Incluso en este último evento, la indemnización estará condicionada a que se cumplan las exigencias propias del juicio de responsabilidad, principalmente, el juicio de imputabilidad.

En lo que respecta a las acciones derivadas de una usurpación de nombre, en los términos expuestos en esta memoria, resulta que el principio de la mayor reparación en naturaleza posible se ve atenuado. En efecto, y como ya se señaló, las acciones correctivas de restitución suponen cierta aptitud como remedios para la reparación del daño causado (deben ser el remedio adecuado y exigible), cuestión que en la especie no se verifica.

Estimamos, pues, que el perjuicio derivado de una usurpación de nombre no se ve eliminado ni disminuido por el ejercicio de este tipo de acciones, por cuanto sus diversas especies no resultan adecuadas para este fin. Por lo tanto, no queda sino impetrar las acciones correctivas indemnizatorias, siempre y cuando se cumplan los requisitos de procedencia.

2.3.3. Acción indemnizatoria en sede extracontractual

Habiendo señalado que en la materia objeto de esta investigación no resulta, en nuestra opinión, procedente la reparación en naturaleza, la totalidad del daño causado deberá ser objeto de una indemnización en dinero. En este punto tiene plena aplicación los criterios de reparación integral del daño que rige en materia civil extracontractual (según el artículo 2.329 del Código Civil), abarcando pues el daño patrimonial y el daño moral.

2.3.3.1. Supuestos de la responsabilidad extracontractual

Toda acción que persiga la responsabilidad extracontractual de un individuo debe contener cuatro requisitos: (1) la existencia de un hecho voluntario; (2) imputabilidad; (3) daño; y, (4) un nexo causal entre el hecho imputable y el daño a la víctima, en virtud de que "cada cual soporta sus propios daños, a menos de que haya una razón para atribuírselo a un tercero"[338].

[338] Ibídem. p.61

El primer elemento es que exista un hecho imputable, puesto que la condición general es que tanto la acción como la omisión debe nacer de un hecho voluntario, de un actuar libre del sujeto, puesto que de otra manera no habría responsabilidad propiamente tal.

El segundo elemento es la exigencia de la imputabilidad a culpa o dolo, conceptos muy diferentes entre sí que pasaremos a exponer:

La culpa en materia extracontractual es un criterio general de responsabilidad relacionado con la "inobservancia del cuidado debido en la conducta susceptible de causar daño a otros"[339], siguiendo por tanto un modelo de conducta, alejándose de características individuales y subjetivas de cada persona, respondiendo a un criterio jurídico y no a un reproche moral.

El estándar de culpa en el área extracontractual se ha relacionado con la culpa leve, puesto que se entiende que está constituida sobre la base de las

[339] Ibídem. p.78

expectativas recíprocas de comportamiento[340] y la diligencia se relaciona con "la virtud de la prudencia, que a su vez, exige un juicio sereno y razonablemente informado de las circunstancias de la acción"[341]. De esta manera, se ha dicho que el juicio de culpabilidad es abstracto y normativo, pero se materializa a través de una apreciación en concreto que atiende a las circunstancias de hecho[342].

Por otro lado, y siguiendo al profesor Barros, el dolo en materia extracontractual se ha definido como "la utilización voluntaria del otro para los propios propósitos"[343], comprendiendo tanto la intensión de dañar a otro como la aceptación voluntaria del injusto estando consciente de la ilicitud de la acción[344].

Cabe hacer una mención especial al análisis del delito de usurpación de identidad en el ámbito del elemento de imputabilidad, puesto que podemos notar ciertas diferencias relevantes que existen respecto de este elemento en

[340] Ibídem. p.82
[341] Ibídem. p.82
[342] Ibídem. p.86
[343] Ibídem. p.159
[344] Ibídem. p.159

materia penal y en materia civil extracontractual. En el primer caso, es evidente que en la imputabilidad juega un rol importante el hecho de que un delito haya sido cometido de forma dolosa o culposa, puesto que la imputación es personal, es decir, que "el sujeto actúa culpablemente cuando ha incurrido en un injusto jurídico penal, a pesar de que en la situación concreta (todavía) podría satisfacer el efecto invocativo de la norma y poseía una suficiente capacidad de autodeterminación, de modo que un comportamiento conforme a la norma le era psicológicamente accesible"[345]. Mientras que por el contrario, en el derecho civil extracontractual no encontramos diferencias al decir que el responsable ha actuado con culpa o dolo y afirmar que la conducta es ilícita, porque la apreciación es impersonal[346] y por tanto, los efectos que producen el actuar de una u otra forma son disímiles.

El tercer elemento es la existencia de un daño por parte de la víctima, el cual resulta ser una condición indispensable bajo cualquier régimen de responsabilidad civil.

[345] ROXIN., Claus. 1997. Derecho Penal Parte General. Fundamentos. La estructura de la teoría del delito. Editorial Civitas. Madrid. p.729
[346] BARROS. Op. Cit. p.84

En cuanto al daño patrimonial derivado de transgresiones al derecho de privacidad en sus aspectos externos -imagen, voz y nombre, entre otros-, la doctrina advierte que la apropiación no autorizada puede dar lugar a daños patrimoniales, principalmente por concepto de lucro cesante, aunque ello no obsta, ciertamente, a que se verifiquen daños emergentes. La apreciación del daño patrimonial puede hacerse tanto en concreto como en abstracto. Por ejemplo, ofertas concretas que el titular tenía para el uso comercial de su nombre, por un lado, y consideraciones sobre cuáles habrían sido los precios de un eventual contrato por este concepto, por el otro[347].

Por último, cabe tomar una postura respecto de la extensión de la reparación del daño moral en este punto. Si bien es cierto que el artículo 2.331 del Código Civil limita la reparación del daño moral cuando se verifiquen atentados contra el honor o reputación de otra persona, la doctrina más autorizada ha señalado que para efectos prácticos dicha limitación no es procedente, toda vez que existe sólida jurisprudencia que ha declarado inaplicable dicho artículo por contravenir lo dispuesto en la

[347] Ibídem. p. 600 y 601

Constitución. La postura mayoritaria, y en nuestra opinión correcta, se inclina por la reparación íntegra del daño, abarcando incluso el daño moral en concordancia con lo dispuesto en el artículo 2.329 del cuerpo legal[348]. Cabe señalar, sin embargo, que la inaplicabilidad por inconstitucionalidad debe ser alegada ante el Tribunal Constitucional de conformidad a lo dispuesto en el artículo 93 N°6 de la Constitución Política de la República, quedando vedada dicho juicio a los jueces civiles.

Siendo procedente la indemnización del daño moral, cabe tener presente que éste se valora en concreto y en observancia del principio de equitativa compensación[349]. Por tanto, resultan relevantes las circunstancias concretas que se verifican en la especie, por ejemplo, las características propias el demandante, su conducta anterior (puesto que de ella dependen los límites impuestos en su relación con otros), las circunstancias en que se verifica la transgresión o conducta ilícita, así como todo otro antecedente concreto que sirva para comprender la extensión del daño ocasionado[350]. En el caso particular de la usurpación de nombre, el afectado puede basar el daño

[348] Ibídem. p. 544 y 603.
[349] Ibídem. p. 311
[350] Ibídem. p.604

moral sufrido en la vulneración del "derecho a la identidad personal" y a "la vida en relación", por cuanto delimita el perjuicio que la confusión en su persona le ocasionado en la sociedad.

Finalmente, el cuarto elemento es la relación de causalidad entre el hecho imputable y el daño causado, puesto que en materia civil, sólo se responde por daños y no por conductas reprochables que no se materializan en perjuicios a un tercero. De esta manera, la causalidad actúa como fundamento de la responsabilidad, ya que se responde por los daños que se ha causado con la conducta; y por otro lado como limitación de ella, porque no se responde de todo daño, sino que se restringe a aquellos perjuicios que en virtud del juicio normativo son atribuibles al hecho[351].

2.3.3.2. Acción por culpa infraccional y acción de responsabilidad extracontractual por culpa

Teniendo claros los elementos necesarios para la configuración de la responsabilidad extracontractual, cabe examinar los distintos supuestos que se pueden dar en el caso del delito de usurpación de identidad. Una primera

[351] Ibídem. p.374

situación es aquella que se origina por la persecución civil por culpa infraccional derivada de una sentencia penal condenatoria por el delito en comento, mientas que la segunda es la de obtener una indemnización de perjuicios por vía de responsabilidad extracontractual de forma autónoma.

En la primera hipótesis nos encontramos ante la existencia de una sentencia condenatoria en contra de quien ha usurpado el nombre de otro, y por tanto, ha infringido un deber de cuidado establecido por el legislador[352] establecido en el artículo 214 del Código Penal.

En virtud de lo establecido en el artículo 178 del Código de Procedimiento Civil, que señala:

"en los juicios civiles podrán hacerse valer las sentencias dictadas en un proceso criminal siempre que condenen al procesado",

Se ha entendido que en la responsabilidad civil extracontractual, el acto es tenido por ilícito, puesto que "la declaración de ilegalidad de una

[352]Ibídem. p.98

conducta lleva implícita la declaración de que dicha actuación ha sido culpable, porque lo ilegal siempre lleva el sello de la culpa"[353].

Es importante mencionar en este punto la discrepancia existente entre la responsabilidad civil –específicamente lo que ocurre con la culpa infraccional- y la responsabilidad penal en el ámbito de la culpabilidad. Así, la culpa civil infraccional no necesita ser completada con una imputación subjetiva del ilícito, a diferencia de lo que ocurre en materia penal, donde el error de prohibición resulta ser una excusa suficiente. De esta manera, el profesor Barros plantea que "en la medida que la culpa es concebida como infracción a un deber de cuidado, son irrelevantes las circunstancias subjetivas en cuya virtud se produjo la contraversión"[354] [355].

[353] Ibídem. p.99
[354] Ídem.
[355] Es tal el caso en que se presume la culpa o responsabilidad, que el autor del delito posee limitadas herramientas para desvanecer este elemento, pudiendo recurrir sólo a la incapacidad, a la involuntariedad del acto, a que le es física o moralmente imposible cumplir con la regla o que en atención a las circunstancias no fue posible actuar de otra manera. En: BARROS. Ibídem. p.100

La segunda hipótesis es demandar civilmente por responsabilidad extracontractual al autor del delito de usurpación de nombre de forma autónoma, esto es, sin la presencia de una sentencia penal condenatoria, persiguiendo la indemnización de perjuicios por el daño causado.

Si bien en ambos casos se debe probar los distintos elementos que configuran la responsabilidad civil extracontractual y tal como lo señalábamos anteriormente, nos parece que en el segundo escenario se dificulta la presentación del actor, dado que debe probar el dolo existente en la configuración del delito, ya que a diferencia de lo que ocurre en sede penal con el delito de usurpación de identidad, tanto en su esfera tradicional como aquella que se da en un contexto de Internet y redes sociales -donde acordamos que el dolo se presume, en cuanto sólo puede existir este ánimo para cometer el ilícito, no siendo posible que proceda la culpa[356]-, en sede civil extracontractual, para obtener una indemnización de perjuicios, debemos hacer un examen más profundo del elemento subjetivo del dolo, por cuando, la regla general es que el dolo no se presume, sino que se debe

[356] Puesto que nadie puede apropiarse de la identidad de otro por negligencia o falta de cuidado.

probar, con la excepción de los casos en que la ley lo señale, no estando contemplada la del delito en comento dentro de estas hipótesis, lo que nos lleva a pensar que es muy difícil y reduce las posibilidades de que una demanda de este tipo sea acogida.

2.4. Tribunal competente

En Chile, la aplicabilidad del derecho penal responde a un criterio espacial, determinado legalmente por los artículos 5 y 6 del Código Penal[357], y los artículos 5 y 6 del Código Orgánico de Tribunales[358], que establecen como el principio más reconocido para determinar la

[357] Artículo 5. La ley penal chilena es obligatoria para todos los habitantes de la República, inclusos los extranjeros. Los delitos cometidos dentro del mar territorial o adyacente quedan sometidos a las prescripciones de este Código.
Artículo 6. Los crímenes o simples delitos perpetrados fuera del territorio de la República por chilenos o por extranjeros, no serán castigados en Chile sino en los casos determinados por la ley.
[358] Artículo 5, inciso primero. A los tribunales mencionados en este artículo corresponderá el conocimiento de todos los asuntos judiciales que se promuevan dentro del territorio de la República, cualquiera que sea su naturaleza o la calidad de las personas que en ellos intervengan, sin perjuicio de las excepciones que establezcan la Constitución y las leyes.
Artículo 6, inciso primero. Quedan sometidos a la jurisdicción chilena los crímenes y simples delitos perpetrados fuera del territorio de la República que a continuación se indican.

competencia de los Tribunales el de territorialidad, es decir, para que los órganos judiciales conozcan de un delito –y fallen conforme a la ley penal chilena-, éste debe haberse cometido dentro del territorio de nuestra República[359].

Sin embargo, y a pesar de la primacía que tiene el principio de territorialidad, la Ley no establece cuándo un injusto es "cometido" dentro del país, por lo que surge la problemática de determinar el lugar de comisión del ilícito[360], lo que se ve exacerbado en el caso de los ciberdelitos.

[359] Reforzando el mismo principio del lugar de comisión, se encuentra el artículo 157, inciso primero, del Código Orgánico de Tribunales, que establece que: "Será competente para conocer de un delito el tribunal en cuyo territorio se hubiere cometido el hecho que da motivo al juicio".

[360] Cabe mencionar que para el caso de que exista un conflicto positivo de jurisdicción entre dos o más Estados, todos partes del Código de Bustamante, dicho cuerpo normativo establece expresamente una solución en su artículo 302, que dice: "Cuando los actos de que se componga un delito, se realicen en Estados contratantes diversos, cada Estado puede castigar el acto realizado en su país, si constituye por sí solo un hecho punible. De lo contrario, se dará preferencia al derecho de la soberanía local en que el delito se haya consumado".

Particularmente, en cuanto a la usurpación de identidad que se ejecuta a través de la Web y las redes sociales, éste "abarca un ámbito delictivo bastante amplio" [361] , en virtud del nacimiento del concepto de "ciberespacio", el que se define como "un espacio virtual de interacción, un espacio relacional que se constituye a través del intercambio de información, es decir, es espacio y es medio" [362] , y que no puede identificarse con un lugar físico determinado[363].

[361] Esto, debido, a que en palabras de la autora, "Internet se presta como medio para cometer delitos que importan emisión, transferencia o intercambio de información, atentados contra datos protegidos y otros" En: CÁRDENAS A., C. 2008. El lugar de comisión de los denominados ciberdelitos. [en línea] Polít. crim., N° 6, 2008, A2-6, <http://www.politicacriminal.cl/n_06/A_2_6.pdf> p. 3.

[362] BALMACEDA HOYOS, GUSTAVO "El delito de Estafa Informática". Ediciones Jurídicas de Santiago año 2009. p. 60. En: GUEVARA M., A. 2011. Aproximación a la problemática de la delincuencia informática, punibilidad y ley aplicable. Magallanes, Universidad de Chile, Facultad de Derecho, Escuela de Postgrado. p. 55.

[363] Incluso, se estima por algunos que habría que convenir que "Internet es todos los sistemas, redes y subredes que se interconectan y cada uno de estos sistemas es de sus distintos titulares, con sus propias reglas jurídicas; del mismo modo que tendríamos que responder que Internet está en cada acceso, proveedor de servicios y en definitiva encada máquina que interviene en el sistema y en todas ellas a la vez, de tal modo que los criterios de regulación territorial aplicables al conjunto del sistema no resultan viables (…)" En: CONSEJO GENERAL del Poder Judicial. 2001. Internet y Derecho Penal. Madrid, España. pp. 651.

Con el fin de dar solución a esta problemática, se han suscitado diferentes alternativas.

Un primer planteamiento sugiere que la "teoría de la actividad" –aquella que se basa en el lugar del principio de ejecución de la conducta-, y la "teoría del resultado" –la cual se apoya en el lugar donde la conducta desenvolvió sus efectos propios-, sean extendidas al contexto de los ciberdelitos[364], o bien, que se aplique la "teoría de la ubicuidad" – la que establece que son competentes para conocer del delito los Tribunales tanto del lugar donde se dio principio a su ejecución como del lugar donde se produjo el resultado punible-, por cuanto "se estima que es la teoría que mejor se adecúa a las exigencias derivadas del respeto a la soberanía territorial del Estado, ya que a éste le corresponde garantizar la seguridad pública dentro de su territorio, la que se perturba tanto si allí tiene lugar la conducta como si allí tiene lugar el resultado[365].

[364] CÁRDENAS. Op. Cit. pp. 6 – 11.
[365] Ibídem. p. 11.

Respecto a las interpretaciones extensivas enunciadas, en la "teoría de la actividad", se entiende que "quien sube datos a Internet no solamente actúa en el lugar donde se encuentra físicamente presente, sino que en todo Estado en el que los datos puedan ser accedidos a través de Internet"[366]. Mientras que, en la "teoría del resultado", se ha establecido un concepto de resultado más amplio, que lo entiende como "la afectación del bien o interés jurídicamente protegido"[367], considerando entonces tanto "aquel lugar en que la concreción del verbo rector tuvo lugar, como todo efecto de la conducta, e inclusive, el lugar en donde existe el peligro abstracto"[368].

Es menester destacar que ambas teorías en su versión extendida producirían un efecto de universalidad que conduciría a una inseguridad jurídica, en cuanto cualquier Estado tendría jurisdicción sobre una conducta punitiva que se desenvuelve en otro Estado, por desarrollarse el ciberdelito en cualquiera de los puntos donde se puede acceder a la información comprometida a través de Internet, lo cual a su vez crea el peligro de que toda persona que esté involucrada en este "transporte" de los datos que son

[366] Ibídem. p. 7.
[367] GÓNZALEZ TAPIA, "El lugar", cit. nota nº 9, p. 354. En: Ibídem. p. 8.
[368] Ídem.

objeto del ilícito sea enjuiciada por cualquier país, y por lo mismo bajo cualquier legislación, donde tal conducta sea punible[369] [370] [371].

Una segunda propuesta para determinar el lugar de comisión del delito, cuando éste se lleva cabo a través de Internet, estima que "es necesario en estos casos, además de la interpretación imaginativa de las reglas existentes (…), el establecimiento de otros criterios distintos del de la territorialidad, como pueden ser los del lugar de la sede principal de los autores y el de la sede de las víctimas o perjudicados, o ambos a la vez adecuadamente combinados" [372], con el fin de facilitar las tareas de investigación y

[369] CÁRDENAS A., C. 2008. El lugar de comisión de los denominados ciberdelitos. [en línea] Polít. crim., N° 6, 2008, A2-6. <http://www.politicacriminal.cl/n_06/A_2_6.pdf> pp. 9 y 10.
[370] GUEVARA. Op. Cit. pp. 56 y 57.
[371] En este mismo sentido, Marchena Gómez indica que "La incondicionada persecución de toda acción delictiva ejecutada mediante Internet no puede sostenerse con un mínimo de rigor. De ahí que la reformulación del principio de universalidad a partir de un criterio puramente instrumental, supondría un verdadero peligro para la coherencia del sistema de delimitación jurisdiccional". En: MARCHENA GÓMEZ, M., "Algunos aspectos procesales de Internet.". pp. 34 y ss. En: MATA Y MARTÍN., R.M. 2001. Delincuencia Informática y Derecho Penal. Madrid, España. Edisofer. , 2001. p. 149.
[372] CONSEJO GENERAL del Poder Judicial. Op. Cit. p. 657.

enjuiciamiento, y dar preferencia a aquel Tribunal que se encuentre en mejor posición de enfrentar dichos cometidos.

Una tercera proposición, ofrecida por el Derecho Penal Internacional, consiste en la creación de un Derecho Internacional Penal de Internet, el cual contempla dos sub-alternativas admisibles.

Como primera opción, configurar una Ley Penal Internacional con tipos penales unificados en relación a Internet, encomendando su enjuiciamiento a órganos judiciales penales de carácter internacional, siendo sus ventajas "patentes desde el punto de vista de la seguridad jurídica, el decaimiento de la impunidad en Internet y de la superación de los problemas de aterritorialidad de la Red" [373]. O bien, como segunda opción, que se desarrolle la configuración de una Ley Penal de Internet única e internacional, pero dejando que los procesos sean efectuados por las jurisdicciones propias de cada país.[374]

[373]Ibídem. p. 660.
[374]Ídem.

Ambas alternativas, a nuestro parecer, son poco viables, ya que más allá de los obvios conflictos que esto generaría entre las jurisdicciones nacionales, la primera haría necesario tanto que todos los Estados acordaran ser parte de este sistema -lo que es utópico por decir lo menos- como que se superaran rápidamente las dificultades que existen actualmente para crear órganos jurisdiccionales internacionales específicos[375] –lo que también se ve imposible de lograr-, y la segunda requeriría de la misma unanimidad en el acuerdo de adoptar una misma Ley, pero basados en el principio de cooperación internacional respecto de su enjuiciamiento en los propios ámbitos nacionales, lo que si bien tiene una tasa de probabilidad mayor, tampoco da total seguridad de que se acabarán los "paraísos penales" para la actividad delictual a través de Internet[376].

Otra posible solución, ésta ya dirigida al campo del Derecho privado, más específicamente para el ámbito de responsabilidad extracontractual, es aquella "dada por el Tribunal de Justicia de la Comunidad Europea en la

[375] Como ocurrió en su momento con la creación del Tribunal Penal Internacional para enjuiciar a quienes ejecutaron delitos contra la humanidad.
[376] Ibídem. pp. 659 y 660.

sentencia Shevill, de 7 de marzo de 1995, que en síntesis y aunque no se trata de un caso producido respecto de Internet, establece la competencia de los tribunales del país donde se produce el hecho causal del daño y los de los países donde se produce el daño, a elección del perjudicado, aunque con ámbitos distintos en cuanto a la determinación de las indemnizaciones pertinentes"[377]. Lo que da una respuesta menos difusa en cuanto a la aterritorialidad que existe en la Web, si la usurpación de identidad no puede configurarse como delito penal y el afectado decide perseguir la reparación del daño sufrido por la vía civil.

A modo de conclusión, pensamos que si bien la aplicación estricta del principio de territorialidad para la utilización de la Ley Penal conlleva a la impunidad de la usurpación de identidad que se ejecuta en las redes sociales, y de los ciberdelitos en general, no son menos los riesgos ligados a las diferentes alternativas que se ofrecen.[378] Dicho esto, estimamos que la mejor alternativa – en virtud de las desafíos que existen actualmente en la

[377] Ibídem. p. 659.
[378] Es por esto que Seminara, en "La pirateria su Internet e il diritto penale", señala que se estaría sustituyendo la anarquía de Internet por una anarquía de Derecho. En: MATA Y MARTÍN. Op. Cit. pp. 149 y 150.

materia- para establecer la competencia de los Tribunales cuando se trate de delitos informáticos, será la interpretación extensiva de las teorías “de la actividad” y “del resultado”, sumado al establecimiento de criterios como los del lugar donde se encuentren los autores o las víctimas, o una combinación de ambos. Junto, claramente, al esfuerzo de uniformizar los tipos penales en relación a Internet en las distintas legislaciones nacionales, que apoyado en la cooperación internacional, permita que los Tribunales con una mejor posición se encarguen de enjuiciar tales ciberdelitos.

3. Distinción con el Robo de identidad

Como ya hemos asegurado, Internet se ha impuesto como una nueva plataforma para la comisión de delitos, por lo que muchos de ellos, incluso hasta los más tradicionales, se han trasladado y acomodado a la era de las nuevas tecnologías. Esto, en virtud de la facilidad que ofrece Internet para cometer delitos desde la comodidad del propio hogar, pudiendo engañar a una mayor cantidad de personas con el sólo uso del computador personal.

Junto con la usurpación de identidad, existe otra figura delictiva que también se hace valer de la sustracción de datos personales para alcanzar un objetivo determinado diferente de la mera suplantación; ya sea defraudar a terceros, obtener una ganancia económica, u otros.

El delito de robo de identidad, al compartir tal rasgo distintivo, puede fácilmente ser confundido con la suplantación de identidad, razón por la cual cabe explicar en qué consiste este ilícito, con el fin de disipar cualquier duda y delimitarlos uno del otro[379].

3.1. Concepto

El robo de identidad o fraude de identidad es "cualquier clase de fraude que dé como resultado la pérdida de datos personales, como por ejemplo contraseñas, nombres de usuario, información bancaria o números de

[379] Debemos destacar que esta distinción no es unánime por parte de la doctrina comparada, ya que existen legislaciones que tratan como sinónimos "robo" y "suplantación" de identidad.

tarjetas de crédito" [380] . Otra conceptualización del robo de identidad determina que éste ocurre "cuando una persona adquiere, transfiere, posee o usa información personal de una persona natural o jurídica de forma no autorizada, con la intención de cometer, o en conexión con, fraude o algún otro crimen"[381].

Entonces, podemos establecer que este delito consiste en conseguir y utilizar, de manera maliciosa mediante fraude o engaño, los datos personales de otra persona con el fin de obtener una ganancia económica.

Es común que con la obtención de tales datos sensibles, el delincuente en cuestión logre el acceso no autorizado de cuentas bancarias o financieras de la víctima, mas este ilícito puede extenderse a la acumulación de deudas o a la comisión de otros delitos bajo el nombre del afectado. Incluso, muchas

[380] MICROSOFT. Centro de seguridad y protección. 2012. ¿Qué es el robo de identidad? [en línea] <http://www.microsoft.com/es-xl/security/resources/identitytheft-whatis.aspx> [consulta: 11 de diciembre de 2013]

[381] ORGANIZATION FOR Economic Co-operation and development. 2008. OECD Policy Guidance on Online Identity Theft. [en línea] Seoul, Korea. OECD Ministerial Meeting on the Future of the Internet Economy. 17-18 june, 2008. <http://www.oecd.org/internet/consumer/40879136.pdf> p. 2.

veces la pérdida que sufre la víctima es respecto de su reputación, lo cual también podría conllevar un perjuicio económico, en cuanto existe un costo financiero asociado a la restauración de su nombradía dentro de la comunidad y a la corrección de la información errónea de la cual el criminal es responsable[382].

Debemos destacar que el delito de robo de identidad tiene directa relación con el fraude y la obtención de una ganancia pecuniaria, a través del uso indebido de los datos personales de un tercero, por lo que se trataría de un delito de orden económico, sin importar si el resultado es una utilidad económica o un desmedro a la reputación de la víctima.

3.2. Formas de búsqueda de información personal

Este tipo de fraude se basa principalmente en la obtención y posterior utilización de datos personales, más allá del resultado perjudicial que se

[382] THE UNITED STATES Department of Justice. Identity theft and Identity fraud. [en línea] <http://www.justice.gov/criminal/fraud/websites/idtheft.html> [consulta: 20 de septiembre de 2013]

provoque con esto, lo cual otorga especial importancia a la forma de búsqueda de tal información.

La mayoría de las personas no tienen noción de la facilidad con la que los criminales obtienen sus datos, mas existen variadas formas de lograrlo, las cuales pueden clasificarse en dos categorías; los métodos tradicionales y las prácticas online para el acceso a la información[383].

3.2.1. Métodos tradicionales para acceder a datos personales

- Shoulder surfing: Esta práctica consiste en observar al afectado desde muy cerca cuando éste se encuentre usando o compartiendo alguna información personal relevante, por lo general de carácter financiera, que después pueda ser ocupada para el robo de identidad.

[383] ORGANIZATION FOR Economic Co-operation and development. 2008. OECD Policy Guidance on Online Identity Theft. [en línea] Seoul, Korea. OECD Ministerial Meeting on the Future of the Internet Economy. 17-18 june, 2008. <http://www.oecd.org/internet/consumer/40879136.pdf> pp. 3 y 4.

- Dumpster diving: Consiste en la revisión del tarro de basura con el fin de obtener copias de cheques, tarjetas de crédito o del estado de la cuenta bancaria de la persona, que por lo general incluyen nombre, dirección y número de teléfono, todos datos que sirven para asumir la identidad de otro.

- Pretexting: Esta fórmula consiste en comunicarse con una institución financiera o una compañía de teléfono, haciéndose pasar por un cliente legítimo, y solicitar la información de la cuenta del mismo. Existen otros casos, en que el pretexto se realiza gracias a información privilegiada de un funcionario de la misma institución o el acceso a los datos se hace a través de la creación fraudulenta de una nueva cuenta en el nombre del afectado.

- Skimming: Se refiere a la captura de la información personal de la banda magnética de las tarjetas de crédito, información que posteriormente es transmitida y recodificada en otras tarjetas de carácter fraudulento.

- Business record Theft: Consiste en el robo de la información personal, por un tercero o por un funcionario de la misma organización, directamente de la institución bancaria.

3.2.2. Métodos Online para acceder a datos personales[384]

- Spam: El "correo basura" consiste en el envío masivo de correos electrónicos no solicitados, no deseados o con remitente desconocido, muchas veces con contenido publicitario, que perjudican en variadas maneras al software del receptor. En ocasiones son mensajes que re-direccionan la información del receptor, siendo vectores de malware y phishing.

- Malware: Consiste en la introducción de un programa o un software codificado en un sistema de información, con la finalidad de causar daño a

[384] Hoy, dichas técnicas se han ampliado al mundo del Internet, donde las nuevas formas de obtener estos datos sensibles son cada vez más comunes y de aspecto menos sospechoso, lo que hace más fácil ser víctima de este tipo de delitos.

tal sistema o a otros, o alterarlos para que se usen de un modo distinto al previsto para sus propios usuarios.

- Phishing: Método que consiste en atraer los datos de identificación personal de los usuarios desprevenidos en Internet, a través de correos electrónicos y sitios web ficticios con apariencia de ser negocios legítimos. Para tales efectos, tanto los e-mails como las páginas web "espejo" utilizan los logotipos o las gráficas de sitios oficiales para confundir a las víctimas y así conseguir la información.

Esta forma de "pescar datos" se beneficia de la confianza que ofrece la entidad que es suplantada para solicitar la información personal, lo cual minimiza las posibilidades de sospecha ante estos correos o páginas electrónicas falsas.[385]

- Hacking: Se basa en la exploración de vulnerabilidades de sistemas electrónicos o software de computadores para robar información personal.

[385] CONSEJO GENERAL del Poder Judicial. 2006. Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad? Madrid, España. pp. 71-73.

3.3. Prácticas de ejecución del robo de identidad[386]

Al ser el robo de identidad un fraude cometido con el fin de utilizar información personal de un tercero -para identificarse como él- sin la determinada autorización, es relevante estudiar qué hace el delincuente con tal información, por lo que a continuación veremos cuáles son las modalidades de ejecución de este delito, después de conseguidos los datos personales respectivos.

---

[386] Respecto de las formas en que se ejecuta el delito de robo de identidad, la gran discusión gira en torno a la responsabilidad, ya que habría un desacuerdo sobre quién debe asumir la culpa en estos delitos.
Es de opinión de varios servidores e instituciones bancarias que la culpa en la comisión de este delito recaería en las víctimas, por cuanto existiría un descuido por parte de aquellas respecto de su propia información personal, más específicamente la de índole financiera, sin embargo, es habitual que las víctimas no tengan conocimiento siquiera de cómo ni quién les robó sus datos personales.
Existen autores que, por el contrario, estiman que al ser -todas estas instituciones y servicios- parte de un mercado competitivo, tal responsabilidad debiese recaer en quien provee el servicio determinado, ya que es su deber ofrecer tales prestaciones con un nivel de seguridad financiera adecuado y suficiente, siendo esta fiabilidad la que se premie con la confianza y lealtad de los consumidores. En: HOOFNAGLE., C. J. 2007. Identity Theft: Making the Known Unknowns known. [en línea] Harvard Journal of Law & Technology. Volume 21, Number 1 Fall 2007. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=969441> [consulta: 25 de septiembre de 2013] pp. 99-100.

3.3.1. Abrir cuenta nueva

En el fraude de cuenta nueva, el impostor utiliza la información personal del afectado para abrir nuevas líneas de crédito, cuentas de teléfono, adquirir tarjetas o cuentas de crédito, de cheques, entre otros. Lo relevante de esta modalidad de ejecución es que la víctima puede adquirir grandes deudas por acción de un tercero, lo que puede perjudicarle al querer conseguir un crédito o, incluso afectarlo en sus anhelos laborales, ya que su reputación se vería degradada.

3.3.2. Malversación de cuenta existente

Esta modalidad de ejecución del robo de identidad consiste en la utilización de cuentas existentes de las víctimas, como cuentas de tarjeta de crédito, cuentas de ahorro, cuentas de teléfono, etc. Por lo general, el impacto de este tipo de fraude es menor que la apertura de nuevas cuentas

bancarias[387], sumado a que detentan una mayor protección por parte de las mismas instituciones financieras, en tanto la mayoría de seguros que se ofrecen están principalmente apuntados al resguardo de las cuentas existentes en el caso de ser utilizadas sin autorización por terceros extraños.

3.3.3. Comisión de otros fraudes

Es posible que el ladrón de identidad utilice la información personal de las víctimas con otras finalidades –distintas a conseguir una ganancia monetaria-, como; darle los datos del afectado a la policía si es detenido o acusado de algún delito, usarla para obtener determinados servicios por parte del gobierno o terceros, o zafarse de pagar alguna obligación previamente adquirida, entre otras incontables situaciones.

4. Tratamiento legal en el Derecho Comparado

[387] Ibídem. p. 103.

En vista de la falta de regulación legal del delito de suplantación de identidad en Internet y las redes sociales en Chile, pasaremos a exponer la situación relativa a este ilícito que existe en diferentes países.

4.1. Normativa en el Sistema Europeo

A pesar de las limitantes que existen para la Unión Europea para legislar dentro de la esfera del Derecho Penal[388] de cada Estado Miembro, esta organización ha elaborado distintas normas relativas a la protección de la identidad y de la privacidad, así como también ha establecido delitos contra el acceso ilegal a los sistemas informáticos[389]. Sin embargo, no existen disposiciones penales que aborden el delito de usurpación de identidad[390].

---

[388] CONSEJO DE EUROPA. 2007. Internet-related identity theft. [en línea] Economic Crime Division. Alemania. 33p. <http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/Internet_related_identity_theft_%20Marco_Gercke.pdf> p.106

[389] NACIONES UNIDAS. 2013. Manual sobre los delitos relacionados con la Identidad. [en línea] Oficina de las Naciones Unidas contra la Droga y el Delito. Nueva York. 380pp. <http://www.unodc.org/documents/organized-crime/13-83700_Ebook.pdf> p.42-43

[390] Aparentemente no se hace una clara distinción entre el delito de usurpación de identidad, suplantación de identidad, robo de identidad y hurto de identidad.

Los problemas que se presentan a propósito de la suplantación de identidad en Internet son conocidos por este organismo[391] y representan una importante preocupación que ha aumentado con los años, cuestión que se hace presente al declarar que "la cooperación policial y judicial en el seno de la Unión Europea se vería facilitada si el robo de identidad se tipificara como delito en todos los Estados Miembros"[392] [393] [394].

El Consejo de Europa por su parte, buscando soluciones concretas a los problemas que nacen a propósito de la delincuencia informática, ha presentado instrumentos para comprender de mejor manera lo que se entiende por usurpación de identidad, siendo uno de estos la Convención

[391] Cabe destacar el Dictamen 5/2009 sobre las redes sociales en línea, donde la Unión Europea plantea los problemas que se generan en torno a estas plataformas. En: CONSEJO DE EUROPA. 2009. Dictamen 5/2009 sobre las redes sociales en línea. [en línea] Grupo de trabajo sobre protección de datos del artículo 29. Bruselas 14p. <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_es.pdf> [consulta:]

[392] Comisión Europea, Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones –Hacia una política general de lucha contra la ciberdelincuencia", 22 de mayo de 2007. En: NACIONES UNIDAS. 2013. Op. Cit. p.43

[393] CONSEJO DE EUROPA. 2007. Op. Cit. p. 170

[394] El dilema de tipificar este delito radica en que los países pertenecientes a esta organización poseen herramientas jurídicas que difieren radicalmente unas de otras, por lo que unificar una solución es una ardua tarea.

sobre Cibercrimen de Budapest de 2001[395], que si bien representa un avance en el tema, no contiene una norma que sancione la suplantación de identidad, ya que sólo contiene sanciones contra el acceso ilegal o acceso a un sistema informático sin autorización, la intercepción ilegal, la interferencia de datos en el sistema y el mal uso de dispositivos[396].

En el año 2007, el Consejo de Europa elaboró un estudio titulado "Hacia una política general de lucha contra la ciberdelincuencia"[397], donde analiza los distintos criterios que existen respecto de la tipificación del robo de identidad relacionado con Internet[398] y señala que: "si bien las disposiciones del Convenio sobre el delito cibernético eran aplicables en los casos de

[395] ROMERO F., R. Las conductas vinculadas a la suplantación de identidad por medios telemáticos: una propuesta de acción legislativa. [en línea] México. pp.849-863. <http://biblio.juridicas.unam.mx/libros/6/2941/24.pdf> p. 860

[396] ABDEL W, M., CHAWKI, M. 2006. Identity Theft Cyberspace: Issues and Solutions. [en línea] Lex Electronica, vol.11, N°1. 41p. <http://www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf> p.30-31

[397] COMISIÓN DE LAS Comunidades Europeas. 2007. Hacia una política general de lucha contra la ciberdelincuencia. [en línea] Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones. Bruselas. <http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:52007DC0267> [consulta: 21 de marzo de 2015]

[398] NACIONES UNIDAS. 2013. Op. Cit. p.44

hurto de identidad, no había disposiciones específicas que abordaran el hurto de identidad en sí que fueran aplicables a todos los actos conexos"[399] [400].

En esta Comunicación, el Consejo hace un estudio sobre la evolución de los ilícitos cibernéticos, tratando la usurpación de identidad como parte de la delincuencia tradicional en las redes electrónicas[401], indicando qué se debe entender por ésta [402] y denunciando que como lucha contra la delincuencia en las redes sociales es necesario "emprender un análisis

[399] Ídem.
[400] CONSEJO DE EUROPA. 2007. Op. Cit. p.30-31
[401] "1.2.2. Delincuencia tradicional en las redes electrónicas: La mayor parte de los delitos se pueden cometer con ayuda de las redes electrónicas. De hecho, diversos tipos de fraude o intentos de fraude son particularmente frecuentes y constituyen una forma de delincuencia cada vez más extendida en las redes electrónicas. Instrumentos como la usurpación de identidad, las estafas por Internet (phishing), los envíos masivos de correo basura y los códigos malévolos pueden servir para cometer fraudes a gran escala. El comercio ilícito nacional e internacional a través de Internet constituye otro problema en aumento. Incluye el tráfico de drogas, armas y especies amenazadas". En: COMISIÓN DE LAS Comunidades Europeas. 2007. Op. Cit.
[402]"En general, por «usurpación de identidad» se entiende la utilización de datos de identificación personales, por ejemplo un número de tarjeta de crédito, para cometer otros delitos. En la mayoría de los Estados miembros, más que por la usurpación de identidad, el responsable será probablemente procesado por el fraude o los demás delitos que cometa, puesto que el fraude se considera una infracción más grave." En: Ídem.

detallado con vistas a la elaboración de una propuesta de normativa específica de la UE contra la usurpación de identidad"[403].

En enero de 2009, ante una serie de preguntas respecto del delito de suplantación de identidad[404] ante la Comisión Europea, ésta respondió que estaban conscientes de que la comisión de este delito -junto con el fraude de identidad- está en aumento en la Unión Europea, motivo por el cual fue incluido en la Comunicación del 2007, lo que consistió en la primera fase concentrada de medidas para mejorar la cooperación y coordinación internacional. En particular, señala que la Comisión se ha puesto en marcha mediante un proceso de licitación para el estudio comparativo respecto al régimen de los distintos Estados Miembros y su reglamentación sobre el delito de robo de identidad[405].

---

[403] Ídem.

[404] PARLAMENTO EUROPEO. 2008. Preguntas parlamentarias. Asunto: Usurpación de identidad. [en línea] <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+WQ+E-2008-5963+0+DOC+XML+V0//ES> [consulta: 6 de abril de 2015]

[405] PARLAMENTO EUROPEO. 2009. Parliamentary questions. Answer given by Mr Barrot on behalf on the Commission. [en línea] <http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2008-5963&language=ES> [consulta: 6 de abril de 2015]

Para el Consejo de Europa, la usurpación de identidad se ha convertido en uno de los más extensos delitos cibernéticos en relación con la vulnerabilidad de la arquitectura de la identidad, ya que el importante desarrollado de las redes sociales ha traído consigo la construcción de una cultura de identidad digital, permitiendo el fácil acceso a la información personal por parte de terceros[406] [407].

El 26 de marzo del mismo año, el Parlamento Europeo emitió una Recomendación destinada al Consejo de Europa, donde se hace un llamado a su Presidencia para reflexionar sobre una estrategia integral que tenga por objeto combatir la delincuencia virtual. En ésta se incluye como propuesta legislar sobre el delito de usurpación de identidad, para que se regule por

[406] CONSEJO DE EUROPA. 2007. Op. Cit. p.7

[407] Sin embargo, es importante señalar que el éxito de la lucha contra la usurpación o robo de identidad no es un punto prioritario dentro del desarrollo de los delitos informáticos, ya que resultan más importantes otros aspectos como la cooperación internacional para hacer efectiva la aplicación de la convención por parte de los países que la han ratificado.

una parte la sanción adecuada para quienes cometan este delito, como una forma apropiada de resarcir a las víctimas de él[408].

Examinando la legislación de algunos Estados en específico del continente europeo, podemos identificar que existen variados criterios y regulaciones al respecto.

Por un lado encontramos países donde no existe todavía una sanción específica al delito de usurpación de identidad digital como es el caso de España[409], donde la ley aplicable debe ser adaptada a figuras delictivas ya existentes como la que se contempla en el artículo 401 del Código Penal Español, que regula la usurpación del estado civil[410].

[408] AREVALO M, P. 2011. Modelo de regulación jurídica de las redes sociales virtuales. [en línea] Revista VIA IURIS, Fundación Universitaria Los Libertadores, Colombia. n° 11, julio-diciembre 2011. pp.109-136. <http://www.redalyc.org/pdf/2739/273922799007.pdf> p.116

[409] DIALNET. 2013. La suplantación de una identidad digital. [en línea] <file:///C:/Users/Nicole/Downloads/Dialnet-LaSuplantacionDeUnaIdentidadDigital-4179718.pdf>

[410] Artículo 401 Código Penal Español: El que usurpare el estado civil de otro será castigado con la pena de prisión de seis meses a tres años.

Pese a lo anterior, en el caso español existe una notoria preocupación al respecto, ya que recientemente -en septiembre del 2014- la Fiscalía General del Estado propuso tipificar el delito de suplantación de identidad en Internet[411]. En este sentido, el Fiscal General del Estado, don Eduardo Torres-Dulce declara que: "se está detectando un incremento cada vez mayor de este tipo de conductas en foros, chats o redes sociales y, en general, en los medios de comunicación electrónicos, con el evidente perjuicio que las mismas pueden generar en el normal desarrollo de la vida

[411] La posible redacción del tipo penal que sería la siguiente:
El que sin consentimiento y de forma creíble se haga pasar por otra persona real o ficticia a través de un sitio Web o por otros medios electrónicos con el fin de ofender, intimidar, amenazar o defraudar al mismo o a un tercero… A los efectos del párrafo anterior, una suplantación es creíble si cualquiera podría creer razonablemente, o creyó, que el sujeto podía ser o es la persona que aparentaba. La expresión «medios electrónicos» comprende la creación de sitios web, la apertura de cuentas de correo electrónico, y la apertura de una cuenta o perfil en redes sociales a nombre de otra persona, real o ficticia. Las penas señaladas se impondrán sin perjuicio de las procedentes por los hechos en que consista la ofensa, amenaza, intimidación o fraude. En: FISCALIA GENERAL del Estado. 2014. [en línea] 7.11 Fiscal de Sala Coordinadora en materia de Criminalidad Informática. España. pp.1103-1157 <https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/memoria2012_vol1_amf_17.pdf?idFile=20d58c12-50c3-42ce-9157-fdef3762090e> [consulta: 20 de marzo de 2015]

y actividad personal y profesional de quien es víctima de esa suplantación de identidad online"[412].

Por otro lado, encontramos países que sí se ha regulado de forma expresa el delito de usurpación de identidad como es el caso de Francia, el cual mediante una modificación en el año 2011 a su Código Penal, en su artículo 226-4-1[413] sanciona este ilícito, indicando que el "acto de hacerse pasar por un tercero (…) se castiga con las mismas penas cuando se cometan en una red de comunicación pública en línea"[414], quedando claro el progreso de la nación francesa en la materia.

---

[412] DIARIO DE NOTICIAS. 2014. La Fiscalía propone tipificar la suplantación en Internet. [en línea] <http://diariodenoticias.laley.es/documento.asp?id=./NE0000492377_20140916.HTML> [consulta: 17 de marzo de 2015]

[413] Article 226-4-1: Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende.
Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne.

[414] Traducción propia. En: FRANCIA. Código Penal de Francia. [en línea] Artículo 226-4-1 <http://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070719&idArticle=LEGIARTI000023709201> [consulta: 22 de febrero de 2015]

4.2. Normativa en Estados Unidos

En Norteamérica, se debe distinguir el tratamiento legal que existe por una parte a nivel federal -donde el término utilizado para referirse a la usurpación de identidad es el "robo o hurto de identidad"[415]- y por otra a nivel estatal[416] -en que se ha legislado como delito de suplantación de identidad-. Podemos identificar al respecto una gran diferencia entre estos dos delitos en Estados Unidos, ya es que el robo de identidad se encuentra relacionado generalmente con el beneficio económico, donde el apropiarse de una cuenta bancaria, número social, entre otros, trae consigo un enriquecimiento pecuniario para su autor. Mientras que la suplantación es

[415] Se utiliza el término robo y hurto indistintamente.

[416] Algunos Estados han desarrollado el delito de suplantación de identidad de forma acabada, como son los Estados de California, Texas, Nueva York y Mississippi entre otros. Sin embargo, a modo de estudio, sólo nos referiremos brevemente a los tres primeros Estados por ser las principales jurisdicciones que han aportado al respecto.

hacerse pasar por otra persona, sin que haya una ganancia económica necesariamente[417].

A nivel Federal existe una sanción específica en contra del "Identity Theft", estatuto promulgado el 30 de octubre de 1998 y que corresponde al 18 United State Code §1028 letra a), número 7)[418]. Este proyecto original fue modificado durante el 2004 cuando se establecieron agravantes para su comisión y el año 2007, momento en que se presentó un proyecto de ley con relación a la aplicación y compensación para las víctimas[419], por lo que hoy corresponde a una norma que se utiliza tanto para enjuiciar a quien o quienes lo han cometido, como para reparar pecuniariamente el daño

[417] ALLCLEARID. 2012. Online impersonation vs. Identity theft: Is there a difference? [en línea] <https://www.allclearid.com/blog/online-impersonatin-vs-identity-theft.> [consulta: 16 de marzo de 2015]
[418] 18 United State Code §1028 a) 7) (a) Whoever, in a circumstance described in subsection (c) of this section (…) (7) knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law;
[419] NACIONES UNIDAS. 2013. Op. Cit. p. 45

causado a las víctimas de este delito, tanto para el ilícito clásico, como para el de identidad digital[420].

Es importante destacar que la misma norma revela qué se entiende por medios de identificación, representando un término bastante amplio[421], incluyendo cualquier nombre o número, sea solo o en combinación con otra información que permita identificar a una persona específica[422], lo que en definitiva admite la conciliación de la ley a través del tiempo respecto de las distintas formas de identificación, como son una cuenta en alguna red social.

[420] BORGHELLO y TEMPERINI. Op. Cit. p. 12

[421] the term "means of identification" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any—
(A) name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
(B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
(C) unique electronic identification number, address, or routing code; or
(D) telecommunication identifying information or access device (as defined in section 1029 (e))

[422] ABDEL W, M., CHAWKI, M. 2006. Op. cit. p.27

El mencionado estatuto -y sus modificaciones- se hacía completamente necesario dentro de la legislación americana, puesto que anteriormente sólo se prohibía la producción o posesión de documentos de identificación falsos[423], lo que por una parte excluía cualquier otro tipo de forma de identificación que no fuera formal, mientras que por otra, no contenía una sanción para el robo o uso sin autorización de la información personal asociado a estos documentos[424], además de que no se adaptaba a la rápida expansión de la tecnología[425] [426].

La legislación norteamericana "completa su esquema a través de la tipificación de la tenencia ilegítima de datos de identificación personal, así como del tráfico (sin consentimiento) de estos datos"[427], dirigiéndose especialmente a subsanar las pérdidas económicas sufridas por el acto ilícito, así "bajo el estatuto federal (…) el procesamiento del acusado de

[423] INTERNAL REVENUE SERVICE. 1999. Memorandum for Assistant Regional Counsel. [en línea] United States. 7p. <http://www.unclefed.com/ForTaxProfs/irs-wd/1999/9911041.pdf> p.4
[424] ABDEL y CHAWKI. Op. cit. p. 26
[425] INTERNAL REVENUE SERVICE. Op. Cit. p.1
[426] Según la opinión de algunos, el robo de identidad facilita la comisión de otros delitos, como son el fraude informático, el fraude con tarjetas de crédito, entre otros.
[427] BORGHELLO y TEMPERINI. Op. Cit. p. 12

robo de identidad en un sitio de redes sociales para fines no económicos probablemente sería un desperdicio"[428].

Siendo este el panorama a nivel Federal, podemos encontrar algunos Estados que se han destacado por sus legislaciones sobre el tema, los cuales, como señalamos antes, tratan este delito de forma más específica[429] dejando de lado el "robo de identidad" y tipificando el delito de "suplantación de identidad" que se asemeja más a la usurpación de identidad que planteamos en la presenta memoria.

Nueva York fue el primer Estado en implementar una figura legal que contempla la suplantación de identidad en Internet. La iniciativa nace a partir de la idea del senador Andrew Lanza el año 2007, señalando que: "el problema de la suplantación de Internet se intensifica con la creciente

[428] Traducción propia En: REZNIK, M. 2013. Identity Theft on Social Networking Sites: Developing Issues of Internet Impersonation. Touro Law Review. Vol. 29, N° 2, Article. 12, 2013. pp 455-483. <http://digitalcommons.tourolaw.edu/cgi/viewcontent.cgi?article=1472&context=lawreview> [consulta: 10 de enero de 2014] p.473

[429] CLANTON, K. 2010. We are not who pretend to be: ODR alternatives to online impersonation statutes. [en línea] Cardozo Journal of Conflict Resolution, Vol. 16. pp. 323-355 <http://cardozojcr.com/wp-content/uploads/2014/11/Clanton_ODR-Alternatives.pdf> p.333

disponibilidad de los datos personales en línea, así como el aumento de sitios de redes sociales y sitios de citas. Los impostores en Internet han encontrado maneras de defraudar y victimizar a las personas (…) debemos abordar el creciente peligro que representa los impostores de Internet pasando por sobre la ley"[430]. Este proyecto sale a luz en 2008 bajo la sección 190.25 del Código Penal del Estado de Nueva York[431].

[430] Traducción propia de Andrew J. Lanza, Senator Lanza Introduces Legislation Making Internet Impersonation a Crime, NYSenate.gov (Apr. 4, 2007). En: Ibídem. p. 338

[431] N.Y. Penal Law Section 190.25: A person is guilty of criminal impersonation in the second degree when he: 1. Impersonates another and does an act in such assumed character with intent to obtain a benefit or to injure or defraud another; or 2. Pretends to be a representative of some person or organization and does an act in such pretend pretended capacity with intent to obtain a benefit or to injure or defraud another; or 3. (a) Pretends to be a public servant, or wear or displays without authority any uniform, badge, insignia or facsimile thereof by which such public servant is lawfully distinguished, or falsely expresses by his words or actions that he is a public servant or acting with approval or authority of a public agency or department; and (b) so acts whit intent to introduce another to submit to such pretended official authority, to solicit funds or to otherwise cause another to act in reliance upon that prense. 4. Impersonates another by communication by internet website or electronic means with intent to obtain benefit or injure or defraud another, or by such communication pretends to be a public servant in order to induce another to submit to such authority or act in reliance on such pretense. Criminal impersonation in the second degree is a class A misdemeanor.

En un memorándum original que fue acompañado a la Asamblea del mismo Estado se señala que el propósito de esta nueva ley es disuadir a quienes intentan desde robar una identidad hasta hacerse pasar por otra persona[432], ya que "la suplantación se ha convertido en un problema cada vez más grande en los Estados Unidos debido a la facilidad de hacerse pasar por otra en las comunicaciones en línea"[433].

El Estado de California promulgó el año 2010 –entrando en vigencia el 1 de enero de 2011- una ley que regula y pretende modernizar la antigua norma de 1872, motivado en gran medida por el Senador Joe Simitian, quien intentó proporcionar protección contra la suplantación en línea[434]. Así nace la sección 528.5 del Código Penal de California, la que sanciona a quien a sabiendas, sin el consentimiento de la persona y de manera razonablemente creíble, suplanta a otra persona a través de o en un sitio Web de Internet o por otro medio electrónico[435] que sea para los propósitos

[432] Ibídem. p.339
[433] Traducción propia En: REZNIK. Op. Cit. p.474
[434] CLANTON. Op. Cit. p. 334
[435] Esta norma utiliza términos de forma específica como "creíble" y "medio electrónico", señalando qué debe entenderse por ellos en el mismo cuerpo normativo limitando la amplitud de su uso común.

de dañar, amenazar o defraudar a otra persona[436]. Esta norma no sólo establece este delito como tipo penal, sino que permite a las víctimas que han sufrido daños con la suplantación en línea presentar una demanda civil[437].

[436] California Penal Code Section 528.5. (a) Notwithstanding any other provision of law, any person who knowingly and without consent credibly impersonates another actual person through or on an Internet Web site or by other electronic means for purposes of harming, intimidating, threatening, or defrauding another person is guilty of a public offense punishable pursuant to subdivision (d).
(b) For purposes of this section, an impersonation is credible if another person would reasonably believe, or did reasonably believe, that the defendant was or is the person who was impersonated.
(c) For purposes of this section, "electronic means" shall include opening an e-mail account or an account or profile on a social networking Internet Web site in another person's name.
(d) A violation of subdivision (a) is punishable by a fine not exceeding one thousand dollars ($1,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.
(e) In addition to any other civil remedy available, a person who suffers damage or loss by reason of a violation of subdivision (a) may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief pursuant to paragraphs (1), (2), (4), and (5) of subdivision (e) and subdivision (g) of Section 502.
(f) This section shall not preclude prosecution under any other law.

[437] HAZZARD, Y. A Little Know Weapon To Combat Online Impersonation: California Penal Code Section 528.5 [en línea] 2p. <http://www.robinskaplan.com/~/media/PDFs/A%20Little%20Known%20Weapon%20to%20Comba%20Online%20Impersonation.pdf> p. 1

La historia de esta ley deja en evidencia cuál es su objetivo, puesto que se indica que esta norma es una "ampliación del falso actual estatuto de suplantación de identidad, donde se incluye la suplantación realizada en un sitio Web de Internet o por medio de otros medios electrónicos como el correo electrónico, Facebook, Twitter y otros sitios Web de medios de comunicación social" [438]. El reglamento de California ha tomado en consideración el detrimento que puede causar a una persona la suplantación de su identidad digital en su vida cotidiana, por lo que, dentro de otras medidas, permite obtener información de los proveedores de servicio para conseguir la identidad del suplantador.

El Estado de Texas, a fines del 2011[439] promulgó una ley en donde regula el delito de suplantación online en la sección 33.07 de su Código Penal[440],

[438]Traducción propia. En: Ídem. p.1
[439] REZNIK. Op. Cit. p.477
[440] Sec. 33.07. ONLINE IMPERSONATION. (a) A person commits an offense if the person, without obtaining the other person's consent and with the intent to harm, defraud, intimidate, or threaten any person, uses the name or persona of another person to: (1) create a web page on a commercial social networking site or other Internet website; or (2) post or send one or more messages on or through a commercial social networking site or other Internet website, other than on or through an electronic mail program or message board program.

donde se castiga justamente –dentro de otros delitos- a quien sin el consentimiento de otra persona, con la intención de dañar, defraudar,

---

(b) A person commits an offense if the person sends an electronic mail, instant message, text message, or similar communication that references a name, domain address, phone number, or other item of identifying information belonging to any person: (1) without obtaining the other person's consent; (2) with the intent to cause a recipient of the communication to reasonably believe that the other person authorized or transmitted the communication; and (3) with the intent to harm or defraud any person.

(c) An offense under Subsection (a) is a felony of the third degree. An offense under Subsection (b) is a Class A misdemeanor, except that the offense is a felony of the third degree if the actor commits the offense with the intent to solicit a response by emergency personnel.

(d) If conduct that constitutes an offense under this section also constitutes an offense under any other law, the actor may be prosecuted under this section, the other law, or both.

(e) It is a defense to prosecution under this section that the actor is any of the following entities or that the actor's conduct consisted solely of action taken as an employee of any of the following entities: (1) a commercial social networking site; (2) an Internet service provider; (3) an interactive computer service, as defined by 47 U.S.C. Section 230; (4) a telecommunications provider, as defined by Section 51.002, Utilities Code; or (5) a video service provider or cable service provider, as defined by Section 66.002, Utilities Code.

(f) In this section: (1) "Commercial social networking site" means any business, organization, or other similar entity operating a website that permits persons to become registered users for the purpose of establishing personal relationships with other users through direct or real-time communication with other users or the creation of web pages or profiles available to the public or to other users. The term does not include an electronic mail program or a message board program. (2) "Identifying information" has the meaning assigned by Section 32.51.

intimidar o amenazar, crea una página o envía uno o más mensajes en alguna red social comercial u otro sitio de Internet.

Una gran diferencia que podemos establecer con el caso de California, es que dentro de la ley se distingue si existe o no intención de causar daño por parte de quien comete el delito, calificando el primer caso como un delito grave y el segundo como uno menor[441]. Esto es importante de destacar porque generalmente se exige dolo para que este delito se configure, lo que "permite que sea lo suficientemente amplio como para aplicarse a los casos en que las personas víctimas o sus fotografías sean utilizadas para crear un perfil en los medios sociales, incluso bajo un nombre falso"[442], casos en que no necesariamente existe una intención de dañar a otro.

4.3. Normativa en Argentina

En la República de Argentina, los últimos 5 años han estado marcados por los esfuerzos de distintos profesionales y políticos con el fin de

[441] CLANTON. Op. Cit. p. 336
[442] Traducción propia. En: Ídem.

encontrar una solución legislativa a la situación de crisis que vive actualmente la identidad, puesto que toda persona que goza de identificación en la Red se ve amenazada por los constantes y crecientes embates de la ciberdelincuencia.

Un primer paso dentro de la lucha por proteger el ámbito digital de la personalidad se desarrolló con la iniciativa de proyecto de ley 2257/11, del 9 de septiembre de 2011, que perseguía incluir el artículo 157 ter al Código Penal de la Nación, tipificando el delito de obtención ilegítima de datos confidenciales ("Phishing")[443]. Tal artículo[444] pretendía que se sancionara a

[443] Información General. Expediente 2257/11. Proyecto de Ley incorporando el art. 157 ter al Código Penal, tipificando el delito de obtención ilegítima de datos confidenciales ("Phishing"). [en línea] <http://www.senado.gov.ar/web/proyectos/verExpe.php?origen=S&numexp=2257/11&tipo=PL&tConsulta=1> [consulta: 20 de febrero de 2015]

[444] Art. 157 ter. Será reprimido con prisión de un (1) mes a dos (2) años o multa de pesos diez mil a pesos cien mil el que:
1. Mediante cualquier forma de ardid o engaño, indebidamente obtuviere o captare datos personales, financieros o confidenciales.
2. Con fines ilícitos, diseñare, programare, desarrollare, vendiere, ejecutare, facilitare o enviare un dispositivo, sistema o programa informático, destinados a la indebida obtención o captura de datos personales, financieros o confidenciales.
En: Información General. Expediente 2257/11. Proyecto de Ley incorporando el art. 157 ter al Código Penal, tipificando el delito de obtención ilegítima de datos confidenciales ("Phishing"). [en línea]

quien captara ilegalmente datos personales, financieros o confidenciales, a través de engaño, o que, con fines ilícitos, diseñare, programare, desarrollare, vendiere, ejecutare, facilitare o enviare un dispositivo, sistema o programa informático, destinados a la indebida obtención de los mismos.

Dentro de la investigación sobre el "Phishing" llevada a cabo por el Abogado Marcelo Temperini y el Licenciado en informática Cristián Borghello –ambos asesores en el proyecto presentado-, se distinguen dos fases en la obtención ilegal de datos confidenciales; la primera consta de la captación de información sensible del usuario a través de distintas técnicas electrónicas (phishing propiamente tal, spam, malware, etc.), donde se engaña al mismo para que entregue voluntariamente los datos solicitados (nombre de usuario, contraseña, números de cuenta, PIN, tarjetas de crédito, etc.). Mientras que en su segunda fase, respecto de la utilización que se le puede dar a la información, el delincuente se haya ante variadas posibilidades, pudiendo vender la información, extraer directamente dinero de las cuentas obtenidas, adquirir bienes o servicios a través de canales

---

<http://www.senado.gov.ar/web/proyectos/verExpe.php?origen=S&numexp=2257/11&tipo=PL&tConsulta=1> [consulta:]

virtuales en nombre de otro, suplantar la identidad de la víctima, publicar los datos en Internet, entre otras[445].

A la época de la iniciativa, lo que se mantiene hasta el día de hoy, el phishing se entendía regulado como un tipo especial -representado en el artículo 173, inciso 16 del Código Penal trasandino[446]- de la figura clásica de la estafa -del artículo 172 del mismo cuerpo legal[447]-, no pudiendo configurarse éste sin la presencia del engaño y del perjuicio patrimonial consecuencia del fraude[448]. Lo que no coincide con lo planteado por estos profesionales, que estiman que el phishing se constituye al completarse su

[445] BORGHELLO y TEMPERINI. Op. Cit. pp. 3-5.
[446] Artículo 173. Sin perjuicio de la disposición general del artículo precedente, se considerarán casos especiales de defraudación y sufrirán la pena que él establece:
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. En: ARGENTINA. Código Penal de la Nación de Argentina. [en línea] <http://www.infoleg.gov.ar/infolegInternet/anexos/15000-19999/16546/texact.htm#18> [consulta: 13 de marzo de 2015]
[447] Artículo 172. Será reprimido con prisión de un mes a seis años, el que defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión empresa o negociación o valiéndose de cualquier otro ardid o engaño. En: Ídem.
[448] BORGHELLO y TEMPERINI. Op. Cit. pp. 9 y 10.

primera fase -la recolección o "pesca" de datos personales-, sin importar el destino que se le dé a la información ilegalmente obtenida, razón por la cual proponían crear un tipo delictual autónomo que sancionara el phishing propiamente tal, sin estar necesariamente vinculado a la estafa[449].

Esta idea, a pesar de los esfuerzos políticos, no proliferó, puesto que hoy no se desliga el phishing del delito de estafa, y no logró incluirse el artículo 157 ter al Código Penal argentino.

Una segunda línea defensiva para la protección de la identidad digital se manifestó en la iniciativa de proyecto de Ley 1312/12, del 15 de mayo de 2012, que buscaba agregar al Código punitivo el artículo 138 bis, tipificando la suplantación de identidad digital como delito[450]. Dicha norma[451] reprime con prisión o multa, según el caso, a aquellos que sin el

[449] Ídem.

[450] Información General. Expediente 1312/12. Proyecto de Ley incorporando el art. 138 bis al Código Penal, por el cual se tipifica el delito de Suplantación de Identidad Digital. [en línea] http://www.senado.gov.ar/web/proyectos/verExpe.php?origen=S&tipo=PL&numexp=1312/12&nro_comision=&tConsulta=1 [consulta: 24 de febrero de 2015]

[451] Artículo 138 bis. Será reprimido con prisión de 6 (seis) meses a 3 (tres)

consentimiento debido, adquieran, tuvieran en posesión, transfirieren, crearen o utilizaren la identidad de una persona física o jurídica que no les corresponda, a través de Internet o cualquier otro medio electrónico, y detenten la intención de dañar, extorsionar, defraudar, injuriar o amenazar a otra persona u obtener beneficio para sí o para terceros.

Este plan, realizado también por Temperini y Borghello, persigue que la identidad digital de las personas físicas y jurídicas sea protegida como un bien jurídico propio, puesto que un daño a ésta se traduce en un perjuicio directo a la personalidad de la víctima, por ser la primera una extensión de la segunda[452].

Según el estudio que respalda la iniciativa, la usurpación de identidad puede ejecutarse de diferentes maneras, mas "sus elementos básicos y la

---

años o multa de pesos veinte mil a pesos doscientos mil, el que sin consentimiento, adquiriere, tuviere en posesión, transfiriere, creare o utilizare la identidad de una persona física o jurídica 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 otra persona u obtener beneficio para sí o para terceros. En: Información General. Expediente 1312/12. Ídem.

[452] Ídem.

finalidad son siempre los mismos: la obtención de información personal para realizar algún tipo de perjuicio"[453]. De tal sencilla estructura, debemos destacar que carece de importancia el carácter que detenta el daño, puesto que puede afectar a la persona en un ámbito económico, en su honor, reputación, en un aspecto laboral, entre otros, lo que genera un claro problema: se hace extremadamente difícil dimensionar las consecuencias que el delito conlleva para la víctima en el mundo físico y en su vida diaria.

La moción para castigar la usurpación de identidad a través de medios electrónicos, como son las famosas redes sociales, se basa entonces en el amplio crecimiento de este delito en Argentina, dada su falta de regulación legal, sumado a la ausencia de capacitación y concientización de las víctimas para proteger su identidad, y la peligrosidad que lleva consigo la suplantación ejecutada, puesto que el ciberdelincuente podrá cometer cualquier otra conducta maliciosa que perjudique a la víctima, ya sea en su patrimonio, en su honor, o en otro ámbito de su individualidad[454].

[453] BORGHELLO y TEMPERINI. Op. Cit. pp. 4-6.
[454] Información General. Expediente 1312/12. Op. Cit.

Siendo patente el riesgo de que la suplantación de identidad puede conllevar a la comisión de otros múltiples delitos, el ímpetu de los políticos María de los Ángeles Higonet y Carlos Verna, que perseguían la protección de la identidad digital como un bien jurídico digno de una tutela más atenta por parte del Estado, no se concreta, caducando el expediente 1312/12 en febrero de 2014, y, en consecuencia, no siendo agregado el artículo 138 bis al Código Penal de la Nación[455].

4.4. Normativa en México

En México, la usurpación de identidad y su posible ejecución en el marco de las redes sociales es una problemática que no se ha desarrollado de manera uniforme, en parte por el sistema federado que detenta este país.

A nivel legislativo federal no existe un tipo penal específico que regule tal conducta ilícita, con la excepción del artículo 249, fracción I, del Código Penal Federal, que "dispone una norma penal relacionada con la variación del nombre o apellido, asumiendo el de otra persona al declarar ante una

[455] Ídem.

autoridad judicial"[456] [457], lo cual tiene poca correspondencia con la usurpación de identidad que ya hemos analizado, y ninguna relación con que este delito se cometa en una plataforma virtual.

En el plano local son pocos los Estados que regulan la usurpación de identidad, y más específicamente aquella que se da en el contexto de las redes sociales.

El Estado de Colima, en abril de 2009, mediante el decreto 525[458], agrega en su Código Penal la fracción VII al artículo 234, que considera

[456] Artículo 249. Se impondrán de diez a ciento ochenta jornadas de trabajo en favor de la comunidad:
I. Al que oculte su nombre o apellido y tome otro imaginario o el de otra persona, al declarar ante la autoridad judicial;
II. Al que para eludir la práctica de una diligencia judicial o una notificación de cualquiera clase o citación de una autoridad, oculte su domicilio, o designe otro distinto o niegue de cualquier modo el verdadero, y
III. Al funcionario o empleado público que, en los actos propios de su cargo, atribuyere a una persona título o nombre a sabiendas de que no le pertenece.
En: Código Penal Federal de México. [en línea] <http://info4.juridicas.unam.mx/ijure/tcfed/8.htm?s=> [consulta: 25 de febrero de 2015]
[457] ROMERO L. 2011. Op. Cit. 163.

como delito “la suplantación de identidades que se realiza por medios informáticos, telemáticos o electrónicos que tienen como consecuencia la obtención de un lucro indebido”[459] [460].

---

[458] DECRETO No. 525. SE REFORMA EL PRIMER PÁRRAFO Y LA FRACCIÓN V, Y SE ADICIONA LA FRACCIÓN VII, AL ARTÍCULO 234 DEL CÓDIGO PENAL PARA EL ESTADO DE COLIMA. [en línea] Tomo 94 Colima, Col., Sábado 09 de Mayo del año 2009; Núm. 19; pág. 763.
<http://www.ordenjuridico.gob.mx/Estatal/COLIMA/Decretos/COLDEC300.pdf>

[459] Artículo 234. Se considera fraude y se impondrá pena de uno a nueve años de prisión y multa hasta por 100 unidades, para el caso de las fracciones I y II, y de tres a nueve años de prisión y multa hasta por la misma cantidad en el caso de las fracciones III, IV, V, VI, y VII en los siguientes casos:

…

VII.- Al que por algún uso del medio informático, telemático o electrónico alcance un lucro indebido para sí o para otro valiéndose de alguna manipulación informática, instrucciones de código, predicción, intercepción de datos de envío, reinyecte datos, use la red de redes montando sitios espejos o de trampa captando información crucial para el empleo no autorizado de datos, suplante identidades, modifique indirectamente mediante programas automatizados, imagen, correo o vulnerabilidad del sistema operativo cualquier archivo principal, secundario y terciario del sistema operativo que afecte la confiabilidad, y variación de la navegación en la red o use artificio semejante para obtener lucro indebido. En: Código Penal del Estado de Colima. [en línea] <http://www.docstoc.com/docs/167421085/Código-Penal---Congreso-del-Estado-de-Colima> [consulta: 25 de febrero de 2015]

[460] ROMERO L. Op. Cit. p. 161.

El Estado de México, por su parte, con el decreto 235 del año 2010, reforma la denominación del Capítulo V, del subtítulo III del Título III, del Libro Segundo de su Código Penal, adicionando los artículos 264 y 265[461] [462], en los cuales tipifica el delito de usurpación de identidad, mas sin establecer la hipótesis de que éste se produzca en las redes sociales. Sin embargo, para poder aplicar tal normativa al escenario de Internet, se deben

[461] Artículo 264. Se le impondrán de uno a cuatro años de prisión y de cien a quinientos días multa, a quien ejerza con fines ilícitos un derecho o use cualquier tipo de datos, informaciones o documentos que legítimamente pertenezcan a otro, que lo individualiza ante la sociedad y que le permite a una persona física o jurídica colectiva ser identificada o identificable, para hacerse pasar por él.
Se equiparan a la usurpación de identidad y se impondrán las mismas penas previstas en el párrafo que precede prevista en el presente artículo a quienes:
I. Cometan un hecho ilícito previsto en las disposiciones legales con motivo de la usurpación de identidad;
II. Utilicen datos personales, sin consentimiento de quien deba otorgarlo;
III. Otorguen el consentimiento para llevar a cabo la usurpación de su identidad; y
IV. Se valgan de la homonimia para cometer algún ilícito.
Las sanciones previstas en este artículo se impondrán con independencia de las que correspondan por la comisión de otro u otros delitos.
Artículo 265. Las penas señaladas en el artículo anterior se incrementarán hasta en una mitad, cuando el ilícito sea cometido por un servidor público aprovechándose de sus funciones, o por quien sin serlo, se valga de su profesión o empleo para ello.
En: Código Penal del Estado de México. Op. Cit.
[462] ROMERO L. Op. Cit. p. 161.

relacionar las disposiciones enunciadas con el artículo 53 de la Ley para el Uso de Medios Electrónicos del Estado de México[463], que sí establece claramente que se comete el delito de sustitución de identidad cuando, por cualquier medio, se obtenga, reproduzca, apodere, administre, utilice o de cualquier forma se dé un uso indebido a "un certificado, a una firma electrónica y/o a un sello electrónico, sin que medie el consentimiento o autorización expresa de su titular o de quien se encuentre facultado para otorgarlos"[464]. Entendiéndose por "cualquier medio", aquellos medios informáticos, telemáticos o electrónicos, en los cuales es común el uso de certificados, firmas o sellos electrónicos, comprendiendo, por tanto, todo medio virtual en que se transfiera información personal que pueda ser usada de forma indebida por alguna persona a la que no corresponda.

[463] Artículo 53. Comete el delito de apropiación de certificado y sustitución de identidad, el que por cualquier medio obtenga, reproduzca, se apodere, administre, utilice o de cualquier forma dé un uso indebido a un certificado, a una firma electrónica y/o a un sello electrónico, sin que medie el consentimiento o autorización expresa de su titular o de quien se encuentre facultado para otorgarlos.
Por la comisión de este delito se impondrá una pena de tres a ocho años e prisión y una multa de ochocientos a mil quinientos días de salario mínimo general vigente en la zona de que se trate, independientemente de las sanciones administrativas o penales que puedan corresponder a la conducta realizada. En: ROMERO L. Op. Cit. pp. 162 y 163.
[464] Ídem.

En el caso del Código Penal para el Distrito Federal, éste fue reformado el 29 de Junio de 2010, con la creación del "Capítulo III denominado de la "usurpación de identidad o personalidad" del Título XII, mediante el cual se adicionó el artículo 211 bis[465]. La Asamblea Legislativa del Distrito Federal, al adicionar este precepto penal, indicó que la iniciativa se orientaba a buscar la protección en la intimidad de las personas, así como la certeza jurídica en sus posesiones cuando alguien vulnerare su identidad con fines delictivos"[466].

Cabe recalcar que, dentro de los considerandos expuestos en el Dictamen relativo a la iniciativa de reforma del Código punitivo para el Distrito

[465] Artículo 211 bis. Al que por cualquier medio usurpe, con fines ilícitos, la identidad de otra persona, u otorgue su consentimiento para llevar a cabo la usurpación en su identidad, se le impondrá una pena de uno a cinco años en prisión y de cuatrocientos a seiscientos días multa.
Se aumentarán en una mitad las penas previstas en el párrafo anterior, a quien se valga de la homonimia, parecido físico o similitud de la voz para cometer el delito establecido en el presente artículo.
En: Asamblea Legislativa del Distrito Federal, VI Legislatura. Código Penal para el Distrito Federal. [en línea] <http://www.aldf.gob.mx/archivo-5b523887b84cba9b46e165101d758f01.pdf> [consulta: 15 de enero de 2014]

[466] ROMERO L. Op. Cit. p. 161.

Federal, se indica especialmente el problema de que "en la actualidad, el fácil acceso a los medios electrónicos, los avances tecnológicos, las llamadas redes sociales y el uso de servicios de banca por Internet, se han constituido en una herramienta primordial para aquellos que adoptan la identidad de un tercero, normalmente para cometer algún ilícito, para ocultarse o para evadirse de la acción de la justicia. La utilización de datos a través de redes sociales, correos electrónicos, solicitudes de servicios, trámites públicos y privados, etcétera; mediante los cuales se aporta información personal a terceros aparentemente "confiables", para los usuarios, permite que los delincuentes obtengan de manera sencilla los datos para realizar esta nueva modalidad de afectación contra la Seguridad de las Personas, constituyéndose en una actividad a todas luces ilícita"[467].

Y por último, en el Estado de Guanajuato, el 29 de enero de 2015, se presentó una iniciativa que busca reformar el Código Penal de la respectiva

[467] Asamblea Legislativa del Distrito Federal. V Legislatura. Diario de los debates de la Asamblea legislativa Federal. [en línea] <http://www.aldf.gob.mx/archivo-3930456bab522331c3f868909142f63d.pdf>

localidad, con el fin de agregar el artículo 215-a, que sancionará la usurpación de identidad.

Dentro de los motivos del proyecto destaca: primero, el carácter inherente de la identidad respecto de la persona humana, la cual debe tener protección penal para garantizar su pleno ejercicio y evitar atentados contra la misma por parte de terceros extraños; y segundo, la posibilidad de que el derecho a la identidad "sea trasgredido por aquellos que valiéndose de la información que poseen, de su argucia y en algunos casos de su habilidad en el manejo de medios electrónicos, se hacen pasar por otros, para obtener un beneficio o lucro indebido, lo que en la actualidad se conoce como usurpación de identidad"[468].

Además, el Poder Legislativo de Guanajuato establece que el delito de usurpación de identidad está estrechamente "ligado con el uso de las nuevas Tecnologías de la Información y Comunicación (TIC) utilizadas

[468] PODER LEGISLATIVO GUANAJUATO. Sala de Prensa. 2015. Propone el GPPAN sancionar la usurpación de identidad. 29/01/2015/ Boletín: 1234. [en línea] <http://www.congresogto.gob.mx/comunicados/propone-el-gppan-sancionar-la-usurpacion-de-identidad> [consulta: 8 de abril de 2015]

comúnmente para la invasión de la privacidad y la obtención de datos personales que sólo su titular es capaz de conocer mediante la generación de claves de acceso, las cuales son apropiadas no siempre para la obtención de un fin eminentemente económico"[469].

Por lo anterior es que esta iniciativa busca que "se sancione (…) a quien empleando cualquier medio y sin el consentimiento de quien legalmente deba otorgarlo, se haga pasar por otra persona, utilice su identidad, ejerza sus derechos o se apropie de sus datos personales, o siendo titular de éstos, otorgue su consentimiento para que se efectúen dichas conductas, en beneficio propio o de un tercero, o para producir un daño al titular de la identidad, a su patrimonio, o a persona ajena"[470].

[469] Ídem.

[470] La sanción correspondería a pena de prisión de uno a cinco años y de diez a cincuenta días multa. "Disponiéndose además, que las sanciones privativas de libertad y económicas se aumentarán cuando: a) El sujeto activo se valga de la homonimia para usurpar la identidad; b) Cuando se aproveche la igualdad física y genética entre hermanos gemelos; y c) Cuando el sujeto activo tenga experiencia en las ramas tecnológicas o de ingeniería, o se aproveche de su profesión o empleo." En: Ídem.

5. Tratamiento legal en Chile de la usurpación de identidad en redes sociales: Proyecto de Ley que modifica el Código Penal, con el propósito de sancionar la suplantación de identidad realizada a través de Internet y redes sociales, ocasionando daños a terceros

En cuanto a los ciberdelitos en general, nuestro país, con la Ley 19.223, se posiciona como pionero en la materia, en cuanto es el primer antecedente en la región latinoamericana que otorga tratamiento legal a los delitos informáticos. En esta normativa se contemplan las figuras delictivas del sabotaje y espionaje informático[471] y, como ya hemos mencionado, protege la calidad, pureza e idoneidad de la información, la propiedad para el caso de los fraudes informáticos y la privacidad, intimidad y confidencialidad de los datos, entre otros[472].

Es indudable que la Ley que tipifica figuras penales relativas a la informática, representaba una solución adecuada a lo que exigía la realidad

[471] PEÑA O., P. 2013. ¿Cómo funciona internet? Nodos críticos desde una perspectiva de los derechos. Guía para periodistas. Chile. ONG Derechos Digitales. p.42.
[472] Historia de Ley 19.223.

en ese entonces, puesto que en el año 1993 la informática e Internet no abarcaban con tal magnitud los diferentes ámbitos de la vida cotidiana como lo hacen hoy.

Diferente es lo que sucede en la actualidad, ya que en virtud de la expansión en el uso que se le da a Internet, dicha Ley no es suficiente para proteger a las personas de las nuevas amenazas que con ello se han creado, como es el caso de los peligros a los que nos vemos expuestos con las redes sociales. Dichas plataformas han sido las grandes protagonistas del último tiempo, pues son utilizadas por la gente común para actividades habituales –como comunicarse con otros, informarse de lo que está pasando dentro y fuera del país o simplemente compartir experiencias-, por los distintos medios de comunicación social –usándolas como punto de conexión con la ciudadanía-, e incluso por entes administrativos –que emiten información oficial del gobierno a través de ellas-, y por esto, se han transformado en un referente crucial para la opinión pública.

Sin embargo, estos foros no están exentos de ser un lugar propicio para cometer delitos informáticos, puesto que debido a su cómodo acceso y lo

fácil en su uso permiten que muchas personas realicen conductas indebidas en la Red, ejemplo claro de esto son aquellos usuarios que se adscriben a las diversas redes sociales sin representarse fielmente a sí mismos, sino que utilizando el nombre, las fotografías u otro signo distintivo de la personalidad de otro con la intención de ejecutar una usurpación de identidad de otro.

Es por esta y por otras razones, que las diputadas María José Hoffmann, Marisol Turres, y los diputados Juan Antonio Coloma, Ramón Farías, Iván Fuentes, Gonzalo Fuenzalida, Sergio Ojeda, René Saffirio y Arturo Squella, presentaron el pasado 6 de noviembre de 2014, mediante el boletín 9700-07, un proyecto de ley que busca modificar el artículo 214 Código Penal, agregando un inciso segundo a fin de sancionar la suplantación de identidad realizada a través de Internet y redes sociales o cualquier otro medio, ocasionando daños a terceros.

El propósito del proyecto es que el artículo 214 quede de la siguiente manera:

El que usurpare el nombre de otro será
castigado con presidio menor en su grado
mínimo, sin perjuicio de la pena que pudiere
corresponderle a consecuencia del daño que
en su fama o intereses ocasionare a la persona
cuyo nombre ha usurpado.

En caso que dicha suplantación se realizare
a través de internet, redes sociales o cualquier
otro medio, ocasionando daños a terceros,
será castigado con presidio menor en su
grado medio y multa de 5 a 30 UTM.

Dentro de los fundamentos expuestos por estos políticos para propulsar tal cambio normativo podemos encontrar: la antigüedad del Código punitivo; el aumento de las denuncias por suplantación de identidad ante la Policía de Investigaciones entre los años 2012 y 2013; la posibilidad de que la usurpación de identidad se dé conjuntamente con otros delitos; la insuficiencia de la Ley 19.223 “por cuanto en la fecha de su creación

Internet y las redes sociales no se habían desarrollado en Chile"[473]; la baja penalidad del actual artículo 214; entre otros.

Más allá de los evidentes errores de redacción y sintaxis que presentan el mencionado proyecto, son las cuestiones de fondo las que merecen una especial atención.

En primer lugar, el argumento basado en lo expuesto por la abogada y profesora de la Pontificia Universidad Católica de Chile Ángela Vivanco, que establece que: "Cuando se invade cualquier tipo de cuenta privada o se usa la imagen sin previo aviso, se viola el artículo 19 números 4 y 5 de la Constitución Política de la República de Chile, es decir, nuestra Constitución establece una inviolabilidad de las comunicaciones privadas. Hacerlo es un delito"[474], no tiene relación con el fin perseguido por la iniciativa parlamentaria, puesto que al tener la intención de agregar un inciso segundo al artículo 214 del Código Penal, es lógico que la

[473] Proyecto de Ley que modifica el artículo 214 del Código Penal, agregando el inciso segundo a fin de sancionar la suplantación de identidad realizada a través de Internet, redes sociales o cualquier otro medio con daños a terceros y a su vez aumenta su penalidad con multas. p.2
[474] Ibídem. p.3

modificación ha de enfocarse en proteger el mismo bien jurídico que su inciso primero, que es la protección al derecho a la identidad y no el que se ampara por las normas constitucionales mencionadas.

No cabe duda que la inviolabilidad de las comunicaciones privadas tiene un ámbito de protección muy amplio, que abarca desde las interceptaciones telefónicas, a la revisión de correspondencia ajena, hasta la intervención del correo electrónico de otra persona, lo que no significa que deba extenderse al absurdo de sancionar un delito bajo el nombre de otro, como sería el hacer pasar la usurpación de identidad por vulneración de comunicaciones privadas.

Un segundo punto a examinar es la falta de sentido que tiene la inclusión en el proyecto lo señalado por el profesor de la Universidad de los Andes, Hernán Corral: “Internet es una plataforma donde se desarrollan formas de relaciones humanas que no pueden quedar al margen del ordenamiento jurídico. Deben estar regidas por reglas o normas que garanticen no sólo un buen funcionamiento sino que se respeten los derechos fundamentales de

las personas”[475]. Aquí se demuestra que los diputados buscan modificar el cuerpo normativo en su artículo 214, con el pretexto de que el desarrollo de Internet amenaza con la trasgresión de derechos fundamentales, sin especificar cuáles de ellos pueden verse afectados y cuál sería la conexión de estos con la suplantación de identidad, revelando la falta de investigación que hay detrás de la iniciativa, puesto que el contenido del párrafo no respalda claramente la idea de crear un inciso segundo para tal precepto, pudiendo utilizarse este argumento para solicitar la tipificación de cualquier delito informático.

Por último, es curioso que los parlamentarios, con el interés de detener el acrecimiento exponencial de este delito, propongan aumentar la pena estipulada en el inciso primero de la norma –presidio menor en su grado mínimo, equivalente a la privación de libertad de 61 días a 540 días, según lo determine el tribunal- cuando se trate de una usurpación de identidad ejecutada a través de Internet o las redes sociales, con daños a terceros -presidio menor en su grado medio, que se traduce en privación de libertad de 541 días a tres años, más multa de 5 a 30 UTM-, puesto que de la sola

[475] Proyecto de Ley que modifica el artículo 214 del Código Penal. Ídem.

lectura del proyecto no se entiende la razón que existe para sancionar más estrictamente el mismo delito, que protege el mismo bien jurídico, cuando sólo cambia el medio que se utiliza para su perpetración.

En conversaciones con María Angélica Silva, asesora legislativa de la Diputada María José Hoffmann –propulsora de la iniciativa en cuestión-, entendemos que el aumento de la pena se debe a la exigencia tanto de que la suplantación de identidad se de en escenario de Internet y las redes sociales, como que esta cause daños a un tercero, siendo requisitos copulativos –en palabras de la misma asesora[476]- para aplicar el incremento de la sanción.

Según dicha asesora legislativa, la penalidad del artículo 214 es extremadamente baja, y en la realidad los delincuentes no cumplen con el presidio establecido, por lo que el pretendido aporte del proyecto es la inclusión de una multa –que fluctúa entre 5 a 30 UTM- en la sanción, con el fin de que ésta sobreviva a la pena de cárcel, y tenga un carácter disuasivo respecto de quien ejecute estas malas prácticas. Esta ampliación tan específica del castigo también carece de lógica, puesto que si la verdadera

[476] Véase Punto IV. Preguntas 9 y 10 del Anexo.

intención de los parlamentarios es que al infractor le signifique un costo monetario la comisión de este delito, no entendemos cuál es la razón para elevar en un grado el presidio ya estipulado[477].

En un comienzo y de la simple lectura del proyecto no preguntamos: ¿cuál es el agravante que existe en la suplantación de identidad que se desenvuelve en las redes sociales? ¿Por qué este caso requiere un castigo mayor? Estas interrogantes no lograban ser respondidas, debido a que primero, la moción sólo proporciona un mínimo de información al respecto, sin ahondar en el concepto básico de la identidad, en los elementos necesarios para que la usurpación se configure como delito y otros aspectos relacionados con el ilícito, y segundo, porque no existe tal agravante y el injusto no demanda una mayor sanción. Esto, en virtud de que la usurpación de identidad que se da en Internet y las redes sociales es el mismo delito, se

[477] Presentando directamente en la entrevista realizada nuestra inquietud sobre el aumento en un grado del presidio dispuesto en el artículo 214, cuando la finalidad del incremento en la sanción es que subsista sólo la multa al momento de penar al delincuente, María Angélica Silva no fue capaz de darnos una respuesta coherente. Véase punto IV, pregunta 13 del Anexo.

configura a través de los mismos elementos, con la única diferencia de situarse en un contexto informático.

Entonces ¿puede sancionarse un mismo delito con diferentes penas sólo por darse en escenarios distintos cuando el bien jurídico protegido es el mismo y éste se ve afectado de la misma manera? La respuesta es no. La suplantación de identidad que puede sufrir una persona en Facebook o Twitter se configura con la apropiación de su nombre, sus imágenes u otro elemento distintivo de su personalidad por parte de otro individuo que tiene la intención de actuar como si fuese la víctima y de que se radiquen las consecuencias de sus actos en esta última, sin la necesidad de que se provoque un daño particular diverso a la conculcación de la "verdad personal", e independiente de los perjuicios que pueda soportar el sujeto pasivo en su fama o intereses por la ejecución de delitos conexos. Tal descripción coincide perfectamente con la figura penal clásica, la que sumada al hecho de que el bien jurídico protegido no es uno distinto, sino

sólo una extensión de éste -abarcando tanto la identidad personal como la identidad digital-, evidencia que no merece un tratamiento diverso[478].

Ahora bien, de la entrevista realizada a María Angélica Silva, pudimos comprobar que el incremento de la pena que formula la iniciativa se debe al daño que la usurpación de identidad que se realizare a través de Internet, redes sociales o cualquier otro medio pueda ocasionarle a terceros, mas esto no se explica de tal manera en la moción, ya que en virtud de los fundamentos que se exponen se estaría agregando el inciso segundo para establecer una sanción a la usurpación de identidad que se da en el entorno de la informática, y no por ocasionar daños a terceros, sumado, a que los diputados no determinan qué se entiende por "ocasionando daños a terceros", ni si estos perjuicios derivan de la suplantación de identidad o de los delitos conexos a ella –situación confusa, ya que en el delito de

[478] De la simple lectura del proyecto, da la impresión que sus autores estiman que el aumento de la pena es necesaria, porque al desarrollarse la usurpación de identidad en Internet y las redes sociales, las consecuencias perjudiciales del ilícito podrían ser más gravosas. Sin embargo, este argumento no es utilizado para fundamentar la modificación de la sanción, por lo cual parece que persigue un cambio arbitrario que no se apoya en ninguna razón de peso para ser aceptado.

usurpación de identidad per sé sólo podría verse afectado el usurpado (la víctima) y no terceros-[479].

Para la asesora de la Diputada Hoffmann, "ocasionando daños a terceros" dice relación con aquella situación en que el suplantador, haciéndose pasar por el suplantado, comete un delito conexo perjudicando a un tercero, siendo aún más pernicioso para la persona del usurpado, lo que junto al hecho de que la usurpación de identidad se desenvuelva en las redes sociales –son requisitos copulativos-, justifican el aumento del castigo.

Sin embargo, examinando más detenidamente la propuesta en cuestión y específicamente lo establecido en el pretendido inciso segundo que dice: "En caso que dicha suplantación se realizare a través de internet, redes sociales o cualquier otro medio, ocasionando daños a terceros, será

[479] De la entrevista con la Asesora Legislativa del Diputado Ramón Farías, se puede desprender que, si bien la motivación de la propulsora del proyecto fue sancionar la usurpación de identidad cuando ocasionare daños a terceros, esta idea no se dio a entender claramente en el proyecto, ya que el Diputado Farías, decidió patrocinar la moción en búsqueda de una modernización del Código punitivo para que se sancione con una mayor pena la suplantación efectuada en Internet y las redes sociales, porque se tiene mayor accesibilidad a ellas y son un medio de comisión más peligroso y no porque se cause un daño a terceros. Véase Punto V del anexo.

castigado con presidio menor en su grado medio y multa de 5 a 30 UTM", podemos deducir otra cosa.

Cuando María Angélica Silva establece que para que proceda la sanción del inciso segundo, el delito debe ser cometido "a través de internet, redes sociales o cualquier otro medio", junto con que produzca daños a terceros, enfatizando lo de "cualquier otro medio", podemos darnos cuenta que no se requiere que la suplantación de identidad se desarrolle en un contexto digital –pudiendo entender por "cualquier otro medio" una realidad física, ya representada en el artículo original-, lo cual deja en evidencia que el requisito "ocasionando daños a terceros" es lo único que se exige para que se configure esta agravante, prescindiendo indirectamente del medio de comisión y quitándole el carácter de copulativo a los requisitos mencionados[480].

Lamentablemente, tanto del proyecto como de la entrevista con la asesora legislativa, no es posible deducir todo esto, porque en todo momento se dedican de forma extensa a explicar lo preocupante que es el

[480] Véase Punto IV. Preguntas 9 y 10 del Anexo.

avance a pasos agigantados de la tecnología, dando a entender que el "ocasionar daños a terceros" tiene la misma relevancia que la comisión del injusto sea haga a través de medios electrónicos, siendo ambos elementos necesarios para la aplicación del aumento de la pena.

Es por los motivos anteriores que estimamos que la inserción del inciso segundo al artículo 214 del Código Penal, en los términos pensados por los parlamentarios, es prescindible, en cuanto por darse la usurpación de identidad en un contexto diferente al mundo físico no requiere de una sanción distinta, ni mucho menos mayor, por configurarse de la misma manera que en su tipificación tradicional. Considerando además que, los casos de suplantación que se den en las redes sociales pueden perfectamente ampararse bajo la norma que ya dispone el cuerpo legal, el derecho a la identidad se protege igualmente por la misma, sin necesidad de modificación o aclaración del escenario en el que debe darse, y que cuando se le provoque un perjuicio a un tercero en virtud de un delito conexo, se tienen mejores recursos para verse resguardado frente a esto.

6. Impacto de la usurpación de identidad: Diferencia entre el mundo físico y el ciberespacio

Una vez identificada la figura tradicional de la usurpación de identidad, tipificada en el artículo 214 del Código Penal, y su forma de configuración en el contexto de las redes sociales, además del examen que se hizo del Proyecto de Ley presentado el pasado noviembre de 2014 que trata sobre la materia, cabe preguntarse acerca del impacto que tiene en el mundo físico una suplantación que se da en plataformas virtuales como Facebook y Twitter.

Como bien lo enuncia Oscar Morales en su libro "Delincuencia informática: problemas de responsabilidad", "cualquier aproximación a los delitos relacionados con las Tecnologías de la Información y la Comunicación, en cualquiera de sus formas de expresión, esto es, utilizando el ordenador como medio, objeto o finalidad de ataque, debe ir precedida de una reflexión sobre el impacto social de tales medios y su capacidad de transformación social; sobre las analogías y diferencias de dos espacios bien diferenciados, como son lo que hoy conocemos como mundo real, por un

lado, y realidad o mundo virtual, por otro. Debe efectuarse, asimismo, una valoración de futuro, siempre arriesgada en un sector como el tecnológico, sometido a una recurrente expansión horizontal pero también autoevolutiva, que permita fijar objetivos y, sobre ellos, construir el sistema de equilibrios entre libertad y control, si es que éstos no han de ser idénticos a los que conocemos en las relaciones clásicas"[481].

Hemos de adelantar que el estudio sobre el impacto que este injusto, cometido en las redes sociales, tiene en la vida cotidiana está basado en información sobre usurpación de nombre proporcionada por distintos órganos público, que si bien son estadísticas que ilustrarán nuestra memoria, debemos aclarar que aun así no se puede hablar en términos concretos sobre las reales consecuencias que puede provocar el ilícito, ya que cualquier aseveración sobre el tema se hará basado en una proyección de índole hipotética.

[481] MORALES G., O. 2002. Criterios de atribución de responsabilidad penal a los prestadores de servicios e intermediarios de la Sociedad de la Información. En: MORALES G., O. 2002. Delincuencia informática: problemas de responsabilidad. Cuadernos de Derecho Judicial, Consejo General del Poder Judicial. Madrid, España p.282

Según el proyecto, gracias a los datos otorgados por la Brigada del Cibercrimen de la Policía de Investigaciones, las denuncias por suplantación de identidad ejecutadas en Internet y las redes sociales aumentaron de un 14% a un 49,4% entre los años 2012 y 2013, lo que denota –en un corto período de tiempo- un incremento exponencial de la amenaza que significa este delito.

En el año 2014, la PDI recabó 177 denuncias por el ilícito de usurpación de nombre en el escenario de Internet y de las redes sociales –considerando correos electrónicos, Facebook y Twitter, entre otros[482]-, de tales reclamos, 54 obtuvieron resultados gracias a la investigación de la Brigada del Cibercrimen, mientras que en 123 caso no se pudo establecer que se haya cometido el injusto, esto obtenido de las investigaciones informadas a la fiscalía en el mismo año[483].

[482] Según la entrevista realizada al Comisario Santiago David Núñez de la Brigada de Cibercrimen de la Policía de Investigaciones, la red social con más denuncias por el delito de usurpación de nombre es Facebook.
[483] Véase gráfico N°4 del punto I del anexo.

En relación a las querellas por el delito de usurpación de nombre, y en virtud de la información entregada por el Ministerio Público, podemos establecer que entre los años 2013 y 2014, son 24 las causas que finalizaron a través de un término facultativo, 8 las causas que se agregaron a otros casos y 11 en las que se optó por una salida judicial. Dentro de estas últimas, sólo 3 arribaron a una sentencia definitiva condenatoria, mientras que la mayoría concluyeron en acuerdo reparatorio, sobreseimiento definitivo y suspensión condicional del procedimiento[484].

De lo anterior, se puede traducir que la mayoría de los casos de suplantación de identidad son resueltos a través de una salida alternativa y no cumpliendo el imputado una pena privativa de libertad, lo que demuestra que no existe justificación detrás del aumento en un grado del presidio ya establecido más la multa de 5 U.T.M. a 30 U.T.M., como bien solicita el proyecto, puesto que en la realidad ni siquiera llega a concretarse la pena de cárcel que estipula actualmente el artículo 214 del Código punitivo.

[484] Véase figura N° 2 del punto II del anexo.

Reanudando la discusión referente al impacto, estimamos que en el caso de una usurpación en los términos de la norma estudiada, los efectos que produce en el mundo físico son perceptibles y tienen una expansión delimitada, por cuanto no pueden abarcar más de lo que es apreciable por nuestros sentidos. Lo que puede observarse, por regla general, en el hecho de que una persona use el nombre o la firma de otra, sin embargo, es difícil que la suplantación se extienda al aspecto físico de la misma, su voz u otras características distintivas de la identidad. Mientras que en un entorno informático, la identidad digital es más fácil de reproducir en todos sus elementos por quien no está autorizado para ello, por lo que dichas consecuencias son inmensurables[485], no sólo en cuanto a la suplantación de identidad misma, sino también respecto de los delitos conexos –como

[485] Según lo planteado por el Comisario Santiago David, de la Brigada del Cibercrimen de la PDI, cuando se utiliza el nombre, la firma o bien las fotografías de una persona en el entorno virtual, estos pasan a ser asequible por todo aquel que tenga Internet a su disposición, pudiendo terminar en múltiples sitios, demostrando que los efectos de una acción en la Red son incalculables.

ocurre con la estafa, la calumnia o injuria- que se sirven de aquella para ejecutarse[486].

Otro aspecto a considerar es la facilidad que existe en Internet para mermar la existencia –y a su vez la reputación- de cualquier individuo, y ya no sólo que esta afectación produzca consecuencias en el mundo virtual, sino que también interfiera en la vida real, puesto que es un hecho que la identidad personal se vive simultáneamente en la Web. Hoy, más que nunca es innegable que la vida cotidiana gira en torno a las nuevas tecnologías y las redes sociales, determinando que el límite entre una y otra realidad es cada vez más difuso, por lo que las conductas delictuales en el ámbito de las comunidades digitales, ya no sólo lesionan intereses del ciudadano Red (citizennet), sino que producen un impacto en la persona como tal, en todos y cada uno de sus aspectos[487].

[486] Esto, porque muchas de las secuelas de estos ilícitos son desconocidas para la víctima, y pueden reproducirse fácil y rápidamente gracias al tráfico de información que se da en la Red.

[487] Según Capeller "Se ha sugerido, incluso, que las conductas criminales en el ámbito de las comunidades virtuales, lesionan intereses del ciudadano en cuanto miembro de la comunidad virtual (citizennet), refiriendo entonces el análisis del impacto de las conductas criminales sólo a la afectación de las pautas de comportamiento como ciudadano red". Sin embargo en nuestra

Si hoy existen estos problemas de usurpación de identidad con el número de redes sociales que conocemos, debemos estar seguros que en el futuro este delito seguirá cometiéndose, y en virtud de la poca probabilidad de que exista un retroceso en el desarrollo de estas plataformas –ya que en lo que respecta a la Web no hay punto de retorno-, hace necesaria la utilización de instrumentos de control de riesgos y prevención en relación a este tipo de ilícitos informáticos, los que debieran germinarse primeramente "en los usos que la comunidad de usuarios conforma con su práctica diaria"[488].

Debemos recordar que "la noción de riesgo es siempre inherente al interés que trata de salvaguardarse y, consecuentemente, sólo una vez definido el interés puede delimitarse el nivel de riesgos que el mismo puede soportar y aquellos cuya peligrosidad para su mantenimiento requieren técnicas de intervención jurídica, no siempre, ni necesariamente, de carácter

---

opinión, las cosas han cambiado en los últimos 14 años, siendo actualmente el ciudadano Red la misma persona que el ciudadano común y corriente, viviendo una única vida en ambos espacios y radicándose recíprocamente las consecuencias de las acciones que se realicen en uno y otro. CAPELLER, W. 2001. Not such a neat net. pp. 5-6. En: MORALES. Delincuencia informática. Op. Cit. p.186.

[488] Ibídem. pp. 188 y 189

penal"[489]. Dicho esto, estimamos que el artículo 214 del Código Penal, en su redacción original, ampara perfectamente el bien jurídico protegido –y por consiguiente soporta el riesgo de su afectación- del derecho a la identidad, cuando la suplantación de ésta se da en las redes sociales, siendo innecesaria una modificación a la norma, puesto que si bien ha aumentado este delito y existe el peligro potencial de que se siga incrementando su ejecución, no se justifica hoy en día la creación de un precepto penal especial que señale que tales injustos pueden cometerse en Internet.

Esto, "pues, unas veces, las normas penales son suficientemente amplias para acoger lo que no son sino manifestaciones más sofisticadas de lo que ya se conoce y otras tantas, en cambio, el principio de legalidad no permite una extensa apertura hacia la absorción de nuevos comportamientos difícilmente conciliables con el ámbito de tutela de la norma; y no son pocas aquellas en las que la novedad de los intereses a tutelar y la violencia de los ataques –confirmado en el estudio criminológico- reclaman la presencia de normas penales específicas"[490]. Tal idea reafirma nuestro

[489] Ibídem. p.188.
[490] Ibídem. pp. 186 y 187

pensamiento; primero, porque el artículo 214 es competente para resguardar una manifestación más particular de la usurpación de identidad; segundo, porque no existe novedad en los intereses a proteger, ya que la identidad personal y la identidad digital en la mayoría de los casos es una sola, y se ve amparada por igual bajo el precepto existente; y tercero, porque la violencia de los ataques no detenta una envergadura tal que requiera de una tipificación nueva y más estricta.

CAPÍTULO V: FACEBOOK Y TWITTER ANTE LA USURPACIÓN DE IDENTIDAD.

Las redes sociales son plataformas que tienen como principal finalidad el compartir información, creando con ello una comunidad de internautas que exponen su identidad en el mundo virtual para ser reconocidos por otros y así relacionarse vía Internet. Tal cometido conlleva el peligro de que dicha información que se publica sea utilizada por terceros de forma indebida o malintencionada, y sin la autorización de su propietario, lo cual muchas veces se da bajo el supuesto de la suplantación de identidad.

En virtud de las posibles consecuencias perjudiciales que se siguen de la comunicación a través de estas nuevas plataformas y la usurpación de identidad, es necesario que revisemos cómo Facebook y Twitter se enfrentan a este fenómeno en crecimiento.

1. Políticas de Facebook

1.1.Normas relativas a la usurpación de identidad

La declaración de derechos y responsabilidades de Facebook, junto a las políticas de privacidad y de uso de datos, o también llamadas "Condiciones", constituyen el contrato que regirá la relación entre la plataforma y quienes accedan a ella. Este conglomerado de normas detenta la calidad de contrato de adhesión, puesto que los términos del contrato se establecen por una de las partes, se aceptan por la otra para su perfeccionamiento, y que pueden ser modificados sólo por quien lo dispuso, en este caso Facebook[491].

Dichas condiciones forman un conjunto de variadas reglas que persiguen la cooperación de los usuarios con la finalidad de evitar diferentes abusos y delitos que se posibilitan con el uso de esta red social, a lo que nosotros sólo haremos referencia a aquellas que conciernen a la problemática que representa la usurpación de identidad.

[491] FACEBOOK. 2015. Condiciones y políticas de Facebook. Todo lo que necesitas saber, en un solo sitio. [en línea] https://es-es.facebook.com/policies/ [consulta: 17 de mayo de 2015]

En la declaración de derechos y responsabilidades, en el segmento nombrado “Seguridad”, la red asegura que si bien toman todas las medidas para que Facebook sea un sitio seguro, no lo garantizan, solicitando además el compromiso de sus usuarios a no compartir ni utilizar información de relevancia, tanto propias como ajenas -tales como claves de acceso de correos electrónicos, datos financieros, entre otras-. Sumado a la prohibición de recopilar información o contenido de otros usuarios y el uso de medios automáticos para su acceso[492].

En cuanto al tópico de “Seguridad de cuenta y registro”, Facebook hace hincapié en que los miembros deben proporcionar sus nombres e información reales, lo que iría asociado a cumplir con ciertas conductas como: no crear más de una cuenta personal o perfiles de contenido falso, no transferir la propia cuenta, ni compartir la contraseña o permitir que otro acceda al sitio a través de la cuenta personal que se tiene. Con esto, y en virtud de la potestad que detentan los administradores del servicio para

[492] FACEBOOK. 2015. Declaración de derechos y responsabilidades. [en línea] <https://es-es.facebook.com/legal/terms> 3. Seguridad. [consulta: 17 de mayo de 2015]

determinar la estructura de gestión del mismo, Facebook se reserva el derecho a inhabilitar cuentas de personas que hayan infringido alguna de estas reglas y, en el caso de seleccionar ellos un nombre de usuario o identificador similar para una cuenta o página determinada, tienen la facultad para eliminarlo o reclamarlo de considerarlo oportuno[493].

Las normas recién mencionadas tienen como objetivo la protección de los derechos de quienes son parte de esta comunidad online, a lo cual esta red hace referencia específicamente en el título "Protección de derechos de otras personas" de la misma declaración, donde se exige que los propios usuarios no publiquen contenido o realicen alguna acción en Facebook que infrinja o viole derechos de otros o cualquier ordenamiento legal, no publiquen documentos de identificación o información financiera de nadie en el sitio, ni recopilen información de otros usuarios. De ser así, los

[493] FACEBOOK. 2015. Declaración de derechos y responsabilidades. [en línea] <https://es-es.facebook.com/legal/terms> 4. Seguridad de la cuenta y registro. [consulta: 17 de mayo de 2015]

administradores podrán retirar cualquier contenido que caiga en tales conductas prohibidas[494] [495].

Con el objeto de cumplir con un cierto criterio de privacidad en Facebook, el sitio mantiene la información de las cuentas en un servidor protegido con un firewall[496], utilizan medidas sociales y automatizadas para aumentar la seguridad -como el análisis de actividad de cuenta para observar comportamientos fraudulentos o anómalos-, y se guarda el derecho de eliminar contenido inadecuado o ilegal, y de suspender o desactivar cuentas en caso de constatar violaciones a la declaración analizada

[494] FACEBOOK. 2015. Declaración de derechos y responsabilidades. [en línea] <https://es-es.facebook.com/legal/terms> 5. Protección de derechos de otras personas. [consulta: 17 de mayo de 2015]

[495] Por otra parte, las normas de la política de privacidad de Facebook -que tienen relación con el resguardo de nuestra identidad respecto del uso no autorizado por otros- se basan principalmente en la responsabilidad del usuario, ya que en él recae la administración de la información que comparte, a través de la "configuración de privacidad", siendo éste quien decide qué datos y contenido desea compartir y cómo distribuirlo.

[496] Según la compañía Windows, firewall es un "software o hardware que comprueba la información procedente de Internet o de una red y, a continuación, bloquea o permite el paso de ésta al equipo, en función de la configuración del firewall", lo que puede ayudar a impedir que hackers o software malintencionado obtengan acceso al equipo a través de internet. En: MICROSOFT. Qué es un Firewall. [en línea] <http://windows.microsoft.com/es-mx/windows/what-is-firewall#1TC=windows-7> [consulta: 20 de mayo de 2015]

anteriormente. Sin embargo, esta red social no promete inmunidad a los riesgos, afirmando que "ninguna medida de seguridad es perfecta ni impenetrable", que no pueden "controlar las acciones de otros usuarios con los que compartas información" ni "garantizar que sólo vean tu información personas autorizadas", incluso, establecen que no pueden "garantizar que la información que compartas en Facebook no pase a estar disponible públicamente". Por lo que, en consecuencia, dicha red no se hace responsable de acciones de terceros que burlen el sistema de configuración de privacidad[497] [498].

En resumen, Facebook establece que no se podrá usar esta Red para cometer actos ilícitos, engañosos, malintencionados o discriminatorios. De lo anterior, se entiende claramente que no se permite que exista

[497] FACEBOOK. 2009. Política de privacidad de Facebook. [en línea] <http://www.facebook.com/note.php?note_id=+322317115300> [consulta: 20 de octubre de 2013]

[498] En cuanto a la política de uso de datos de la misma red social, respecto de la seguridad que ofrecen, se reitera que se hace todo lo posible para mantener a salvo la información de los usuarios, pero que se requiere ayuda y compromiso de los mismos para que no existan problemas de seguridad a futuro, de los cuales Facebook tampoco se hace responsable. En: FACEBOOK. 2015. Política de uso de datos. [en línea] <https://es-es.facebook.com/full_data_use_policy> [consulta: 17 de mayo de 2015]

suplantación de identidad en esta plataforma, aunque la realidad dista bastante de esta expectativa, en cuanto dicho problema se da en esta red social más que en otras.

1.2.Cómo denunciar una suplantación de identidad

En el caso de cometerse una infracción a su declaración de derechos y responsabilidades, Facebook cuenta con un sistema de denuncias a través del mismo sitio Web, donde puede darse aviso que se está siendo víctima de alguna trasgresión o que se conoce la situación de un tercero que se ve afectado por una conducta inadecuada.

En relación a la usurpación de identidad, la red social da la posibilidad de denunciar cuentas falsas –propias, de amigos o de personajes públicos-, ya sean perfiles que finjan ser una persona determinada, utilicen sus fotos, muestren un nombre falso o sencillamente no correspondan a una persona real.

La denuncia de una cuenta falsa, utiliza un procedimiento estándar, el cual consiste en los siguientes pasos: primero, ir a al perfil del impostor; segundo, hacer click sobre la foto de portada (cover photo) y seleccionar la opción "reportar"; y tercero, seguir las instrucciones para completar la denuncia y seleccionar "Enviar"[499].

Dada la eventualidad de ser suplantado en Facebook por un extraño no teniendo cuenta en la misma red social, puede enviarse una solicitud en la misma página de "ayuda para ordenadores", donde aparecerán las siguientes opciones: "Alguien está usando mi dirección de correo electrónico en su cuenta"; "Alguien ha creado una cuenta para mi empresa u organización"; o "Alguien ha creado una cuenta que se hace pasar por mí o un amigo", debiendo seleccionarse la que mejor se ajuste a la situación personal del afectado[500].

[499] Para el caso de las denuncias por suplantación de algún amigo debe especificarse que se está abogando por otra persona, seleccionando las opciones "Esta persona se está haciendo pasar por" o "Alguien que conozco", y escribiendo el nombre del amigo respectivo. En: FACEBOOK. 2015. Ayuda para ordenadores. Reporta una violación. [en línea] <https://es-es.facebook.com/help/263149623790594/> [consulta: 17 de mayo de 2015]

[500] Ídem.

Es importante destacar que las denuncias tienen carácter anónimo, por lo que, cuando se contacta a la persona responsable no se le comunica ningún tipo de información sobre el denunciante, como tampoco se le informa al tercero afectado en caso de estar denunciando la situación de algún amigo[501].

Recibida la denuncia por Facebook, ésta es estudiada por sus administradores, teniendo ellos la total discrecionalidad para eliminar la cuenta o contenido que ha sido denunciado, siempre y cuando infrinja las "Condiciones" de Facebook, entendiéndose con ello que no toda denuncia dará pie a la eliminación de la información con la que se tenga problema.

El estado de las denuncias por infracción a las "Condiciones" del sitio puede ser comprobado en el "panel de ayuda" –que se encuentra en la barra lateral derecha de los "Ajustes de privacidad y herramientas o Privacy Settings and Tools", del módulo "Atajos de privacidad o Privacy shortcuts"-, el cual sólo puede verse por cada usuario en su propio perfil. En

[501] Ídem.

el panel de ayuda se puede obtener más información sobre las políticas de Facebook, consultar si se ha llevado a cabo una acción a consecuencia de la denuncia y cuál es la decisión que se ha tomado respecto del reclamo[502].

2. Políticas de Twitter

2.1. Normas relativas a la usurpación de identidad

La plataforma Twitter, como ya lo hemos establecido, tiene por objeto principal proporcionar un servicio donde las personas puedan descubrir información desde fuentes de interés y compartir su propio contenido con otros. De esto, se infiere que cada usuario tiene un derecho de propiedad sobre la información que sube a la red y, en consecuencia, es responsable de la misma[503].

---

[502] Además, de haber denunciado algo por equivocación se podrá cancelar la denuncia, mientras no haya sido revisada por la administración de la red, lo que se lleva a cabo a través del "panel de asistencia" de la configuración de la cuenta. En: FACEBOOK. 2015. Ayuda para ordenadores. Reporta una violación. Ídem.

[503] TWITTER. 2014. Condiciones de servicio. [en línea] <https://twitter.com/tos> [consulta: 20 de febrero de 2014]

Twitter, si bien determina que la red social no vigilará de manera activa ni censurará el contenido expuesto por sus usuarios -en virtud de los principios del derecho de propiedad y la responsabilidad que se tiene sobre los propios tweets-, crea un conglomerado de normas, más conocidas como "Reglas de Twitter" y "Condiciones de Servicio", que cumplen con los requerimientos legales y que sólo procederán en situaciones de violencia o amenaza, de abusos y spam, de suplantación de identidad, de uso ilegal del sitio, o donde se infrinja derechos de autor o marcas comerciales, entre otras[504].

A continuación, revisaremos la postura de Twitter respecto de variados temas que pudieran tener relación con la problemática de la usurpación de identidad, a través de la exposición de algunas de sus políticas.

En primer lugar, es esencial que destaquemos que Twitter establece derechamente una "Política de suplantación de identidad", donde determina

[504] TWITTER. Centro de ayuda. 2014. Las reglas de Twitter. [en línea] <https://support.twitter.com/groups/56-policies-violations/topics/236-twitter-rules-policies/articles/72688-las-reglas-de-twitter> [consulta: 20 de febrero de 2014]

que “las cuentas de Twitter que finjan ser de otra persona o entidad con el fin de confundir o engañar”[505] se considerarán una conducta infractora de las normas de este sitio, lo cual dará pie a su suspensión permanente. Debemos enfatizar que las cuentas con nombres de usuario iguales o de apariencia similar no infringen de forma automática esta política, puesto que de compartirse el nombre, pero ningún otro elemento en común y de indicarse claramente que no se asocia ni relaciona una cuenta determinada a otro individuo de nombre similar, se entiende que no existiría usurpación de identidad, ya que no existiría la intención de “retratar a otra persona de forma engañosa o confusa”[506].

Esta limitación se relaciona directamente con la “Política de cuentas de parodias, comentarios y admiradores”, que basados en la libertad de expresión y la creatividad de los miembros de Twitter, permite que los mismos creen cuentas de este tipo, en las cuales se deberá precisar –en el lenguaje a elección y que estimen conveniente los usuarios- que detentan tal

[505] TWITTER. Centro de ayuda. 2014. Política de suplantación de identidad. [en línea] <https://support.twitter.com/articles/72692-politica-de-suplantacion-de-identidad> [consultas: 20 de febrero de 2014]
[506] TWITTER. 2014. Centro de ayuda. Política de suplantación de identidad. Ídem.

motivación[507], con lo que podrán desarrollarse libremente y sin problemas. Sólo en el caso de que las cuentas con este propósito tengan una clara intención de engañar o confundir a otros, o conduzcan a malas interpretaciones, y no se alineen con las buenas prácticas, serán consideradas como casos de suplantación de identidad, y por tanto, quedarán sujetas a la política respectiva y serán susceptibles de suspensión[508].

Por otro lado, y en cuanto a aquella información privada y confidencial publicada en las cuentas, que puede ser captada por terceros sin autorización, y acarrear eventualmente una suplantación de identidad, Twitter establece que se considerarán una infracción a su normativa.

---

[507] Para reflejar claramente que el creador de la cuenta no es la misma persona o entidad que es sujeto de la parodia o comentario, Twitter recomienda que, tanto el nombre de usuario como el nombre en el perfil y la biografía no sean idénticos al de la persona objeto de la cuenta, debiendo tener siempre un calificativo tal como "no soy", "falso", "admirador", “cuenta de juego de rol” o “no estamos afiliados con…”. Y que las comunicaciones con otros no sean de carácter falaz, no estando permitido mandar mensajes haciéndose pasar por otra persona o celebridad.

[508] TWITTER. Centro de ayuda. 2014. Política de cuentas de parodias, comentarios y admiradores. [en línea] <https://support.twitter.com/groups/56-policies-violations/topics/236-twitter-rules-policies/articles/371626-politica-de-cuentas-de-parodias-comentarios-y-admiradores> [consulta: 20 de febrero de 2014]

Dentro de esta información sensible se encuentran, enunciadas por la red social a modo de ejemplo: la "información de tarjetas de crédito, números de la seguridad social u otros documentos nacionales de identidad, direcciones o ubicaciones que se consideran y se tratan como privadas, números telefónicos privados, no públicos y direcciones de correo electrónico personales, no públicas" [509]. A lo que podríamos sumar, siguiendo la lógica de que tales datos deben ser secretos para limitar su publicación, las claves de acceso a correos electrónicos y cuentas bancarias[510].

En lo que respecta a la información que se comparte -relacionado a la privacidad que se solicita de la plataforma-, Twitter recomienda que los

[509] TWITTER. Centro de ayuda. 2014. Información privada publicada en Twitter. [en línea] <https://support.twitter.com/groups/56-policies-violations/topics/236-twitter-rules-policies/articles/20170167-informacion-privada-publicada-en-twitter> [consulta:]

[510] Es relevante exponer que no todas las publicaciones de este tipo de contenido constituirán una infracción, en cuanto a que, si la información que se reclama privada al publicarse en Twitter ha sido expuesta en otro sitio online de forma previa, no se infringen las reglas del sitio. Y que de publicarse información ajena, debe detentarse documentación que indique que se tiene "autorización para actuar en nombre de la persona cuya información confidencial ha sido publicada". En: TWITTER. 2014. Centro de ayuda. Información privada publicada en Twitter. Ídem.

usuarios sean quienes controlen su propio contenido; ya sea a través del módulo "Ajustes", descansando en la postura "Think before you tweet", o mediante la petición al usuario que esté publicando información de terceros que remueva el contenido indebido, y –de no ser eficaces ninguna de estas medidas- reportar la respectiva infracción[511]. Esto, en virtud principalmente de los principios rectores de esta red social, que son el derecho de propiedad sobre el contenido que se comparte a través de los tweets y de la responsabilidad que surge de este derecho, mencionado anteriormente[512].

[511] TWITTER. Centro de ayuda. 2014. Protecting your personal information. [en línea] <https://support.twitter.com/articles/18368> [consulta: 20 de febrero de 2014]

[512] A propósito de lo anterior, la "Política de apropiación de nombres" establece que aquella conducta está prohibida por las reglas de Twitter, y que dicha Red no liberará nombres de usuarios inactivos o expropiados, salvo en casos de violación a leyes de marca registrada. En el caso de que una cuenta "no ha tenido actualizaciones, ni imagen de perfil, y no hay una intención de inducir a error, esto generalmente significa que no hay apropiación de nombres ni suplantación de identidad". Tanto lo anterior, como "los intentos de vender, comprar o solicitar otras formas de pago a cambio de nombres de usuario" se consideran infracciones a las condiciones para participar de Twitter, pudiendo ocasionarse la suspensión permanente de la cuenta determinada. En: TWITTER. Centro de ayuda. 2014. Política de apropiación de nombres. [en línea] <https://support.twitter.com/groups/56-policies-violations/topics/236-twitter-rules-policies/articles/72706-politica-de-apropiacion-de-nombres> [consulta: 20 de febrero de 2014]

Entonces, en resumen, existe la posibilidad de que los administradores de esta plataforma dejen en suspenso, pongan fin al uso de ciertas cuentas o, incluso, dejen de proveer alguno, todos o parte de los Servicios ofrecidos, ya "en cualquier momento y por cualquier razón, incluyendo, y sin limitación alguna, para aquellos casos en los que razonablemente"[513] se estime que: se han infringido las condiciones de Twitter; se genere a la red social un cierto riesgo o exposición legal; o si resulta que la prestación de los servicios ya no es comercialmente viable para determinada persona[514]. Y al ser la suplantación de identidad una de las principales materias dignas de protección para la comunidad online Twitter, se entiende que la misma sea causa suficiente para la eliminación de cuentas que infrinjan dicha política, siempre teniendo en cuenta que tal usurpación debe cumplir con los requisitos –fingir ser otra persona o entidad con el fin de confundir o engañar a terceros- que la conformen como tal.

2.2. Cómo denunciar una suplantación de identidad

[513] TWITTER. 2014. Condiciones de servicio. Op. Cit.
[514] Ídem.

El problema de la usurpación de identidad es una de las mayores preocupaciones a las que se enfrenta Twitter con su conjunto de políticas, mas éstas por sí solas no son suficientes, por lo que la plataforma ha creado un sistema para reportar infracciones a las mismas.

La denuncia de suplantación de identidad de un individuo o usurpación de marca en Twitter, deberá hacerse por la persona cuya identidad está siendo suplantada o por alguien que esté autorizado legalmente para actuar en su nombre, caso en el cual deberá proporcionar pruebas de tal autorización, ya que de no ser el representante legal de la víctima, no se tomarán acciones respecto de la solicitud de eliminación de cuenta[515].

El reporte se realiza a través de la propia cuenta, seleccionando el módulo "Ayuda", que se encuentra en "Ajustes o Settings" –ubicado en la parte superior derecha de la página personal-, que guiará a la persona al "Centro de ayuda" de Twitter, donde hay varios links que conducen a la

[515] TWITTER. Centro de ayuda. 2014. Cómo reportar las cuentas de suplantación de identidad. [en línea] <https://support.twitter.com/articles/20170183-como-reportar-las-cuentas-de-suplantacion-de-identidad> [consulta: 20 de febrero de 2014]

página de “Reportar una cuenta por suplantación de identidad”[516]. Aquí aparecerá un formulario, donde el afectado o quien abogue por él deberá rellenar con la opción “Mi identidad está siendo suplantada”, pudiendo incluir “una descripción detallada de la información de la cuenta que muestra una clara representación de su identidad real” –ya sea la información de la biografía, enlaces a Tweets o enlaces a contenido reproducido-, pudiendo incluso denunciar quien no tenga una cuenta en Twitter[517].

De recibir Twitter un reporte válido, el sitio estudiará si se trata de una usurpación de identidad, comprobando la identificación de la persona que presenta la denuncia y las cuentas que potencialmente infrinjan la política respectiva, o no cumplan con la política de parodias y comentarios, de lo cual, si resulta que existe una infracción a las reglas de Twitter, se

[516] TWITTER. Centro de ayuda. 2014. Reportar una cuenta por suplantación de identidad. [en línea] < https://support.twitter.com/forms/impersonation> [consulta: 20 de febrero de 2014]

[517] TWITTER. 2014. Centro de ayuda. Cómo reportar las cuentas de suplantación de identidad. Ídem.

suspenderán las cuentas responsables o se les solicitará que realicen las correspondientes modificaciones[518].

Asimismo, en virtud de lo directamente vinculado que se encuentra de la usurpación de identidad, creemos importante exponer sobre el reporte de las infracciones por publicación de información privada en Twitter. Este tipo de denuncias, para que sean procesadas, deben ser presentadas por el individuo cuya información está publicada o por su representante legal, sin que sea necesario que el afectado posea cuenta de Twitter.

Para realizar el reporte, y de forma similar a los casos de suplantación de identidad, se debe hacer click en el módulo "Ajustes" y luego en "Ayuda" -todo en la propia cuenta-, acción que conducirá a la página "Centro de ayuda", donde se debe seleccionar el link "Quiero reportar una infracción", para luego seleccionar el link "Acoso". Posteriormente, en el formulario de título "Estoy reportando a un usuario abusivo", deberá escogerse la opción "Un usuario de Twitter está publicando mi información privada", debiendo confirmar con ello que: "la información privada que contienen los tweets

[518] Ídem.

reportados le pertenece, y que no ha publicado la información reportada en ningún otro sitio de Internet" [519] . Además, el denunciante deberá proporcionar: los enlaces a los tweets que revelan su información privada; la confirmación de que la información sensible que contienen los tweets denunciados le pertenece; la confirmación de que no ha publicado la información denunciada en ningún otro sitio virtual; y la dirección de correo electrónico que utiliza para acceder a la plataforma[520].

Recibido el reporte de que se ha publicado información privada en Twitter -debiendo éste ser completo y válido-, la administración investigará la cuenta y los tweets denunciados, con lo que se revisará el lugar donde se ha publicado la información, y su calidad de verídicos, tomándose acciones sólo en el caso de que la correspondiente información no haya sido

[519] TWITTER. Centro de ayuda. 2014. Cómo reportar información privada publicada en Twitter. [en línea] <https://support.twitter.com/groups/56-policies-violations/topics/238-report-a-violation/articles/20170171-como-reportar-informacion-privada-publicada-en-twitter> [consulta: 20 de febrero de 2014]

[520] TWITTER. Centro de ayuda. 2013. Cómo reportar infracciones. [en línea] <https://support.twitter.com/groups/56-policies-violations/topics/238-report-a-violation/articles/108038-como-reportar-infracciones> [consulta: 28 de diciembre de 2013]

previamente publicada en otro sitio web, puesto que esto no constituiría una infracción a las políticas de la red[521].

3. Propuestas para proteger la propia identidad en las redes sociales

La protección de nuestra identidad virtual en las comunidades online, y potencialmente el resguardo de nuestra identidad en el mundo real, depende tanto de las medidas que toman los administradores de las redes sociales –con el fin de ofrecer un mejor servicio-, como de la conciencia que los usuarios tengan respecto de las mismas.

En cuanto a la responsabilidad que tienen las redes sociales, éstas, y en general todos los servicios ofrecidos en Internet, tienen el deber de informar al usuario, claramente y en lenguaje sencillo, sobre las condiciones de funcionamiento del servicio, y sobre el alcance y difusión de la información que el usuario aporte a la misma. Para esto, no puede incluirse en las condiciones de uso de la red social respectiva ninguna restricción al

[521] TWITTER. 2014. Centro de ayuda. Cómo reportar información privada publicada en Twitter. Op. cit.

ejercicio del derecho a la información que tiene el usuario.

Es necesario y obligatorio entonces, que se pongan a disposición de los usuarios todas las herramientas técnicas –debiendo éstas ser de fácil acceso- para que sean ellos quienes controlen, en todo momento, cómo quieren utilizar la red social y el grado de privacidad que deseen mantener en la misma[522].

Es de suma importancia mencionar que, cuando se decide ser parte de una de estas plataformas virtuales, el usuario debe dar su consentimiento expreso e inequívoco, el cual se otorga, por lo general, al final de la lectura del contrato de adhesión que aparece cuando completa su inscripción. Muchas veces, tal aceptación del usuario se adjunta sin siquiera mirar las condiciones de la red social determinada, conducta común y bastante perjudicial para el usuario, en cuanto fomenta la falta de control que se tiene sobre los propios perfiles y sobre el contenido personal que pueden

[522] INSUA., M. 2013. Suplantación de identidad en las redes sociales. [en línea] Insua Vidal Avogados. Blog. Febrero, 2014. <http://www.insuavogados.com/es/suplantación-de-identidad-en-las-redes-sociales> [consulta: 10 de mayo de 2015]

potencialmente utilizar los administradores de tales redes, ya que por desconocer cómo funciona la plataforma a la cual se está accediendo, podemos otorgar un mayor dominio de nuestros datos por parte de los propietarios de las redes sociales y otros terceros extraños.

La privacidad que esperamos sea protegida en las redes sociales, y con esto la seguridad de nuestra identidad, obedece principalmente a la gestión que nosotros mismos realizamos de la información personal que compartimos en éstas, puesto que la exposición de ciertos datos conlleva la peligrosidad de ser utilizados de forma malintencionada por otros. Para contrarrestar dicho peligro: los usuarios deben entender sobre el funcionamiento de la Red en la que participan; conocer las políticas de los servidores respectivos; controlar directamente la configuración de sus perfiles; y tener máximo cuidado respecto de la información que deliberadamente muestren en estas populares plataformas[523].

[523] Asimismo, es necesario que se forme una conciencia colectiva sobre el abuso que existe de las redes sociales y otros sitios web, que se erigen sobre la base de obtención de datos personales de los usuarios, puesto que inscribirse en un sinnúmero de comunidades online puede causar confusión respecto del contenido que compartimos en cada una de ellas, muchas veces perdiendo el rastro de lo que subimos a la red sobre nosotros, lo que puede

El exceso de información personal compartida, muchas veces se debe a que la gente se muestra más dispuesta a divulgar este tipo de información en las redes sociales por considerarlos círculos de confianza donde se comparte entre amigos, lo que generaría una familiaridad un tanto ficticia en la que no habría peligro en dicha exhibición. Esto, por supuesto, dista bastante de lo que sucede en la realidad, donde es común que los usuarios no sepan completamente quienes pueden acceder a sus perfiles, puesto que aceptan como amigos o seguidores a personas desconocidas o bien no saben que al proporcionar datos como: nombre, fecha de nacimiento y redes de amigos, entre otros, se revela más de lo que se imagina[524].

En base a lo anterior, podemos establecer que los riesgos a los que nos exponemos y "los límites de la privacidad varían de acuerdo con la persona

---

convertirse en un riesgo, sobre todo en relación al desconocimiento de las otras personas que también son parte de las mismas redes y pueden aprovecharse de lo que mostramos en nuestros múltiples perfiles.

[524] TECNOLOGÍA. Universia Knowledge Wharton. 2007. Las redes sociales online redefinen la privacidad personal. [en línea] Wharton University of Pennsylvania. Junio, 2007. <http://www.wharton.universia.net/index.cfm?fa=viewArticle&id=1730> [consulta: 15 de octubre de 2013]

y que esos límites están siendo probados por las redes sociales"[525]. Y es por esto que se hace necesaria la recomendación de algunas medidas que los usuarios pueden llevar a cabo, con el fin de que Facebook y Twitter sean más seguros, sobre todo en lo relacionado con nuestros datos sensibles.

Primero, el usuario debe preocuparse del buen funcionamiento de su computador personal y de la forma con que se enfrenta a estas plataformas, lo cual puede realizarse considerando lo siguiente.

- Mantener el sistema operativo actualizado para evitar vulnerabilidades en la seguridad del computador.

- Contar con soluciones antivirus activas y actualizadas; para evitar la instalación o ejecución de programas maliciosos, que puedan obtener una mayor cantidad de datos sensibles del usuario.

- Utilizar algún gestor de correo electrónico con funciones anti-spam que borre directamente del servidor los correos no deseados.

[525] Ídem.

- Usar contraseñas seguras; con una mayor cantidad de dígitos, preferentemente alfanuméricas, y que contengan mayúsculas y minúsculas.

- Guiarse siempre por el sentido común, que es la mejor herramienta de protección frente a cualquier tipo de ataque a la seguridad[526].

Además, el usuario que ya participa de alguna o varias redes sociales debe tomar ciertas medidas que lo ayuden a gestionar mejor su actividad social en Internet. Aquí algunas sugerencias.

- Leer consciente y regularmente las declaraciones de reglas y diferentes políticas de las redes sociales a las que se pertenece, y no aceptar sus condiciones sin siquiera reparar en ellas. Es importante recordar que éstas son contratos de adhesión unilaterales que pueden ser alterados, en cualquier momento, por los dueños de los sitios web respectivos, por lo que hay que estar siempre bien informado.

[526] INSUA., M. 2013. Op. Cit.

- Considerar el uso de nombres de usuario y contraseñas diferentes para cada perfil.

- Variar las contraseñas y cambiarlas regularmente.

- No dar el nombre de usuario ni la contraseña a terceros.

- Minimizar el uso de información personal en los perfiles, sobre todo si puede ser utilizada por otros para acceder a las cuentas personales de distintos sitios web o al propio correo electrónico, como por ejemplo: la información que se pide para verificar la contraseña.

- Contestar con otras contraseñas las preguntas de seguridad que se requieren para verificar la contraseña de las respectivas redes sociales o del correo electrónico, en vez de contestarlas literalmente.

- Evitar completar datos en exceso, como fecha de nacimiento, lugar de residencia, dirección del domicilio, dirección de correo electrónico, entre otros.

- Nunca compartir números sociales de identificación, documentos de identificación oficial, ni información bancaria.

- Invitar y aceptar, para ser “amigos” en Facebook o “seguidores” en Twitter, sólo a conocidos que sean parte del propio círculo social, y evitar que “amigos de amigos” o extraños puedan ver el perfil.

- Preocuparse de lo que se publica en los propios perfiles y otras páginas de las redes sociales. Evitar contenido que exponga demasiado sobre sí mismo, que sea de carácter ofensivo o discriminatorio, o bien que pueda posteriormente ser usado en contra.

Y en caso de ser víctima del delito de usurpación de identidad, se recomienda seguir los siguientes pasos.

- Conservar un registro con todos los detalles de los trámites y documentación relacionada con la persona afectada.

- Comunicar e informar de la situación a toda empresa que reclame actividades crediticias o financieras realizadas en nombre de la víctima.

- Comunicar e informar de la situación a organizaciones encargadas de emitir documentación personal.

- Reportar y denunciar el delito de suplantación de identidad ante una entidad policial.

- Informar a su vez a la organización en que se tiene el perfil virtual (correo electrónico, red social, foro, entre otros).

- Intentar recuperar o, en su defecto, cerrar toda cuenta -real o virtual- que se considere comprometida por los delincuentes.

- Contar siempre con documentos físicos que respalden la identidad del afectado, ya sean partidas de nacimiento, documentos oficiales, declaraciones juradas, denuncias por escrito que se hayan hecho ante la autoridad policial, ante las entidades financieras, o ante las mismas redes sociales, etc.

Vistas algunas herramientas y medidas útiles para proteger la seguridad de nuestra identidad en las redes sociales, cabe concluir que tal amparo de nosotros mismos y nuestras vidas, dependen absolutamente del uso que hagamos de los servicios que Internet nos ofrece, siendo fundamental que se instaure la conciencia de que el ciberespacio no tiene límites y, por tanto, es imposible conocer a todos quienes tienen acceso a nuestra información personal, lo que conlleva intrínsecamente el peligro de que sea utilizada maliciosamente por terceros extraños.

<u>CAPÍTULO VI:</u> ANÁLISIS JURISPRUDENCIAL DE LA USURPACIÓN DE IDENTIDAD EN LOS TRIBUNALES CHILENOS.

Ya profundizado el estudio de la suplantación de identidad, tanto desde el punto de vista tradicional como aquel que se da en un contexto virtual, pasaremos a revisar una serie de causas, vistas por Tribunales nacionales, en que se ha reclamado por el delito de usurpación de nombre ya sea en el plano físico o en las redes sociales.

Respecto a los casos de usurpación de nombre que se desenvuelven en el mundo real –en su mayoría juicios donde se cometió un delito de mayor envergadura y el imputado al ser cuestionado por la policía da un nombre que no corresponde al propio, sino, por lo general, a algún familiar o persona conocida-, no existe un criterio unitario por parte de la jurisprudencia para determinar cómo se configura el delito, encontrándose ésta dividida en dos posturas.

Por un lado[527], se estima que el ilícito de usurpación de nombre, siguiendo lo planteado por la doctrina, es un delito de mera actividad, conformándose por la sola circunstancia de que el acusado en el caso concreto indique un nombre diferente al suyo, no siendo necesaria la concreción de un resultado específico[528].

Al efecto, los Tribunales que siguen esta línea argumentativa se basan principalmente en lo esbozado por el Profesor Garrido Montt, que señala que "el tipo penal objetivo se conforma por el simple hecho de usar el nombre y apellido de otra persona, siempre que pueda inducir a error en cuanto a la identidad de quien lo usa"[529], y que "el bien jurídico protegido es la vida en relación, y por ello la prohibición legislativa de la alteración del nombre, el cual es un delito de mera actividad, en el cual no es necesaria

[527] A modo de ejemplo, véase los siguientes fallos: TRIBUNAL ORAL EN LO PENAL DE TALCA. 21 de diciembre de 2005. RIT 101-2005; TRIBUNAL ORAL EN LO PENAL DE COPIAPÓ. 5 de julio de 2011. RIT 46-2011.
[528] TRIBUNAL ORAL EN LO PENAL DE COPIAPÓ. Op. Cit.
[529] Ídem.

la concreción de un resultado"[530]. Por lo que, si un individuo -al ser cuestionado por la policía respecto de sus antecedentes- se atribuye o arroga el nombre de una persona viva, existente y real incurre en la figura del artículo 214 del Código Penal[531] [532].

Por otro lado[533], existen Tribunales que consideran que "la sola circunstancia de haberse identificado con otro nombre luego de ser detenido, no implica que haya usurpado ese nombre, es decir, que se hubiera apoderado del derecho al nombre que legítimamente le pertenecía a

---

[530] Ídem.
[531] Ídem.
[532] Otro argumento que aduce el fallo en cuestión dice relación con la acepción de la palabra "usurpar" que ofrece el Diccionario de la Real Academia Española, que establece es "arrogarse la dignidad, empleo u oficio de otro, y usarlo como si fuera propios". En contraposición al significado de "ocultamiento" –puesto que la defensa persigue que se sancione la simple falta del artículo 496 Nº 5 del Código Penal, por ocultar el nombre y apellidos verdaderos a la autoridad que tenga la facultad para exigirlos- por el cual se entiende "esconder, tapar, disfrazar, encubrir a la vista, disfrazar la verdad". En: Ídem.
[533] A este respecto, véanse los fallos: SEXTO TRIBUNAL ORAL EN LO PENAL DE SANTIAGO. 24 de noviembre de 2010. RIT 592-2010; PRIMER TRIBUNAL ORAL EN LO PENAL DE SANTIAGO. 31 de diciembre de 2010. RIT 165-2010; TRIBUNAL ORAL EN LO PENAL DE VIÑA DEL MAR. 16 de septiembre de 2011; CORTE DE APELACIONES DE RANCAGUA. 12 de diciembre de 2011. ROL 359-2011; TERCER TRIBUNAL ORAL EN LO PENAL DE SANTIAGO. 01 de abril de 2014. RIT 46-2014.

otro, como se colige de la lectura de la definición que da el Diccionario de la Real Academia de la Lengua Española"[534], esto, porque tal "suministro carece de la entidad requerida para la configuración del delito de usurpación de identidad, desde que no es acompañada o dada en un contexto de verdadero convencimiento de poseerse esta otra identidad (…)"[535]. Esto más bien conformaría la simple falta del artículo 496 Nº 5 del Código punitivo, puesto que se cumplen los dos requisitos exigidos por el tipo penal, "a saber: a) que una persona oculte su nombre y apellidos, y b) que dicho ocultamiento lo haga a la autoridad que tenía derecho para exigir su manifestación"[536].

Aquí, para optar por sancionar con la falta mencionada y no el delito de usurpación de nombre, se establece que no puede configurarse éste último en tanto el bien jurídico es la vida en relación y, cuando el nombre y apellidos de otra persona se "usa" por un sujeto al que no corresponden, esto no tiene la aptitud para inducir a error respecto a la identidad, ya que a

[534] SEXTO TRIBUNAL ORAL EN LO PENAL DE SANTIAGO. Op. Cit.
[535] TERCER TRIBUNAL ORAL EN LO PENAL DE SANTIAGO. Op. Cit.
[536] SEXTO TRIBUNAL ORAL EN LO PENAL DE SANTIAGO. Op. Cit.

las autoridades les atañe su verificación, y hoy en día sí existen los medios técnicos y científicos adecuados para ello[537]. Incluso, este razonamiento apunta a que del artículo 214 del Código Penal "se infiere que la utilización del nombre por parte del agente importa atribuirse las características propias de un tercero, de sus demás atributos o de su personalidad, lo que no ocurre con la mera mención de un nombre que no le pertenece"[538], lo que se refuerza en la idea de que el artículo 496 Nº 5 del mismo texto legal "no hace distinción respecto de ocultar el nombre verdadero utilizando otro nombre falso o real"[539], bastando que se acredite tal ocultamiento para que se constituya la falta dispuesta por la norma.

A pesar de la discrepancia que existe en la jurisprudencia nacional relativa al delito de usurpación de nombre, aparece de manifiesto que cuando se configura dicho ilícito, éste abarca sólo el nombre –tanto el propio como el patronímico- y no así los otros elementos distintivos de la personalidad, aunque a veces los mismos jueces en la fundamentación de

[537] PRIMER TRIBUNAL ORAL EN LO PENAL DE SANTIAGO. Op. Cit.
[538] Gaceta Jurídica, Año 2011, Nº 372, páginas 253, 255 a 257. En: TRIBUNAL ORAL EN LO PENAL DE VIÑA DEL MAR. Op. Cit.
[539] CORTE DE APELACIONES DE RANCAGUA. Op. Cit.

las sentencias lo traten como usurpación de identidad, lo que acota claramente el alcance de la norma y su posible aplicación.

En cuanto al delito de usurpación de nombre que se ejecuta a través de Internet y las redes sociales, cabe revisar más atentamente una serie de causas que ilustrarán lo que ocurre en este contexto.

1. Zalaquett con Olguín[540]

En el año 2012, Pablo Zalaquett –en ese entonces alcalde de la comuna de Santiago- se vio afectado por una usurpación de nombre llevada a cabo a través de la red social conocida como Twitter, por parte de Matías Olguín Muñoz -estudiante universitario domiciliado en San Felipe-.

En la cuenta creada por este último, aquél se apersonaba como "@pablo_zalaquet", utilizando además la misma fotografía que el militante

[540] SÉPTIMO JUZGADO DE GARANTÍA. 19 de febrero de 2014. RIT N°16.848-2012.

de la Unión Democrática Independiente (UDI) tenía en su propio y auténtico perfil.

El ex edil expresó que: "Este plagio me trajo muchos problemas frente a la comunidad porque la gente creía que era yo insultando a todo el mundo diciendo frases realmente descabelladas en contra de todo: las personas, la democracia, de lo que venga"[541], motivo suficiente para acudir a la Justicia.

Formalizada la investigación, y exhortada la causa a San Felipe, el tribunal exhortado declara la suspensión condicional del procedimiento, el que cumplido y sumado al transcurso del plazo correspondiente sin que se haya revocado, deriva en la extinción de la acción penal y el sobreseimiento definitivo de la causa.

Este caso es prueba de lo establecido por los datos entregados por el Ministerio Público, los que determinan que la mayoría de las causas por

[541] EMOL. 2012. Zalaquett suplantado en Twitter: "El daño que me hizo fue muy grande". [en línea] Chile. <http://www.emol.com/noticias/nacional/2012/08/24/557221/detienen-a-joven-por-suplantar-a-alcalde-zalaquett-en-twitter.html> [consulta: 17 de marzo de 2015]

usurpación de nombre que llegan a Tribunales, y respecto de las cuales se desarrolla un juicio, arriban en salidas alternativas, y por lo mismo no cumpliendo los imputados pena de cárcel, siendo innecesario el aumento en un grado del presidio más la multa de 5 a 30 UTM que propone el proyecto.

2. Luksic con Ferrari[542]

El reconocido empresario Andrónico Luksic Craig, también en 2012, presenta una querella contra Rodrigo Ferrrari Prieto por el ílicito establecido en el artículo 214 del Código Penal, aduciendo los siguientes hechos: ser una persona de connotación nacional e internacional, por estar vinculado a variadas empresas que aportan a la economía del país; tener una reputación determinada por sus cualidades personales e intelectuales que no se condicen con la proyección que ha erigido el imputado en Twitter –a través de las cuentas "@andronicoluksic" y "@luksicandronico"-; ser utilizado su nombre patronímico para representar una imagen de él superficial y de habla vulgar, que confunde a sus supuestos "seguidores"

[542] SÉPTIMO JUZGADO DE GARANTÍA. Op. Cit.

respecto de su conducta personal y profesional; y por afectar éstas y otra cuenta falsa –"@losluksic"- a su vez a los hermanos de la víctima.

Para el Sr. Luksic, era verificable de la sola exposición de los hechos, la intención que tenía el querellado de apropiarse de su identidad, a través de la utilización indebida de su nombre y de la interacción con los demás usuarios de la plataforma digital. Sin embargo, el juez desestimó dicha postura, considerando que "no existe este ánimo subjetivo de usurpación y que los comentarios efectuados están efectivamente hechos a modo de sátira y de ironía, no existiendo gravemente un compromiso a la dignidad o al nombre de la persona involucrada" [543] , dictando finalmente el sobreseimiento definitivo de la causa.

Debemos tener presente que para que exista la usurpación de nombre, debe considerarse "el contexto de enunciación en el cual se realiza la acción de apropiación nominativa en cuestión, puesto que dicho contexto de enunciación determina la intención ilocutiva del sujeto que se apropia

[543] Extracto de audiencia de sobreseimiento, llevada a cabo el día 19 de abril de 2013. En: SÉPTIMO JUZGADO DE GARANTÍA. Op. Cit.

del nombre de otro, determina las expectativas y conocimientos del receptor de su mensaje, y en general determina todo aquello que está en juego en la enunciación misma y que constituye el contexto de la misma."[544]

En este caso, se aprecia con claridad que la intención del querellado era burlar a la persona de Andrónico Luksic y no hacerse pasar por él, lo que sumado al hecho de que la acción se formuló en el contexto de Twitter -que es una plataforma donde se permite la parodia-, la misma no tiene correspondencia con el bien jurídico protegido por la norma, ya que no habría una afectación sustancial a la "verdad personal" ni tampoco a la "vida en relación", por cuanto es absurdo pensar que habría confusión por parte de los otros usuarios respecto de la persona del famoso empresario, ya que los comentarios que se hacen a su nombre son irónicos y se le representa con una imagen –billetes cayendo del cielo- que es ridícula, y manifiestamente en tono de broma.

Aquí, la usurpación de nombre debió detentar un elemento subjetivo fraudulento, consistente en la apropiación de la identidad del querellante,

[544] MUÑOZ. Op. Cit. p. 159.

para que se determinara la comisión del delito, puesto que "lo que permite calificarla como fraudulenta es que ella persigue la formación de un engaño mediante técnicas comunicativas de todo tipo que reducen la posibilidad de descubrir la falsedad de dicha representación, a fin de lograr resultados en el plano ya sea de las interacciones jurídicas –la creación, modificación o extinción de derechos-, ya sea de las transacciones económicas, o bien de ambos."[545] Mas en el caso concreto, no hubo artimaña alguna y existía la posibilidad de captar fácilmente la falsedad de la cuenta, con lo que no hubo afectación y, por consiguiente, tampoco tipicidad.

3. Orrego con Bustamante[546]

C.O.L.[547], deduce querella por el delito usurpación de nombre contra M.B.L., por cuanto se crea una cuenta en Twitter utilizando el nombre y la imagen del primero, y señalando además el cargo público que detentaba en

[545] MUÑOZ. Op. Cit. pp. 159 y 160.
[546] DÉCIMO TERCERO JUZGADO DE GARANTÍA DE SANTIAGO. 4 de noviembre de 2009. RIT Nº 8.865-2009.
[547] Por petición de la Magistrada del Décimo tercer Juzgado de Garantía de Santiago, en adelante se utilizarán las iniciales de las personas involucradas para proteger su identidad.

aquel tiempo –mismos datos que el querellante usaba en su cuenta real-. En la querella se establece como argumento principal, la vulneración del artículo 214 del Código Penal, que tiene por bien jurídico a proteger la seguridad del tráfico jurídico y la fe pública, por considerarse que hubo una falta de fidelidad en los datos de identificación otorgados a través de esta plataforma virtual, y existiría una suplantación "de los medios legales y materiales de identificación de la persona a través de os cuales se fundamenta la creencia y relación en este sentido entre las personas que integran una comunidad social."[548]

En la audiencia de formalización de la investigación, celebrada el 19 de febrero de 2010, se aprobó la suspensión condicional del procedimiento respecto del imputado por el plazo de un año, por establecerse su autoría y la calidad de consumado del ilícito.

Este caso, al igual que los anteriores, viene a reafirmar el hecho de que las causas por usurpación de nombre terminan en su mayoría en salidas

[548] Extracto de la querella. En: DÉCIMO TERCERO JUZGADO DE GARANTÍA DE SANTIAGO. Op. Cit.

alternativas, por lo que el imputado cumplirá una pena menos drástica que la de presidio menor en su grado mínimo.

De los procedimientos mencionados, podemos establecer que es la víctima quien determina que la utilización de cualquier signo distintivo de la identidad personal por parte de un individuo al cual no pertenecen es suficiente para alegar que se ha incurrido en el simple delito dispuesto en el artículo 214 del Código Penal, extendiendo con ello el alcance de la norma –recordemos que en el plano físico sólo abarca el nombre-, sin embargo, al terminar estos juicios -en su gran mayoría- en salidas alternativas, no es posible precisar si los Tribunales estiman que para configurarse la usurpación de identidad sólo se requiere que proceda respecto del nombre o si, por el contrario, habría tal suplantación cuando haya una utilización indebida de cualquiera -uno o más- elementos característicos de la personalidad.

CONCLUSIONES

En virtud del trabajo desarrollado, podemos definir la identidad personal como el conjunto de características de la persona que sirven para su individualización en la sociedad, su identificación como única y diferente de los demás, que proviene de la concurrencia del ámbito biológico de la persona con la expresión social de la misma, lo que la dota, por tanto, de un espíritu cambiante que sólo responde a la potencialidad de la vida.

Es aquella proyección social de la identidad la que le otorga a ésta el carácter de bien jurídico a resguardar, en virtud de la susceptibilidad de ser ofendida por terceros, por lo que podemos determinar que el derecho a la identidad tutela la "verdad personal" y la "vida en relación", es decir, la cualidad de ser idéntico a sí mismo, que hace a los sujetos únicos e inconfundibles para el resto de los individuos, y que se representa a través de ciertos elementos distintivos: como es el nombre, la imagen, la firma, entre otros –a los cuales debe acotarse el ámbito de protección, y sólo

cuando exista una verdadera tergiversación de la identidad, con el fin de no crear una exaltación desmedida de la misma y su derecho-.

En cuanto a la identidad que desarrollamos en Internet, y más específicamente en las redes sociales -conceptualizada como el conjunto de características propias de un individuo o de un colectivo en un medio de transmisión digital-, ésta no responde a la materialidad predefinida por el cuerpo, sino más bien a la construcción o invención de la misma, sin parámetros que la limiten en su número –pueden tenerse varias personalidades en la Web- o respecto de su autenticidad –pueden crearse perfiles ficticios o donde se utilicen elementos distintivos que no correspondan a la persona que representan sino a otra que no ha autorizado tal uso-.

El ilícito de usurpación de identidad digital carece de un tratamiento legal y doctrinario en nuestro país, por lo que al estructurar los elementos para su configuración dentro de esta investigación, establecemos que: el sujeto pasivo podría ser tanto una persona natural como una persona jurídica; el sujeto activo sólo podría ser una persona natural; solo cabría

respecto de la acción de usurpar –excluyéndose la suplantación por omisión-, consistente en la apropiación de datos personales por medios tradicionales y digitales y la facultad adoptada de forma ilegal para utilizar dicha información con fines de usurpación de identidad; se exigiría como elemento subjetivo el dolo -la intención de apropiarse de la personalidad de otro-; y por último, no requeriría que la víctima sufra un daño, bastando el hecho de la suplantación.

Además es posible determinar que el bien jurídico protegido de la "verdad personal" y la "vida en relación", se extiende a su vez a los datos personales sensibles –que muchas veces incluyen claves de accesos a diferentes sistemas y redes-, que se comunican y circulan a través de la Web.

Hasta el momento el delito de usurpación de identidad se encuentra bajo el alero del artículo 214 del Código Penal, el cual es aplicado de forma extendida al mismo injusto cuando se ejecuta en las redes sociales, otorgando evidentemente la vía penal para que se reclame el ilícito. Sin embargo, también existe la posibilidad de que la víctima solicite una

indemnización en sede civil a raíz de la suplantación cuando ésta cumpla los elementos necesarios para la configuración de la responsabilidad extracontractual.

En relación al proyecto de ley que “modifica el Código Penal, con el propósito de sancionar la suplantación de identidad realizada a través de internet y redes sociales, ocasionando daños a terceros”, podemos establecer que contiene no sólo errores de forma, sino también de fondo: como no definir qué se entiende por “identidad”; estar basado en argumentaciones incoherentes; tener la intención sin sentido de aumentar la pena de presidio en un grado, cuando sólo se pretende que sobreviva la multa; y por sobre todo, no ser suficientemente claro respecto de la conexión que tiene Internet y las redes sociales con el verdadero objetivo de la inclusión del inciso segundo al artículo 214 del Código punitivo, que es sancionar a quien cause daños a terceros en virtud de una suplantación de identidad.

Por otro lado, en cuanto a la jurisprudencia nacional, vemos que existe un escaso número de causas por el delito de usurpación de nombre en su

vertiente tradicional, y aún menos por suplantación de identidad en las redes sociales -estando divididos los jueces en cuanto a la calificación jurídica que conlleva el uso no autorizado de nombre ajeno en ambos escenarios-, terminando la gran mayoría de ellas en salidas alternativas, esto por el bajo porcentaje de denuncias relativas a este injusto y la exigua cifra que llega a tribunales, sumado a la casi nula exposición de los jueces a la regulación de las nuevas tecnologías, ya que éstos limitadas veces se han visto enfrentados a causas desafiantes que permitan un cambio jurisprudencial.

Por todo lo anterior estimamos que, a pesar del progreso constante de la informática, aún no es necesario un cambio en la legislación penal nacional, como lo sugiere el Proyecto de Ley en cuestión, y que la suplantación de identidad queda perfectamente amparada bajo el artículo 214 en su texto original.

BIBLIOGRAFÍA

1. Libros, revistas, tesis, entre otros.

ABOSO., G. E. y ZAPATA., M. F. 2006. Cibercriminalidad y derecho penal: la información y los sistemas informáticos como nuevo paradigma del derecho penal: análisis doctrinario, jurisprudencial y de derecho comparado sobre los denominados "delitos informáticos". B de F, Montevideo. 221p.

ADMINISTRACIONES PÚBLICAS y nuevas tecnologías. 2005. Josefa Cantero “et al”. Lex Nova, España. 379p.

AGENCIA ESPAÑOLA de Protección de Datos., Instituto nacional de tecnologías de la comunicación. 2009. “Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales on line”. España. 158p.

ALVAREZ., C, L. 2011. Internet y derechos fundamentales. Editorial Porrúa, México. 283p.

APPIAH., A. 2007. La ética de la identidad. Traducido por Lilia Mosconi. Buenos Aires, Katz. 401 p.

ARCIERO., G. 2005. Estudios y diálogos sobre la identidad personal: reflexiones sobre la experiencia humana. Buenos Aires, Amorrortu. 339p.

AROCENA., G. 1997. De los delitos informáticos. Revista de la Facultad de Derecho, Universidad Nacional de Córdoba. Vol. 5, nº 1. pp. 41-60.

BARROS., E. 2007. Tratado de Responsabilidad Extracontractual. Editorial Jurídica de Chile, Santiago, Chile. 1230p.

BARROS., M. Y QUIROGA., V. 2011. El Periodismo en tiempos de Twitter. Nuevas formas y actores en el mundo de las comunicaciones

¿Pueden todos ejercer el oficio del periodista? Tesina para optar al grado de Licenciado en Comunicación Social. Santiago, Universidad Diego Portales, Facultad de Comunicación y Letras, Escuela de Periodismo. 65 h.

BIBLIOTECA CONGRESO NACIONAL. 2012. Informe sobre Delitos por Internet: Legislación Nacional elaborado por Juan Pablo Cavada Herrera, Asesor Técnico Parlamentario. Chile. 9p.

BORGARELLO, SUSANA E. Derecho a la imagen. Córdoba, Argentina : Marcos Lerner Editora, 1996. 62p.

CABEZAS L., P. y MOYA M., F. 2008. El derecho al anonimato del usuario de internet. Memoria para optar a la licenciatura en ciencias jurídicas y sociales. Santiago, Universidad de Chile, Facultad de Derecho. 189 h.

CASTELLS., M. 2001. La Galaxia internet. Areté, España. 317p.

CASTELLS., M. 2009. Comunicación y poder. Alianza Editorial, España. 679p.

CHINCHILLA S., C. 2004. Delitos Informáticos. Elementos básicos para identificarlos y su aplicación. Farben Grupo Editorial Norma. San José, Costa Rica. 1a. ed. 152p.

COLLANTES S., C. y GONZÁLEZ G., C. 2001. Identidad personal, identificación e identidad genética. Memoria para optar a la licenciatura en ciencias jurídicas y sociales. Santiago, Universidad de Chile, Facultad de Derecho. 317, [17] h.

CONSEJO GENERAL del Poder Judicial. 2006. Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad? Madrid, España. 373p.

CONTRERAS., S. 2012. La protección del honor, la intimidad y la propia imagen en Internet. Aranzadi, España, Thomson Reuters. 344p.

CONTRERAS., P. 2004. Me llamo Kohfam: identidad hacker: una aproximación antropológica. Barcelona, España, Gedisa. 166p.

CONSEJO GENERAL del Poder Judicial. 2001. Internet y Derecho Penal. Madrid, España. 663 p.

CREVILLÉN., C. 1995. Derechos de la personalidad. Honor, intimidad personal y familiar y propia imagen en la jurisprudencia. Actualidad, Madrid. 611p.

CRUZ D., J. 2006. Derecho penal y nuevas tecnologías. Aspectos sustantivos. Difusión jurídica y temas de actualidad, España. 341p.

DAFFAU G., F. 2008. Derecho a la privacidad, su contenido esencial, limitaciones y colisión con otros derechos fundamentales. Memoria para optar a la licenciatura en ciencias jurídicas y sociales. Santiago, Universidad de Chile, Facultad de Derecho. 145 h.

DE CUPIS, A. 1959. I diritti della personalitá. Dott. Antonino Giuffrè. Milano. Tomo I. 371p.

DE CUPIS, A. 1961. I diritti della personalitá. Dott. Antonino Giuffrè. Milano. Tomo II. 217p.

DERECHO Y TECNOLOGÍAS de la Información. 2002. Iñigo de la Maza Gazmuri “et all”. Universidad Diego Portales, Facultad de Derecho: Fundación Fernando Fueyo Laneri, Alfabeta Artes Gráficas. Santiago de Chile. 1a. ed. 497p.

DICCIONARIO DE LA Real Academia de la Lengua Española

DONOSO L., M. 2002. Bien Jurídico Protegido y Delincuencia Informática. Memoria para optar a la licenciatura en ciencias jurídicas y sociales. Santiago, Universidad Adolfo Ibáñez, Facultad de Derecho. 163 h.

DURAN B., M.A. 2010. Tratamiento del delito informático en Chile. Memoria para optar a la licenciatura en ciencias jurídicas y sociales. Santiago, Universidad de Chile, Facultad de Derecho. 178 h.

EUROPEAN COMMITTEE ON CRIME PROBLEMS. 1990. Computer-related crime. Recommendation No. R. (89) 9 on computer-related crime and final report of the European Committee on Crime Problems. Strasbourg. Council of Europe, Publishing and Documentation Service. 114p.

FERNÁNDEZ S., C. 1992. Derecho a la identidad personal. Buenos Aires, Astrea.

FIGUEROA Y., G. 2000-2001. El derecho de la persona como rama autónoma del derecho civil. Revista de Derecho y Humanidades (8): 57-63.

FIGUEROA Y., G. 2001. Derecho civil de la persona: del genoma al nacimiento. ;[prólogo de Agustín Squella Narducci] Santiago, Chile, Jurídica de Chile.

GONZALEZ K., C. D. 2012. Derecho a la propia imagen: esfera constitucional y legal del derecho a la propia imagen en Chile y en el derecho comparado. Memoria para optar a la licenciatura en ciencias jurídicas y sociales. Santiago, Universidad de Chile, Facultad de Derecho. 125 h.

GUERRA V., A. 2011. Delitos informáticos - Caso de estudio. [en línea] Tesis para obtener el grado de Maestro en Ingeniería en seguridad y tecnologías de la información. Instituto Politécnico Nacional, Escuela Superior de Ingeniería Mecánica y Eléctrica. México D.F. 124p. <http://www.repositoriodigital.ipn.mx/bitstream/handle/123456789/12653/TESIS.%20DELITOS%20INFORMÁTICOS-CASO%20DE%20ESTUDIO.pdf?sequence=1> [consulta:10 de diciembre de 2013]

GUEVARA M., A. 2012. Aproximación a la problemática de la delincuencia informática, punibilidad y ley aplicable. Magallanes, Universidad de Chile, Facultad de Derecho, Escuela de Postgrado. 62 h.

GUTIÉRREZ., M. 2005. Internet y libertad: ampliación tecnológica de la esencia humana. Sevilla, Comunicación Social. 160p.

GUZMÁN, B., A. 2012. Los orígenes de la noción de sujeto de derecho. Bogotá, Colombia, Temis, Pontificia Universidad Javeriana, Facultad de Ciencias Jurídicas. 157p.

HINE, C. 2004. Etnografía virtual. Barcelona, UOC. 210p.

HOYOS, C., I, M. 1990. La dimensión jurídica de la persona Humana. Bogotá. D.E., Colombia, Universidad de la Sabana. 35p.

IDENTIDADES, SUJETOS y subjetividades. 2005. Leonor Arfuch "et al". 2ª edición. Prometeo, Buenos Aires, Argentina. 87p.

JONES, S, G. 2003. Cibersociedad 2.0: una nueva visita a la comunidad y la comunicación mediada por ordenador. Editor. Barcelona, UOC. 253p.

LESSIG., L. 2001. El código y otras leyes del ciberespacio. Grupo Santillana de ediciones. Madrid, España. 540p.

LESSIG., L. 2005. Por una cultura libre. Cómo los grandes grupos de comunicación utilizan la tecnología y la ley para clausurar la cultura y controlar la creatividad. Traficantes de sueños. Madrid, España. 303p.

LESSIG., L. 2009. El código 2.0. Traficantes de sueños, Madrid, España. 563p.

LONG P., J. 1986. Tratamiento de los derechos de la personalidad en códigos civiles modernos. Memoria para optar a la licenciatura en ciencias jurídicas y sociales. Santiago, Universidad de Chile, Facultad de Derecho. 101 h.

MATA Y MARTÍN., R.M. 2001. Delincuencia Informática y Derecho Penal. Madrid, España. Edisofer. , 2001. 172 p.

MOLINA., C. 2009. El derecho comunitario y la I+D+T: Hacia el diseño de un perfil para el futuro. Textos universitarios. Universidad de Alcalá, servicios de publicaciones. Dykinson. Madrid, España. 136p.

MORALES G., O. 2002. Criterios de atribución de responsabilidad penal a los prestadores de servicios e intermediarios de la Sociedad de la Información. En: MORALES G., O. 2002. Delincuencia informática: problemas de responsabilidad. Cuadernos de derecho judicial, Consejo General del Poder Judicial. Madrid, España. 347p.

MORALES G., O. 2002. Delincuencia informática: problemas de responsabilidad. Cuadernos de derecho judicial, Consejo General del Poder Judicial. Madrid, España. 347p.

NAVA., A. 2005. Análisis de los delitos informáticos. 1a.ed. Porrúa, México. 119p.

PEÑA, O., P. 2013. ¿Cómo funciona internet? Nodos críticos desde una perspectiva de los derechos. Guía para periodistas. Chile. ONG Derechos Digitales. 74p.

PLINER, A. 1989. El nombre de las personas: legislación, doctrina, jurisprudencia, derecho comparado. Buenos Aires : Astrea, 2a. ed. act. xxiii, 427p.

ROA N., M. A. 2013. Facebook frente al derecho a la vida privada y la protección de datos personales. Memoria para optar a la licenciatura en ciencias jurídicas y sociales. Santiago, Universidad de Chile, Facultad de Derecho. 155 h.

RODRÍGUEZ, G., A. 2001. La persona humana. Revista chilena de derecho 28(2) pp. 239-247.

ROMERO L., L. 2011. Jus informa TIC's. 1ª ed. México. 202p.

ROMERO, F. R. y TÉLLEZ, V. J. 2011. La usurpación o suplantación de identidad: una aproximación conceptual y los posibles elementos constitutivos del tipo penal. En: ROMERO L., L. 2011. Jus informa TIC's. 1ª ed. México. 202p.

ROVIRA D., E. 2002. Delincuencia informática y fraudes informáticos. Editorial Comares. Granada, España. 693p.

ROXIN., Claus. 1997. Derecho Penal Parte General. Fundamentos. La estructura de la teoría del delito. Editorial Civitas.Madrid. 1071p.

SMITH, M. A. Y KOLLOCK, P. Editores. 2003. Comunidades en el ciberespacio. 1ª ed. en lengua castellana. Barcelona, UOC. 388p.

TURKLE, S. 1997. La vida en la pantalla: la construcción de la identidad en la era de Internet. 1ª ed. Barcelona; Paidós. 414p.

URETA A., L. 2009. Retos a superar en la administración de justicia ante los delitos informáticos en el Ecuador. [en línea] Tesis de grado para optar al título de magíster en sistemas de información gerencial. Facultad de ingeniería en electricidad y computación, Escuela Superior Politécnica del Litoral. Guayaquil, Ecuador. 113p. <http://www.dspace.espol.edu.ec/bitstream/123456789/5792/5/TESIS%20-%20DELITOS%20INFORMATICOS%20EN%20ECUADOR%20Y%20ADMINISTRACION%20DE%20JUSTICIA.pdf> [consulta:10 de diciembre de 2013]

VAN WEEZEL., A. 2011. Límites de la imputación penal. Estudios 2000-2010. Universidad Externado de Colombia. Bogotá, Colombia. 1a.ed. 464p.

VODANOVIC S., N. 1981. Los derechos de la personalidad en las legislaciones positivas extranjeras. Memoria para optar a la licenciatura en ciencias jurídicas y sociales. Santiago, Universidad de Chile, Facultad de Derecho. 99 h.

2. Recursos electrónicos y revistas electrónicas, entre otros.

ABDEL W, M., CHAWKI, M. 2006. Identity Theft Cyberspace: Issues and Solutions. [en línea] Lex Electronica, vol.11, N°1. 41p. <http://www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf>

ACURIO D., S. Delitos Informáticos: Generalidades. [en línea] Cátedra de Derecho Informático, Pontificia Universidad Católica del Ecuador. 67p. <http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf>

AHUATZIN S., G. Desarrollo de un esquema de traducción de direcciones IPv6-IPv4-IPv6. Capítulo II. Teoría y métodos de transición IPv4 a IPv6. [en línea] pp. 33-86 <http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/ahuatzin_s_gl/capitulo2.pdf>

ALLCLEARID. 2012. Online impersonation vs. Identity theft: Is there a difference? [en línea] <https://www.allclearid.com/blog/online-impersonatin-vs-identity-theft.> [consulta: 16 de marzo de 2015]

ANZIT G., R. Los delitos informáticos en la era de la revolución científico-tecnológica: Hacking, cracking, phreacking, phishing, scamming. [en línea] Argentina. 14p. <http://www.anzit-guerrero.net/admin/pdf/119759803.pdf>

AREVALO M, P. 2011. Modelo de regulación jurídica de las redes sociales virtuales. [en línea] Revista VIA IURIS, Fundación Universitaria Los Libertadores, Colombia. n° 11, julio-diciembre 2011. pp.109-136. <http://www.redalyc.org/pdf/2739/273922799007.pdf>

ARGENTINA CIBERSEGURA. ¿Cómo realizar una denuncia ante un delito informático? [en línea] <https://www.argentinacibersegura.org/admin/resources/files/consejos/28/1308_-_Qué_hacer_ante_un_delito_informático.pdf>

AROCENA., G. 2012. La Regulación de los delitos informáticos en el Código Penal Argentino. Introducción a la Ley Nacional Núm. 26.388. [en línea] Boletín de Derecho Comparado, vol. XLV, núm. 135, septiembre-

diciembre. Universidad Nacional Autónoma de México. pp. 945-988. <http://www.redalyc.org/pdf/427/42724584002.pdf>

ASAMBLEA LEGISLATIVA DEL Distrito Federal. V Legislatura. Diario de los debates de la Asamblea legislativa Federal. [en línea] <http://www.aldf.gob.mx/archivo-3930456bab522331c3f868909142f63d.pdf>

ASAMBLEA LEGISLATIVA DEL Distrito Federal. VI Legislatura. 2010. Reformas al Código Penal Protegen más a menores y tipifican como delito la usurpación de identidad. [en línea] <http://www.aldf.gob.mx/comsoc-reformas-al-codigo-penal-protegen-mas-menores-y-tipifican-como-delito-usurpacion-identidad--6163.html> [consulta: 15 de enero de 2014]

ASAMBLEA LEGISLATIVA DEL Distrito Federal. V Legislatura. Dictamen que presenta la Comisión de Administración y Procuración de Justicia, respecto de la iniciativa de reforma, con proyecto de decreto, por la que se crea un Capítulo III en el Título Segundo del Código Penal para el Distrito Federal. [en línea] <http://www.aldf.gob.mx/archivo-bd7ef91df50268b00a2c680bea0255ef.pdf> [consulta: 20 de marzo de 2015]

ASOCIACIÓN ARGENTINA de Derecho de Alta Tecnología. Delitos Informáticos. Antecedentes Internacionales para una Legislación Nacional. Proyectos Legislativos. Por Nora Paterlini, Carolina Vega, Gabriela Guerriero y Mercedes Velázquez. [en línea] <http://www.aadat.org/delitos_informaticos20.htm> [consulta: 20 de marzo de 2015]

BARRIUSO R., C. 2010. Las Redes Sociales y la protección de datos hoy [en línea] Memorias. XIV Congreso Iberoamericano de Derecho e Informática. Tomo I "Revolución Informática con Independencia del Individuo", Nuevo León, México: Universidad Autónoma de Nuevo León. pp. 81 – 104. <http://biblio.juridicas.unam.mx/libros/6/2940/7.pdf>

BENDERBR. 2013. Facebook elimina la opción de que no puedan buscarte por tu nombre. [en línea] <http://www.laneros.com/temas/facebook-

elimina-la-opci%C3%B3n-de-que-no-puedan-buscarte-por-tu-nombre.205049/> [consulta: 25 de octubre de 2013]

BLACKMAN., J. 2009. Omniveillance, Google, Privacy in Public, and the right to your digital identity: A tort for recording and disseminating an individual's image over the internet. [en línea] Santa Clara Law Review. Vol. 49, Nº 2, 2009. pp. 313-392. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1116776> [consulta: 20 de octubre de 2013]

BORGHELLO, C. y TEMPERINI, M. La captación ilegítima de datos confidenciales como delito informático en Argentina. [en línea] <http://www.elderechoinformatico.com/publicaciones/mtemperini/JAIIO_DI_Phishing_Camera_Ready.pdf>

BORGHELLO, C. y TEMPERINI, M. Suplantación de Identidad Digital como delito informático en Argentina. [en línea] Simposio Argentino de Informática y Derecho. 16p. <http://www.elderechoinformatico.com/publicaciones/mtemperini/JAIIO_DI_Identidad_Camera%20Ready.pdf>

BRENNER., S. 2012. La Convención sobre Cibercrimen del Consejo de Europa. [en línea] Revista Chilena de Derecho y Tecnología. Centro de estudios de derecho informático. Vol.1 n°1. pp. 221-238. Universidad de Chile. <http://www.revistas.uchile.cl/index.php/RCHDT/article/viewFile/24030/25629> [consulta: 10 de enero de 2015]

BUENDÍA., A. El extraño origen del Hashtag en Twitter #historia. [en línea] <http://www.apolorama.com/2013/07/el-extrano-origen-del-hashtag-en-twitter-historia/> [consulta: 20 octubre de 2013]

CALVO M., M., ROJAS L., C. 2009. Networking. Uso práctico de las redes sociales. [en línea] Esic. Madrid, España. 181p. <http://books.google.cl/books?id=4eczQreEaLwC&pg=PA95&lpg=PA95&dq=suplantacion+de+identidad+en+redes+sociales&source=bl&ots=h55Qa_6tn2&sig=9hrI7VLUW0-W6FbB0WEkoEUlHGM&hl=es-

419&sa=X&ei=lCaAUfynFoiu8QSc5YC4AQ&ved=0CEUQ6AEwBDha#v=onepage&q=suplantacion%20de%20identidad%20en%20redes%20sociales&f=false> [consulta: 15 de septiembre de 2013]

CAMPOS., F. Las redes virtuales emergen como nuevas plataformas de gestión del conocimiento. [en línea] Facultad de Ciencias de la Comunicación de la Universidad de Santiago, España. <http://www.iiis.org/CDs2008/CD2009CSC/CCC2009/PapersPdf/D644IQ.pdf>

CAMPOS., F. 2012. La nueva generación de herramientas de la comunicación. Sistemas, cibernética e informática. vol. 9, nº 1. pp. 36-41 <http://www.iiisci.org/journal/CV$/risci/pdfs/HCB089JD.pdf>

CÁRDENAS A., C. 2008. El lugar de comisión de los denominados ciberdelitos. [en línea] Polít. crim., N° 6, 2008, A2-6, pp. 1-14. <http://www.politicacriminal.cl/n_06/A_2_6.pdf>

CASSOU R., J. 2009. Delitos informáticos en México. [en línea] Revista del Instituto de la Judicatura Federal. Núm. 28. pp. 207-236. <http://www.ijf.cjf.gob.mx/publicaciones/revista/28/Delitos_informáticos.pdf>

CLANTON, K. 2010. We are not who pretend to be: ODR alternatives to online impersonation statutes. [en línea] Cardozo Journal of Conflict Resolution, Vol. 16. pp. 323-355 http://cardozojcr.com/wp-content/uploads/2014/11/Clanton_ODR-Alternatives.pdf

COM 2001/140/final. 2001. Comunicación de la Comisión, de 13 de marzo de 2001. "eEurope 2002. Impacto y prioridades". Comunicación preparada para el Consejo Europeo de Estocolmo el 23 y 24 de marzo de 2001. [en línea] <http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=es&type_doc=COMfinal&an_doc=2001&nu_doc=140> [consulta: 21 de marzo de 2015]

COMISIÓN DE LAS Comunidades Europeas. 2007. Hacia una política general de lucha contra la ciberdelincuencia. [en línea] Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones. Bruselas. <http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:52007DC0267> [consulta: 21 de marzo de 2015]

COMISION DE LAS Comunidades Europeas. 2000. COM 202 (2000) final. Comunicación de la Comisión al Consejo y al Parlamento Europeo. La organización y gestión de Internet. Cuestiones de política europea e internacional 1998-2000. 4 de noviembre de 2000. Bruselas [en línea] <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0202:FIN:ES:PDF>

COMPUTACIÓN APLICADA al Desarrollo. "Historia de Facebook". [en línea]: <http://www.cad.com.mx/historia_de_facebook.htm> [consulta: 20 de octubre de 2013]

COMPUTACIÓN APLICADA al Desarrollo. "Historia de Twitter". [en línea]: <http://www.cad.com.mx/historia_de_twitter.htm> [consulta: 20 de octubre de 2013]

CNN México. 2010. México podría ser el primer país en castigar el mal uso de las redes sociales. [en línea] CNN México. 15 de Junio, 2010. <http://mexico.cnn.com/nacional/2010/06/15/mexico-podria-ser-el-primer-pais-en-castigar-el-mal-uso-de-redes-sociales> [consulta: 10 de enero de 2014]

CONSEJO DE EUROPA. 2007. Internet-related identity theft. [en línea] Economic Crime Division. Alemania. 33p. <http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/Internet_related_identity_theft_%20Marco_Gercke.pdf>

CONSEJO DE EUROPA. 2009. Dictamen 5/2009 sobre las redes sociales en línea. [en línea] Grupo de trabajo sobre protección de datos del artículo 29. Bruselas 14p.

<http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_es.pdf>

CROFT., C. 2007 A brief history of The Facebook. [en línea] 18 de diciembre. 3p. <http://charlenegagnon.files.wordpress.com/2008/02/a-brief-history-of-the-facebook.pdf>

DE UGARTE., D. El poder de las redes. [en línea] 78p. <http://chuerta.com/libros/El_Poder_De_Las_Redes.pdf>

DEFINICION.DE. 2008-2013. Qué significa TCP IP. [en línea] <http://definicion.de/tcp-ip/> [consulta: 10 de octubre de 2013]

DELPIAZZO., C. Enfoque jurídico de las redes sociales. [en línea] Revolución informática con independencia del individuo. XIV Congreso Iberoamericano de Derecho e Informática, Monterrey. pp. 277-291<http://biblio.juridicas.unam.mx/libros/6/2940/18.pdf>

DEPARTAMENTO DE Justicia de los Estados Unidos. Sección de delitos informáticos y propiedad Intelectual. [en línea] 1p. <http://www.oas.org/juridico/english/cyb_mex_info.pdf>

DIALNET. 2013. La suplantación de una identidad digital. [en línea] <file:///C:/Users/Nicole/Downloads/Dialnet-LaSuplantacionDeUnaIdentidadDigital-4179718.pdf>

DIARIO DE NOTICIAS. 2014. La Fiscalía propone tipificar la suplantación en Internet. [en línea] <http://diariodenoticias.laley.es/documento.asp?id=./NE0000492377_20140916.HTML> [consulta: 17 de marzo de 2015]

DIAZ., A. 2010. El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest. [en línea] REDUR 8, diciembre 2010, pp. 169-203. <http://www.unirioja.es/dptos/dd/redur/numero8/diaz.pdf>

DOMISFERA. 2009. El origen de Twitter. [en línea] 25 de febrero. <http://www.domisfera.com/el-origen-de-twitter/> [consulta: 21 de octubre de 2013]

ECHEVERRÍA, J. 2007. Gobernanza de la sociedad europea de la información. [en línea] Rev. iberoam. cienc. tecnol. soc. v.3 n.8. Ciudad Autónoma de Buenos Aires, abr. 2007. <http://www.scielo.org.ar/scielo.php?pid=S1850-00132007000100006&script=sci_arttext> [consulta: 21 de octubre de 2013]

EVOCA COMUNICACIÓN e imagen. [en línea] Cuadernos de comunicación evoca. Identidad digital y reputación online 50p <http://www.evocaimagen.com/cuadernos/cuadernos5.pdf>.

ESTRADA G., M. Delitos informáticos [en línea] 26p. <http://perso.unifr.ch/derechopenal/assets/files/articulos/a_20080526_32.pdf>

EMOL. 2012. Zalaquett suplantado en Twitter: "El daño que me hizo fue muy grande". [en línea] Chile. <http://www.emol.com/noticias/nacional/2012/08/24/557221/detienen-a-joven-por-suplantar-a-alcalde-zalaquett-en-twitter.html> [consulta: 17 de marzo de 2015]

EUROPA. Síntesis de la legislación de la UE. 2005. eEurope: Una sociedad de la información para todos. [en línea] <http://europa.eu/legislation_summaries/information_society/strategies/l24221_es.htm> [consulta: 22 de enero de 2015]

EUROPEAN Foundation for Information Society. 2013. ¿Qué es la fundación Europea para la Sociedad de la Información? [en línea] <http://www.european-foundation.org/es/> [consulta: 22 de enero de 2015]

FACEBOOK. 2013. Ayuda para ordenadores. ¿Cómo se usan los hashtag?. [en línea]

<https://www.facebook.com/help/587836257914341?sr=2&sid=0164mb7pGcvLC3kkO> [consulta: 20 de octubre de 2013]

FACEBOOK. 2013. Ayuda para ordenadores. Denuncia la cuenta de un impostor. [en línea] <https://es-es.facebook.com/help/contact/169486816475808> [consulta: 20 de octubre de 2013]

FACEBOOK. 2015. Ayuda para ordenadores. Reporta una violación. [en línea] <https://es-es.facebook.com/help/263149623790594/> [consulta: 17 de mayo de 2015]

FACEBOOK. 2013. Ayuda para ordenadores. ¿Qué diferencia hay entre las páginas y los grupos? ¿Cuál debo crear? [en línea] <https://www.facebook.com/help/www/162866443847527> [consulta: 20 de octubre de 2013]

FACEBOOK. 2013. Ayuda para ordenadores. ¿Qué es una aplicación de Facebook? [en línea] <https://www.facebook.com/help/www/217453588274571> [consulta: 20 de octubre de 2013]

FACEBOOK. 2013. Ayuda para ordenadores. ¿Qué es la biografía de Facebook? [en línea] <https://www.facebook.com/help/www/467610326601639> [consulta: 20 de octubre de 2013]

FACEBOOK. 2013. Ayuda para ordenadores. Revisión de la biografía. [en línea] <https://www.facebook.com/help/www/399043533452321?sr=3&sid=00XJ1FtslvhusOYlt> [consulta: 20 de octubre de 2013]

FACEBOOK. 2015. Condiciones y políticas de Facebook. Todo lo que necesitas saber, en un solo sitio. [en línea] <https://es-es.facebook.com/policies/> [consulta: 17 de mayo de 2015]

FACEBOOK. 2015. Declaración de derechos y responsabilidades. [en línea] <https://es-es.facebook.com/legal/terms> [consulta: 17 de mayo de 2015]

FACEBOOK. 2013. Ayuda para ordenadores. Edad mínima. [en línea] <https://www.facebook.com/help/www/216323255079947> [consulta: 20 de octubre de 2013]

FACEBOOK. 2009. Política de privacidad de Facebook. [en línea] <http://www.facebook.com/note.php?note_id=+322317115300> [consulta: 20 de octubre de 2013]

FACEBOOK. 2015. Política de uso de datos. [en línea] <https://es-es.facebook.com/full_data_use_policy> [consulta: 17 de mayo de 2015]

FARALDO C., P. 2010. Suplantación de identidad y uso de nombre supuesto en el comercio tradicional y electrónico. [en línea] Revista de Derecho Penal y Criminología. 3° Época, n°3. pp. 73-134. <http://e-spacio.uned.es/fez/eserv/bibliuned:revistaDerechoPenalyCriminologia-2010-3-5030/Documento.pdf>

FISCALIA GENERAL del Estado. 2014. [en línea] 7.11 Fiscal de Sala Coordinadora en materia de Criminalidad Informática. España. pp. 1103-1157
<https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/memoria2012_vol1_amf_17.pdf?idFile=20d58c12-50c3-42ce-9157-fdef3762090e> [consulta: 20 de marzo de 2015]

FERNANDEZ B., P. 2012. Aspectos jurídicos de la identidad digital y la reputación online. [en línea] Revista Científica de Estrategias, Tendencias e Innovación en Comunicación. número 3. pp. 125-142 <http://repositori.uji.es/xmlui/bitstream/handle/10234/43024/Pablo%20Fern%C3%A1ndez%20Burgue%C3%B1o.pdf?sequence=1> [consulta: 4 de octubre de 2015]

GAMERO., R. 2009. La configuración de la identidad digital. [en línea] Nota eter. UniversitatPolitécnicaa de Valencia. España. 6p.

<https://observatorio.iti.upv.es/media/managed_files/2009/06/03/11569.pdf>

GARCÍA A., L. 2007. ¿Web 2.0 vs Web 1.0? [en línea] Editorial BENED. 8p. <http://ddd.uab.cat/pub/dim/16993748n10a4.pdf>

GARCÍA G., A. 2013. Reflexiones en torno a la protección de los datos personales en Internet y las redes sociales. Retos y perspectivas en un mundo hiperconectado. [en línea] Derecho comparado de la información. enero-junio de 2013. pp. 39-67. <http://biblio.juridicas.unam.mx/revista/pdf/DerechoInformacion/21/art/art2.pdf>

GIONES V. Aina, SERRAT I B. Marta. 2010. La gestión de la identidad digital: una nueva habilidad informacional y digital. [en línea] BiD: textos universitaris de biblioteconomia i documentació, juny, núm. 24. <http://www.ub.edu/bid/24/giones2.htm> [consulta: 10 de octubre de 2013]

GONZÁLEZ, L. 2012. Redes sociales: crecen los casos de robo de identidad. [en línea] Clarín en Internet. 02 de Junio, 2012. <http://www.clarin.com/sociedad/Redes-sociales-crecen-casos-identidad_0_711528989.html> [consulta: 10 de marzo de 2015]

GONZALEZ., J. 2011. Ley de Delitos Informáticos (26.388). Violación de Secretos y Privacidad. [en línea] Administración y Gestión de Proyectos de Software. 26p. <http://www.cs.uns.edu.ar/~prf/teaching/APS11/downloads/Trabajos%20Legislacion/Informes/Informe%20-%20Ley%20de%20Delitos%20Informaticos.pdf>

GOOGLE.SITES. Web 1.0 historia. [en línea] <https://sites.google.com/site/web10historia/> [consulta: 8 de septiembre de 2013]

GRUVIX FREEWARE. 2013. Historia 2.0: Cómo nació Facebook. [en línea] <http://gruvix.com/historia-2-0-como-nacio-facebook/> [consulta: 10 de septiembre de 2013]

HAZZARD, Y. A Little Know Weapon To Combat Online Impersonation: California Penal Code Section 528.5 [en línea] 2p. <http://www.robinskaplan.com/~/media/PDFs/A%20Little%20Known%20Weapon%20to%20Comba%20Online%20Impersonation.pdf>

HERNANDEZ., L. 2009. El delito informático. [en línea] Eguzkilore n°23 pp. 227-243. San Sebastián, España. <http://www.ivac.ehu.es/p278-content/es/contenidos/boletin_revista/eguzkilore_23_homenaje_ab/es_eguzki23/adjuntos/18-Hernandez.indd.pdf>

HOOFNAGLE., C. J. 2007. Identity Theft: Making the Known Unknowns known. [en línea] Harvard Journal of Law & Technology. Volume 21, Number 1 Fall 2007. Pp. 98-122. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=969441> [consulta: 25 de septiembre de 2013]

INSUA., M. 2013. Suplantación de identidad en las redes sociales. [en línea] Insua Vidal Avogados. Blog. Febrero, 2013. <http://www.insuavogados.com/es/suplantación-de-identidad-en-las-redes-sociales> [consulta: 10 de mayo de 2015]

INTERNAL REVENUE SERVICE. 1999. Memorandum for Assistant Regional Counsel. [en línea] United States. 7p. <http://www.unclefed.com/ForTaxProfs/irs-wd/1999/9911041.pdf>

JARAMILLO., O. 2010. La desarticulación de lo público y lo privado en las redes sociales. [en línea] 15p. <http://oscarjaramillo.cl/wp-content/uploads/2011/04/PO-Oscar.pdf>

LANDA D., G. 2007. Los delitos informáticos en el Derecho penal de México y España. [en línea] Revista del Instituto de la Judicatura Federal, Núm. 24. pp. 233-256. <http://new.pensamientopenal.com.ar/sites/default/files/2012/03/r24_9.pdf>

LINKSYS. Direcciones IP estáticas y dinámicas. [en línea] <http://kb.linksys.com/Linksys/GetArticle.aspx?docid=c99208d371f04cdd82c0ae93e07b24eb_jm_temp.xml&pid=82&converted=0> [consulta: 5 de diciembre de 2013]

LÓPEZ J., D. 2009. La protección de datos de carácter personal en el ámbito de las redes sociales electrónicas: el valor de la autorregulación. [en línea] Anuario Facultad de Derecho Universidad de Alcalá. nº 2. pp. 237-274.
<http://dspace.uah.es/dspace/bitstream/handle/10017/6445/proteccion_lopez_AFDUA_2009.pdf?sequence=1> [consulta: 9 de febrero de 2015]

LOPUCKI., L. 2001. Human Identification Theory and the Identity Theft Problem. [en línea] Texas Law Review, Vol 80. pp. 89-134. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=263213> [consulta: 20 de septiembre de 2015]

LOS ANGELES TIMES. 2009. Twitter creator Jack Dorsey illuminates the site's founding document. Part I. [en línea] Los Angeles Times. 18 de febrero 2009. <http://latimesblogs.latimes.com/technology/2009/02/twitter-creator.html l> [consulta: 23 de octubre de 2013]

LUCHA CONTRA LOS Delitos Informáticos. 2005. Síntesis de la legislación de la Unión Europea. Lucha contra los delitos informáticos. [en línea]
<http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l33193b_es.htm> [consulta: 20 de febrero de 2015]

MAUSKOPF., S. 2012. Tailored Trends bring you closer. [en línea] <https://blog.twitter.com/2012/tailored-trends-bring-you-closer> [consulta: 23 de septiembre de 2013]

MICROSOFT. Centro de seguridad y protección. 2012. ¿Qué es el robo de identidad? [en línea] <http://www.microsoft.com/es-xl/security/resources/identitytheft-whatis.aspx> [consulta: 11 de diciembre de 2013]

MICROSOFT. Centro de seguridad y protección. 2012. Reconozca correos electrónicos de suplantación de identidad (phishing) o vínculos de este tipo. [en línea] <http://www.microsoft.com/es-es/security/online-privacy/phishing-symptoms.aspx> [consulta: 11 de diciembre de 2013]

MICROSOFT. Qué es un Firewall. [en línea] <http://windows.microsoft.com/es-mx/windows/what-is-firewall#1TC=windows-7> [consulta: 20 de mayo de 2015]

MIRÓ LL., F. 2011. La oportunidad criminal en el Ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. [en línea] Revista Electrónica de ciencia Penal y Criminología. Nº 13, 2011. 55p. <http://criminet.ugr.es/recpc/13/recpc13-07.pdf>

MORRACHIMO R., M. 2011. La privacidad después de Facebook. [en línea] Lima, Perú. 22p. <http://www.blawyer.org/docs/morachimo_privacidad_facebook.pdf>

MUÑOZ L., F. 2013. ¿Es punible la parodia a través de Twitter? [en línea] Revista chilena de Derecho y Tecnología. Centro de estudios en Derecho Informático. Universidad de Chile. Vol. 2. Núm. 1 (2013). p. 149-168. <http://www.revistas.uchile.cl/index.php/RCHDT/article/viewFile/27015/28938> [consulta: 4 de febrero de 2015]

NACIONES UNIDAS. 2010. 12° Congreso de las Naciones Unidas sobre prevención del delito y justicia penal. [en línea] Tema 8 del programa provisional. Salvador, Brasil. 18p <http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050385s.pdf>

NACIONES UNIDAS. 2013. Manual sobre los delitos relacionados con la Identidad. [en línea] Oficina de las Naciones Unidas contra la Droga y el Delito. Nueva York. 380pp. <http://www.unodc.org/documents/organized-crime/13-83700_Ebook.pdf>

NAVAL., C. 1995. Identidad personal, hábito y educación. [en línea] Concepción Naval. Universidad de Navarra. Revista Tópicos. Universidad Panamericana, México. p. 31-50. <http://topicos.up.edu.mx/topicos/wp-content/uploads/2012/12/1995_TOP09_A_Naval.pdf>

NOGUEIRA A., H. 2007. El derecho a la propia imagen como derecho fundamental implícito. Fundamentación y caracterización. [en línea] Revista Ius et Praxis, Vol. 13, Nº. 2, 2007. pp. 245-285. <http://www.scielo.cl/pdf/iusetp/v13n2/art11.pdf>

NOTICIAS JURÍDICAS. Ley Orgánica 10/1995, 23 de noviembre, 2010, del Código Penal. [en línea] <http://noticias.juridicas.com/base_datos/Penal/lo10-1995.l2t13.html> [consulta: 3 de marzo de 2015]

NUÑEZ P., J. 2010 Redes sociales en internet y derecho informatico en el Perú. [en línea] Revolución informática con independencia del individuo. XIV Congreso Iberoamericano de Derecho e Informática, Monterrey. pp. 578-585 <http://biblio.juridicas.unam.mx/libros/6/2941/7.pdf>

ORGANIZATION FOR Economic Co-operation and development. 2008. OECD Policy Guidance on Online Identity Theft. [en línea] Seoul, Korea. OECD Ministerial Meeting on the Future of the Internet Economy. 17-18 june, 2008. 20p. <http://www.oecd.org/internet/consumer/40879136.pdf>

PARR., B. Based Trending Topics. [en línea] <http://mashable.com/2010/01/22/twitter-local-trend/> [consulta: 22 de octubre de 2013]

PARLAMENTO EUROPEO. 2008. Preguntas parlamentarias. Asunto: Usurpación de identidad. [en línea] <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+WQ+E-2008-5963+0+DOC+XML+V0//ES> [consulta: 6 de abril de 2015]

PARLAMENTO EUROPEO. 2009. Parliamentary questions. Answer given by Mr Barrot on behalf on the Commission. [en

línea] <http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2008-5963&language=ES> [consulta: 6 de abril de 2015]

PIÑA L., H. Los delitos informáticos previstos y sancionados en el Ordenamiento Jurídico Mexicano. [en línea] 27p. <http://www.ordenjuridico.gob.mx/Congreso/2doCongresoNac/pdf/PinaLibien.pdf>

PODER LEGISLATIVO GUANAJUATO. Sala de Prensa. 2015. Propone el GPPAN sancionar la usurpación de identidad. 29/01/2015/ Boletín: 1234. [en línea] <http://www.congresogto.gob.mx/comunicados/propone-el-gppan-sancionar-la-usurpacion-de-identidad> [consulta: 8 de abril de 2015]

POLITICA DE LA Sociedad de la Información. Guía práctica de la Unión Europea. No. 27. [en línea] <http://www.madrid.org/cs/Satellite?blobcol=urldata&blobheader=application%2Fpdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1352807270520&ssbinary=true> [consulta: 7 de abril de 2015]

PSUV. MANUAL de usuario. Twitter. Configuración. Principales funcionalidades. [en línea] Venezuela. 17p. <http://desarrollo.psuv.org.ve/files/2010/07/Manual-de-Usuario-Twitter.pdf>

RAMIREZ B., E. AGUILERA R., A. 2009. Los delitos informáticos. Tratamiento internacional. [en línea] Constribuciones a las ciencias sociales. 13p. <http://www.eumed.net/rev/cccss/04/rbar2.pdf>

RAMOS., J. Delitos informáticos. [en línea] 9p. <http://julioramos.bligoo.com.mx/media/users/23/1189400/files/338082/DELITOS_INFORMATICOS.pdf>

REVISTA INFORMATICA Jurídica. 2013. Legislación Unión Europea, Consejo de Europa y Comité de Ministros del Consejo de Europa. [en línea] <http://www.informatica-juridica.com/legislacion/union_europea.asp> [consulta: 15 de enero de 2014]

REZNIK, M. 2013. Identity Theft on Social Networking Sites: Developing Issues of Internet Impersonation. Touro Law Review. Vol. 29, N° 2, Article. 12, 2013. pp. 455-483. <http://digitalcommons.tourolaw.edu/cgi/viewcontent.cgi?article=1472&context=lawreview> [consulta: 10 de enero de 2014]

RFG. Desarrollo web. Twitter. Qué es y cómo utilizarlo. [en línea] 20p. <http://www.rfg84.com/twitter/El_ABC_de_Twitter.pdf>

RÍOS E., J.J. 1997. Derecho e informática en México. Informática Jurídica y Derecho de la informática. [en línea] Instituto de investigaciones Jurídicas de la UNAM. México, D.F. 175p. <http://www.bibliojuridica.org/libros/libro.htm?l=147> [consulta: 27 de marzo de 2015]

RIZZO G., M. Redes. Una aproximación al concepto. [en línea] Barcelona, España. 7p. <http://www.cecaargentina.com.ar/documentosinteres/redes.pdf>

RODRÍGUEZ P., L. F. 2012. Suplantación de identidad en redes sociales: Nueva realidad. [en línea] La Gaceta Jurídica de la Empresa Andaluza. Revista de HispaColex Servicios Jurídicos. Núm. 38. Noviembre, 2012. pp. 14 y 15. <http://www.hispacolex.com/pdf/suplantacion_de_identidad_en_redes_sociales.pdf>

ROLLAN., F. 2012. Tailored Trend los “trending topics” según el usuario y su localización. [en línea] <http://www.semseo.es/blog/general/tailored-trends-los-%E2%80%98trending-topics%E2%80%99-segun-el-usuario-y-su-localizacion.php> [consulta: 22 de octubre de 2013]

ROMERO F., R. La Usurpación o Suplantación de identidad: Una aproximación conceptual y los posibles elementos constitutivos del tipo penal. [en línea] México. <http://xa.yimg.com/kq/groups/17424855/799161400/name/LA+USURPACI%C3%93N+O+SUPLANTACI%C3%93N+DE+IDENTIDAD.+UNA+A

PROXIMACI%C3%93N+CONCEPTUAL+Y+LOS+POSIBLES+ELEMENTOS+CONSTITUTIVOS+DEL+TIPO+PENAL> [consulta: 4 de enero de 2015]

ROMERO F., R. Las conductas vinculadas a la suplantación de identidad por medios telemáticos: una propuesta de acción legislativa. [en línea] México. pp. 849-863. <http://biblio.juridicas.unam.mx/libros/6/2941/24.pdf>

SAN MARTIN del Rey Aurelio. Twitter. [en línea] España. 17p. <http://www.smra.eu/files/Twitter.pdf>

SARMIENTO., A. 2013. Identidad digital, cuida lo que no quieres que otros sepan de ti. [en línea] Consultoría BBVA, Formando Ideas. Enero, 2013. <http://blog.bbvaconsultoria.com/2013/01/identidad-digital-cuida-lo-que-no-quieres-que-otros-sepan-de-ti/> [consulta: 15 de octubre de 2013]

SOCIEDAD DE LA Información. Normas que pueden servir. <http://europa.eu/legislation_summaries/information_society/index_es.htm> [consulta: 10 de noviembre de 2013]

SOLOVE., D. 2003. Identity Theft, Privacy, and the Architecture of Vulnerability. [en línea] Hastings Law Journal, Vol. 54. 46p. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=416740> [consulta: 12 de octubre de 2013]

STATISTIC BRAIN. 2013. Facebook statistic. [en línea] <http://www.statisticbrain.com/facebook-statistics/> [consulta: 9 enero 2014]

STATISTIC BRAIN. 2013. Twitter Statistics. [en línea] <http://www.statisticbrain.com/twitter-statistics/> [consulta: 9 enero 2014]

STURM., C. 2013. Facebook ahora tiene Hashtag. [en línea] <http://www.fayerwayer.com/2013/06/facebook-ahora-tiene-hashtags/> [consulta: 10 de diciembre de 2013]

TECNOLOGÍA. Universia Knowledge Wharton. 2007. Las redes sociales online redefinen la privacidad personal. [en línea] Wharton University of Pennsylvania. Junio, 2007. <http://www.wharton.universia.net/index.cfm?fa=viewArticle&id=1730> [consulta: 15 de octubre de 2013]

TEMPERINI, M. 2012. Cruzada para tipificar el delito de Suplantación de Identidad Digital (Argentina). [en línea] Red Iberoamericana. <http://www.elderechoinformatico.com/index.php?option=com_content&view=article&id=1149:cruzada-robo-identidad&catid=34:delitos-inf&Itemid=56> [consulta: 24 de marzo de 2015]

THE UNITED STATES Department of Justice. Identity theft and Identity fraud. [en línea] <http://www.justice.gov/criminal/fraud/websites/idtheft.html> [consulta: 20 de septiembre de 2013]

TREVIÑO G., R. 2002. La persona y sus atributos. [en línea] Universidad Autónoma de Nueva León. Facultad de Derecho y Criminología. 1ª. ed. 131p. <http://www.corteidh.or.cr/tablas/23961.pdf>

TRABAJO PRESENTADO en la materia de redes lan y man (IPv4 Vs IPv6). 2008. Ana Bejarano "et al". [en línea] Maestría en telemática, vicerrectorado de investigación y posgrado, Universidad Rafael Belloso Chacín, República Bolivariana de Venezuela. 13p. <http://www.urbe.edu/info-consultas/web-profesor/12697883/articulos/Redes%20Informaticas/IPv4%20Vs%20IPv6.pdf>

TWITTER: 5 años. Un recorrido por la herramienta que se convirtió en plataforma. Miguel Jorge "et al". [en línea] 107p. <http://www.antonioconstantino.com/pdf/twitter.pdf>

TWITTER. 2014. Condiciones de servicio. [en línea] <https://twitter.com/tos> [consulta: 20 de febrero de 2014]

TWITTER. Centro de ayuda. 2013. Cómo reportar infracciones. [en línea] <https://support.twitter.com/groups/56-policies-violations/topics/238-report-a-violation/articles/108038-como-reportar-infracciones> [consulta: 28 de diciembre de 2013]

TWITTER. Centro de ayuda. 2014. Políticas y Violaciones. Conoce las reglas de Twitter y denuncia infracciones. [en línea] <https://support.twitter.com/groups/56-policies-violations#topic_236> [consulta: 20 de febrero de 2014]

TWITTER. Centro de ayuda. 2014. Las reglas de Twitter. [en línea] <https://support.twitter.com/groups/56-policies-violations/topics/236-twitter-rules-policies/articles/72688-las-reglas-de-twitter> [consulta: 20 de febrero de 2014]

TWITTER. Centro de ayuda. 2014. Política de suplantación de identidad. [en línea] <https://support.twitter.com/articles/72692-politica-de-suplantacion-de-identidad> [consultas: 20 de febrero de 2014]

TWITTER. Centro de ayuda. 2014. Política de cuentas de parodias, comentarios y admiradores. [en línea] <https://support.twitter.com/groups/56-policies-violations/topics/236-twitter-rules-policies/articles/371626-politica-de-cuentas-de-parodias-comentarios-y-admiradores> [consulta: 20 de febrero de 2014]

TWITTER. Centro de ayuda. 2014. Información privada publicada en Twitter. [en línea] <https://support.twitter.com/groups/56-policies-violations/topics/236-twitter-rules-policies/articles/20170167-informacion-privada-publicada-en-twitter> [consulta:]

TWITTER. Centro de ayuda. 2014. Protecting your personal information. [en línea] <https://support.twitter.com/articles/18368> [consulta: 20 de febrero de 2014]

TWITTER. Centro de ayuda. 2014. Política de apropiación de nombres. [en línea] <https://support.twitter.com/groups/56-policies-violations/topics/236-

twitter-rules-policies/articles/72706-politica-de-apropiacion-de-nombres> [consulta: 20 de febrero de 2014]

TWITTER. Centro de ayuda. 2014. Cómo reportar las cuentas de suplantación de identidad. [en línea] <https://support.twitter.com/articles/20170183-como-reportar-las-cuentas-de-suplantacion-de-identidad> [consulta: 20 de febrero de 2014]

TWITTER. Centro de ayuda. 2014. Reportar una cuenta por suplantación de identidad. [en línea] < https://support.twitter.com/forms/impersonation> [consulta: 20 de febrero de 2014]

TWITTER. Centro de ayuda. 2014. Cómo reportar información privada publicada en Twitter. [en línea] <https://support.twitter.com/groups/56-policies-violations/topics/238-report-a-violation/articles/20170171-como-reportar-informacion-privada-publicada-en-twitter> [consulta: 20 de febrero de 2014]

TWITTER. Centro de ayuda. 2014. Estoy reportando un usuario abusivo. [en línea] <https://support.twitter.com/forms/abusiveuser> [consulta: 20 de febrero de 2014]

TWITTER. 2013. Cuenta personal de Jack Dorsey. Actualización de su estado el 21 de marzo de 2006. [en línea] <https://twitter.com/jack/status/20> [consulta: 20 de febrero de 2014]

UNCITRAL. 2001. Ley modelo de la CNUDMI sobre firmas electrónicas con la guía para su incorporación al derecho interno. [en línea] 91p. <http://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf>

UNIÓN INTERNACIONAL de telecomunicaciones. 2009. El coberdelito: Guía para los países en desarrollo. [en línea] recursos jurídicos contra el ciberdelito. 238p. <http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf>

VÁZQUEZ., F. A lawbook para Facebook. [en línea] Revolución informática con independencia del individuo. XIV Congreso Iberoamericano de Derecho e Informática, Monterrey. pp. 781-793. <http://biblio.juridicas.unam.mx/libros/6/2941/20.pdf>

VÁZQUEZ R., T.2012. La tutela de la información personal y el uso de las redes sociales. [en línea] Universitas. Revista de Filosofía, Derecho y Política. nº 15. pp. 125-147. <http://universitas.idhbc.es/n15/15-06.pdf>

Viega., R. M. "Un nuevo desafío jurídico: Los Delitos Informáticos". [en línea] <http://mjv.viegasociados.com/wp-content/uploads/2011/05/DelitosInformaticos.pdf>

WALNUTERS. Manual de Twitter. [en línea] España. 97p. <http://www.redsaludandalucia.es/sites/default/files/null/Twitter%20manual_0.pdf>

3. Congresos, conferencias y reuniones

BORGHELLO, C. y TEMPERINI, M. 2012. Suplantación de Identidad Digital como delito informático en Argentina. [videograbación] Simposio de Informática y Derecho de las Jornadas Argentinas de Informática (JAIIO) Nº 41. 19:33 min., sonido, color. [en línea] <https://www.youtube.com/watch?v=jayX9ApzP6c> [consulta: 14 de marzo de 2015]

SIMPOSIO ARGENTINO de informática y derecho. Suplantación de identidad digital como delito informático en Argentina. 27 y 28 de agosto de 2004. Buenos Aires, Argentina. pp. 79-93 <http://www.41jaiio.org.ar/sites/default/files/7_SID_2012.pdf>

SIMPOSIO INTERNACIONAL de derecho de autor: Derecho de autor un desafío para la creación y el desarrollo. 12 y 13 de noviembre de 2004. 2004. Santiago, Chile. Programa "Pensamiento y Cultura" del Consejo Nacional de Cultura. 237p.

4. Documentos y leyes

ARGENTINA. Código Penal de la Nación de Argentina. [en línea] <http://www.infoleg.gov.ar/infolegInternet/anexos/15000-19999/16546/texact.htm#18> [consulta: 13 de marzo de 2015]

CHILE. Constitución Política de la República. 1980.

CHILE. Código Civil.

CHILE. Ministerio de LEY Nº 17.366, Apéndice Código Civil, publicada en el Diario Oficial Nº 27.761, del 2 de octubre del año 1970.

CHILE. Historia de la ley 19.611.

CHILE. Historia de la ley 19.223.

CHILE. Historia de la ley 19.799.

CONVENIO DE Budapest sobre la ciberdelincuencia. [en línea] <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_spanish.PDF>

DECRETO No. 525. SE REFORMA EL PRIMER PÁRRAFO Y LA FRACCIÓN V, Y SE ADICIONA LA FRACCIÓN VII, AL ARTÍCULO 234 DEL CÓDIGO PENAL PARA EL ESTADO DE COLIMA. [en línea] Tomo 94 Colima, Col., Sábado 09 de Mayo del año 2009; Núm. 19; pág. 763.
<http://www.ordenjuridico.gob.mx/Estatal/COLIMA/Decretos/COLDEC300.pdf>

ESPAÑA. 2015. Código Penal Español y legislación complementaria. Edición actualizada a 5 de enero de 2015. Boletín oficial del Estado. Madrid. 836p.

ESTADOS UNIDOS. Código Penal del Estado de California Sección 528-539. [en línea] <http://www.leginfo.ca.gov/cgi-

bin/displaycode?section=pen&group=00001-01000&file=528-539> [consulta: 20 de febrero de 2015]

ESTADOS UNIDOS. Código Penal del Estado de Nueva York Sección 190.25. [en línea] <http://codes.lp.findlaw.com/nycode/PEN/THREE/K/190/190.25> [consulta: 20 de febrero de 2015]

ESTADOS UNIDOS. Código Penal del Estado de Texas. [en línea] Título 7, Ofensas Contra la Propiedad. Capítulo 33, Crímenes Computacionales. <http://www.statutes.legis.state.tx.us/Docs/PE/htm/PE.33.htm> [consulta: 20 de febrero de 2015]

FRANCIA. Código Penal de Francia. [en línea] Artículo 226-4-1 <http://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070719&idArticle=LEGIARTI000023709201> [consulta: 22 de febrero de 2015]

Información General. Expediente 2257/11. Proyecto de Ley incorporando el art. 157 ter al Código Penal, tipificando el delito de obtención ilegítima de datos confidenciales ("Phishing"). [en línea] <http://www.senado.gov.ar/web/proyectos/verExpe.php?origen=S&numexp=2257/11&tipo=PL&tConsulta=1> [consulta: 20 de febrero de 2015]

Información General. Expediente 1312/12. Proyecto de Ley incorporando el art. 138 bis al Código Penal, por el cual se tipifica el delito de Suplantación de Identidad Digital. [en línea] <http://www.senado.gov.ar/web/proyectos/verExpe.php?origen=S&tipo=PL&numexp=1312/12&nro_comision=&tConsulta=1> [consulta: 24 de febrero de 2015]

MÉXICO. Código Penal Federal de México. [en línea] <http://info4.juridicas.unam.mx/ijure/tcfed/8.htm?s=> [consulta: 25 de febrero de 2015]

MÉXICO. Asamblea Legislativa del Distrito Federal, VI Legislatura. Código Penal para el Distrito Federal. [en línea]

<http://www.aldf.gob.mx/archivo-5b523887b84cba9b46e165101d758f01.pdf>

MÉXICO. Código Penal del Estado de México. [en línea] <http://www.edomex.gob.mx/legistelfon/doc/pdf/cod/vig/codvig006.pdf>

MÉXICO. Código Penal del Estado de Colima. [en línea] <http://www.docstoc.com/docs/167421085/Código-Penal---Congreso-del-Estado-de-Colima> [consulta: 25 de febrero de 2015]

5. Jurisprudencia.

PRIMER TRIBUNAL ORAL EN LO PENAL DE SANTIAGO. 31 de diciembre de 2010. RIT N° 165-2010.

CORTE SUPREMA DE CHILE. 11 de octubre de 2007. Rol N° 2.370-2007.

TERCER TRIBUNAL ORAL EN LO PENAL DE SANTIAGO. 01 de abril de 2014. RIT N° 46-2014.

SEXTO TRIBUNAL ORAL EN LO PENAL DE SANTIAGO. 24 de noviembre de 2010. RIT N° 592-2010.

SÉPTIMO JUZGADO DE GARANTÍA DE SANTIAGO. 17 de mayo de 2013. RIT N° 17.117-2012.

SÉPTIMO JUZGADO DE GARANTÍA DE SANTIAGO. 19 de febrero de 2014. RIT N°16.848-2012.

DÉCIMO TERCER JUZGADO DE GARANTÍA DE SANTIAGO. 4 de noviembre de 2009. RIT N° 8.865-2009.

TRIBUNAL ORAL EN LO PENAL DE TALCA. 21 de diciembre de 2005. RIT N° 101-2005.

TRIBUNAL ORAL EN LO PENAL DE COPIAPÓ. 5 de julio de 2011. RIT N° 46-2011.

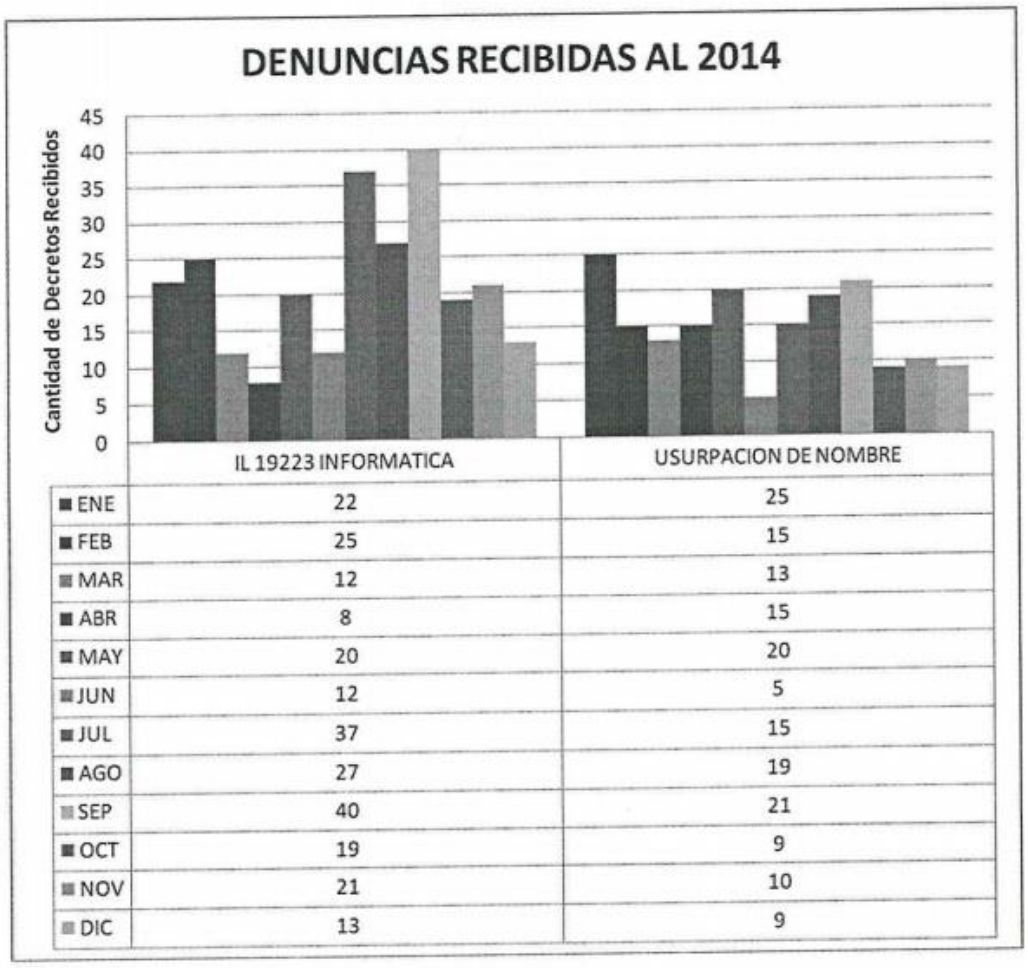
TRIBUNAL ORAL EN LO PENAL DE VIÑA DEL MAR. 16 de septiembre de 2011.

CORTE DE APELACIONES DE RANCAGUA. 12 de diciembre de 2011. ROL N° 359-2011.

ANEXO 1.

I. Información proporcionada por la Brigada del Cibercrimen de la Policía de Investigaciones.

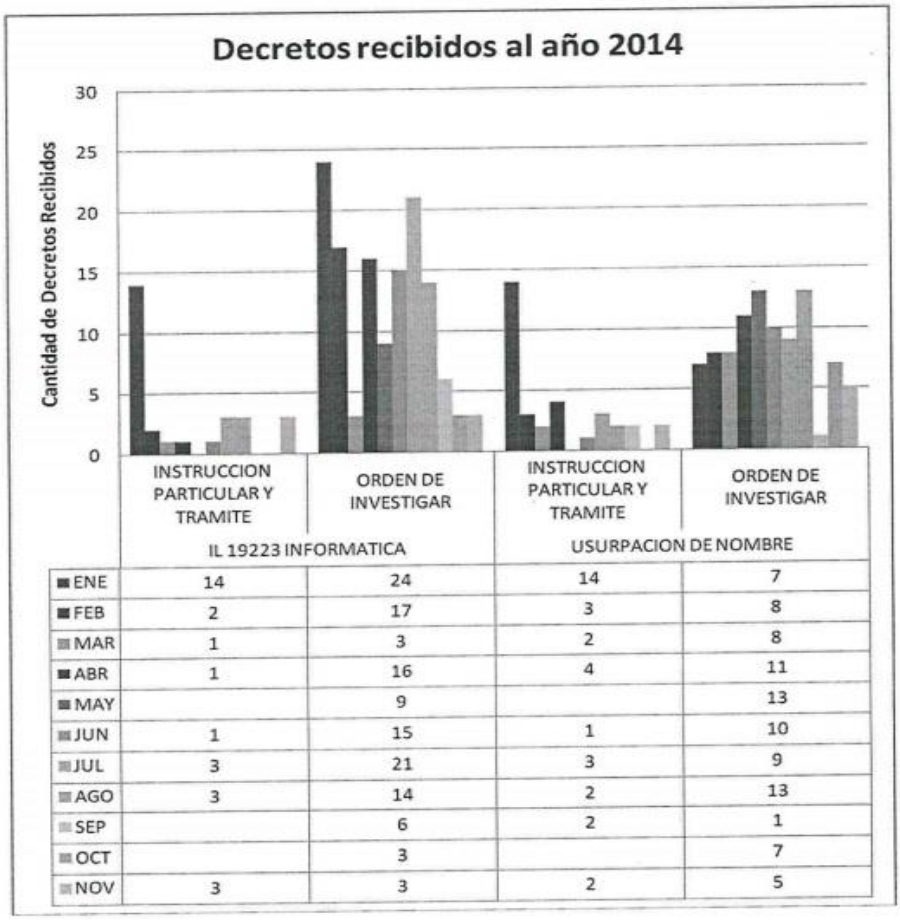
Gráfico Nº 1.



	IL 19223 INFORMATICA	USURPACION DE NOMBRE
ENE	22	25
FEB	25	15
MAR	12	13
ABR	8	15
MAY	20	20
JUN	12	5
JUL	37	15
AGO	27	19
SEP	40	21
OCT	19	9
NOV	21	10
DIC	13	9

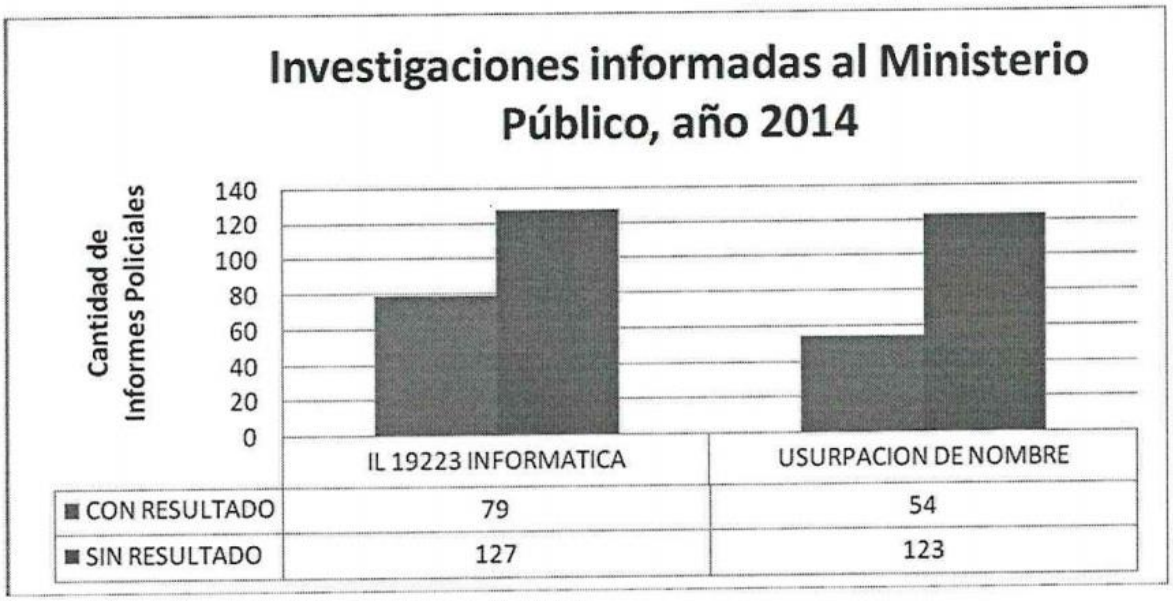
Gráfico Nº 2.

Gráfico Nº 3.



	IL 19223 INFORMATICA		USURPACION DE NOMBRE	
	INSTRUCCION PARTICULAR Y TRAMITE	ORDEN DE INVESTIGAR	INSTRUCCION PARTICULAR Y TRAMITE	ORDEN DE INVESTIGAR
ENE	14	24	14	7
FEB	2	17	3	8
MAR	1	3	2	8
ABR	1	16	4	11
MAY		9		13
JUN	1	15	1	10
JUL	3	21	3	9
AGO	3	14	2	13
SEP		6	2	1
OCT		3		7
NOV	3	3	2	5

Gráfico Nº 4.


Investigaciones informadas al Ministerio Público, año 2014
Cantidad de Informes Policiales
140
120
100
80
60
40
20
0
IL 19223 INFORMATICA
USURPACION DE NOMBRE
CON RESULTADO
79
54
SIN RESULTADO
127
123

II. Información proporcionada por el Ministerio Público.

Figura Nº 1.

Ficha técnica	
Período	2013 - 2014
Unidades de medida	Querellas Ingresadas
Desagregaciones	Año y Estado de la Causa
Cobertura	A escala nacional.
Definición del contenido	Querellas Ingresadas por el delito usurpación de nombre.
Metodología	La información fue extraída y procesada desde la base de datos del Sistema de Apoyo a los Fiscales (SAF) de acuerdo con los criterios establecidos en el documento metodológico *Técnicas de conteo en los Informes Estadísticos*, elaborado en mayo de 2009 por la División de Estudios, Evaluación, Control y Desarrollo de la Gestión. Disponible en: http://fnintranet/RepositorioIntraMinpu/Archivos/rbarreira/documentos/estudios/INF_TECNICAS_CONTEO.pdf
Fuente de la información	Tablas SAFEST del Sistema de Apoyo a los Fiscales (SAF), base de datos del Ministerio Público.
Fecha de captura de la información desde la base de datos	31-01-2015
Delitos considerados	309

Figura Nº 2.

QUERELLAS INGRESADAS POR EL DELITO USURPACION DE NOMBRE PERIODO DE AÑOS: 2013-2014							
		AÑO 2013			AÑO 2014		Total general
TERMINOS	TIPO DE TERMINOS	VIGENTE	TERMINADO	SUSPENDIDO	VIGENTE	TERMINADO	
TERMINO FACULTATIVO	ARCHIVO PROVISIONAL		1			2	3
	DECISION DE NO PERSEVERAR		15			4	19
	INCOMPETENCIA				1		1
	PRINCIPIO DE OPORTUNIDAD		1				1
SALIDA JUDICIAL	ACUERDO REPARATORIO		1	1			2
	SENTENCIA DEFINITIVA CONDENATORIA		3				3
	SOBRESEIMIENTO DEFINITIVO		2			2	4
	SUSPENSION CONDICIONAL DEL PROCEDIMIENTO		1	1			2
OTROS TERMINOS	AGRUPACION A OTRO CASO		1			7	8
VIGENTE		21			42		63
Total general		21	25	2	43	15	106

ANEXO 2.

Entrevista con el Comisario Santiago David Núñez de la Brigada del Cibercrimen de la Policía de Investigaciones. Miércoles 8 de abril de 2015

1. Cuando se realizan denuncias, ¿Qué se reclama como suplantado? Nombre, apellido, imágenes, u otros elementos distintivos de la identidad.

-¿Cuando viene la persona como tal?

Nosotras: claro, cuando viene la víctima.

- Cuando viene la víctima, independiente de si tiene todos los antecedentes, que serían ideales al momento de hacer una denuncia, ya que se llegaría al "ConR", al con resultado cuando se termine con la investigación. Por eso nosotros tratamos siempre de pedir el máximo de información, pero la gente por lo general no llega con ese máximo de información.

Nosotras: La pregunta es ¿qué siente la persona que ha sido suplantada? No quien ha sido el autor de la suplantación, sino que la persona dice "me suplantaron porque están usando mi nombre o me suplantaron porque están utilizando mis fotos".

- Por lo general, para ellos todo.

Nosotras: ¿Cualquier cosa?

- Si, cualquier cosa, por lo general dicen por las fotos o por el nombre completo, se sienten igual de afectadas, para ellos...

Nosotras: O sea ¿tampoco hay una distinción acá si la persona llega reclamando las fotos o el nombre, sino todo se toma como usurpación de identidad?

- Claro, hay que pensar también que la persona se siente dañada, necesita que alguien la escuchen, y por ende, es un derecho de cualquiera,

independiente si se configura o no se configure el delito, el hecho. Es un derecho de la persona venir y decir “yo vengo a denunciar por tal cosa”, aunque uno diga “mira lo tuyo tal vez, por ejemplo una estafa, no cuadra, falta algo acá, no está el perjuicio económico, “pero es que yo vengo”… se toma la denuncia independiente de. Y por esto, después como va a la fiscalía, el fiscal obviamente está en su derecho o, en este caso de archivar la causa o nace una orden de investigar, y dentro de la orden de investigar que se agoten todas las diligencias posibles. Y ahí nosotros nuevamente empezamos a solicitar más información, que en ese momento por nerviosismo, por tiempo, etc. no lo entregó la persona en su momento.

Nosotras: o sea en su opinión, la generalidad de las personas tienen un conocimiento colectivo de la suplantación de identidad, vienen en esa postura a denunciar. No solo con el nombre, sino que también incluyen las imágenes.

- Correcto, ellos se ven afectados y dicen, por ejemplo, una foto que fue trucada, porque puede ser la cara y trucada con Photoshop en un cuerpo que no corresponde, de una mujer que esta desnuda y ahí dicen “mire”

Nosotras: El artículo que ampara la suplantación de identidad, según nuestra opinión, es el artículo 214 del Código Penal, el que habla de usurpación de nombre, en parte porque el Código es de 1874, y en el Congreso hubo un informe de un asistente técnico jurídico que estableció que sólo había que estarse a lo literal de las palabras de la ley, que sólo protege el nombre, ya que la identidad era demasiado amplia y confusa. Pero según nuestro criterio, creemos que el nombre no es suficiente, y que la norma también abarca otros elementos de la identidad como las fotografías, corroborándose por las denuncias hechas por las mismas personas.

- Otro ejemplo, es que la gente a veces viene a denunciar ese mismo hecho, pero por el Nickname de la persona, su alias. Y para ellos se ven igual de afectados. Y ahí estamos entrando a que ella fue amenazada de muerte en un mundo virtual, y fue amenazada desde México, otra jurisdicción. Las leyes cómo las cuadran. Pero que me dice a mí que el día de mañana ese que está en México tiene un contacto acá en Chile y

efectivamente el otro día amanece muerta. ¿se la tomo o no se la tomo la denuncia? Se la tomo. Y eso lo hacemos. Sin ir más lejos ayer pasó algo así, era otra jurisdicción, era prácticamente como un alias de una persona, es un tema.

2. ¿Quiénes pueden llegar a ser víctimas de la usurpación de identidad en redes sociales?

- ¿En qué sentido? En el universo de las personas?

Nosotras: Claro. ¿Cualquier persona, personas más o menos conocidas, políticos? ¿Cuál es el perfil de la víctima?

- Es un universo amplio, no tiene un margen. Cualquier persona, incluso, por ejemplo alguien se molestó, es típico, sucede cuando alguien de su mismo entorno le cayó mal algo y automáticamente se puede producir este tema. Ahora, lamentablemente en el Facebook mi cantidad de amigos que tengo son 4.000, 3.000, ahora ¿quién de esos fue? O sea, no hay un control interno de cada una de las personas en ese sentido. O sea, el universo es amplio.

3. ¿Cuál es el perfil de quien comete este tipo de delitos? Por ejemplo, según la edad, según la experticia informática, etc.

- También es relativo, porque por lo general obviamente una persona con poco de conocimiento informático… hoy en día está todo en la red, tú no sabes algo, tú no sabes hackear, o ser un lamer o ser alguien con un poquito más de conocimiento, YouTube ¿cómo hackear tal cosa? Entro, modifico, arreglo, cambio, modifico, y listo. Y tú cuando llegas en este caso al imputado y lo ves que es menor de edad, que puede tener trece, no hay límites, nada. Sin conocimientos, me meto y busco y después llego a ser incluso un experto en el área, porque navegué, navegué y me metí en el tema. Y ni siquiera estudio.

Nosotras: Es decir, el acceso a Internet puede transformar perfectamente a un ciudadano común y corriente en sujeto activo de un delito informático.

- Correcto.

4. De acuerdo a las denuncias, ¿cuál es la red social en la que se da más el delito de suplantación de identidad?

- Facebook. Lejos Facebook. A las personas no les gusta cuando les dicen "pero mire, hagamos una cosa, vamos a denunciar y después posterior a esto dígale a su hijo que cierre Facebook, y esto para toda la familia, para el hijo, mamá, papá, a todos. Y nadie va a querer hacerlo y no lo hacen. Lamentablemente si yo subo una foto o algo mío a la red es de todos, o sea ok, cierro este Facebook, mañana me apareció acá la foto, pasado y pasado en otros lugares.

5. ¿Cuáles son las principales dificultades a la hora de investigar estos delitos?

- La respuesta por parte de otras entidades. Por ejemplo, de repente la respuesta de Google, de Facebook.

Nosotras: O sea, el apoyo por parte de las redes sociales en la investigación.

- Claro, eso debería ser como.. se deberían acotarse los tiempos de respuestas. Ese es el tema.

Nosotras: ¿Y respecto de las víctimas?

- Claro, por ejemplo, yo necesito algo urgente de Facebook, lo tengo que pedir a través de un correo, como corresponde, pero el tiempo de respuesta debiera ser óptimo. Se entiende porque es una empresa privada, no es un organismo público que debiera responder de forma inmediata. Y en este caso nosotros tenemos que esperar su respuesta cuando ellos determinen. Están los conductos, están las formas, pero los tiempos no son óptimos.

Nosotras: Y ¿eso afecta, por ejemplo, el resultado de la investigación?

- Afecta, porque, por ejemplo, no está considerado acá el tema de la

flagrancia. ¿Qué pasa con la flagrancia? La flagrancia necesito, ejemplo de eso, andan dos colegas, uno que está allá con unos audífonos, que está viendo en un monitor grande varias imágenes, y vas a encontrar que de repente está viendo pornografía, está editando videos, está revisando, y eso es una herramienta grande técnica donde él puede revisar y puede ir encontrando y a medida que va encontrando va editando y va viendo, va buscando videos y viendo videos, alguien entra por acá y puede decir oh! Mira está viendo pornografía, oye la persona, es un policía". Y él está analizando un disco duro o en este caso un celular donde hay evidencia, y esa evidencia tienen que ejecutarla en el momento, porque ellos están trabajando en la flagrancia del día de ayer. Con otro tema que está bien fuerte en este tema del video de Fifi, de una menor de edad que anda ahí por las redes, donde tuvo relaciones con varios otros menores de edad. Esa diligencia está de ayer y yo necesitaban hacer en el momento, en el sitio, todo el proceso investigativo, ¿por qué? Por el tema tiempo. Y ahí justo en otros casos se necesita eso mismo de Facebook, obtener más información al respecto. ¿Y cómo yo la obtengo? Si yo le digo a ellos que la necesito en 24 horas, porque estamos en flagrancia y estamos trabajando sobre eso. ¿Por qué? Porque yo el otro día temprano, tengo que entregar el informe policial al Fiscal. Eso no figura en esas estadísticas, que también involucra mucho tiempo y mucho desgaste para obtener ese resultado, con resultado, "ConR".

Nosotras: Y en cuanto al tiempo ¿también afecta, por ejemplo, a los efectos del delito, en cuanto a su ramificación?, por ejemplo, por el hecho de que no le entreguen al tiro la información, crea mayores efectos o efectos más nocivos que de la suplantación de identidad, como por ejemplo, si le hubieran entregado oportunamente la información habría quedado en eso y no se habría expandido a otros delitos.

- Claro, se traduce… si lo miramos desde el punto de vista de la detención de la persona, o sea, nosotros buscamos la detención de ese imputado que esta cometiendo este tipo de delitos, claro, mientras antes lo detengamos, obviamente la detención va a ser, vamos a evitar que siga cometiendo otros hechos.

6. La Brigada del Cibercrimen tiene conocimiento de que el pasado

noviembre se presentó en la Cámara de Diputados un proyecto de Ley que pretende sancionar con una pena aumentada en un grado más multa la usurpación de identidad que se da en Internet y las redes sociales. ¿Qué opina de esto?

- Explicando que es nuevo en la Brigada del cibercrimen, desconoce del proyecto que se presentó en la cámara de diputados que persigue la modificación del articulo 214 del Código Penal referente a la suplantación de identidad en el contexto de Internet y las redes sociales.

Nosotras: Pero cuál es su opinión en que la pena de presidio menor en su grado mínimo se aumente a presidio menor en su grado medio más multa de 5 a 30 UTM, cuando la suplantación de identidad se produce en Internet y las redes sociales.

- Bien me parece. Porque actualmente ¿qué penas tiene? Con eso se busca que la gente, al momento de ver, con algo ejemplificador, se detuvo a la persona, tuvo una pena mayor, alguien que después quiera hacer lo mismo, obviamente la va a pensar dos veces. Si ya es un incremento, está bien.

ANEXO 3.

Entrevista a María Angélica Silva, Asesora legislativa de la Diputada maría José Hoffmann. Lunes 13 de Abril, 2015.

- Lo que pasa es que todo lo que dice relación con delitos cometidos a través de redes sociales no están contemplados en nuestra legislación, entonces son delitos que no están tipificados, es una forma de cometerlos que hoy día no está contemplado en la ley. Entonces hay unos que son más puristas, hay una corriente mucho más purista que dicen que ni siquiera es necesario, porque se debe aplicar el delito tal cual está contemplado en el Código Penal y que, en definitiva, con eso se estaría configurando y, por lo tanto, da lo mismo si se comete a través de una web o una red social, pero el delito en el fondo no varía. El planteamiento de este proyecto plantea algo distinto desde ese punto de vista, está con la corriente contraria digamos, que establece que en definitiva hoy día cometer estos delitos a través de las redes sociales, llámense Facebook, página web, etc. facilita mucho la comisión de ese delito, entonces, incluso no hace mucho la propia Ministra Rincón fue objeto, no sé si ustedes se enteraron, fue objeto de una situación como ésta. Aparece un mail que ella manda, como si fuera su Gmail pidiendo plata, y esto es como el dato freak recibió ella plata, y después ella tuvo que hacer la aclaración de que le habían hackeado su correo electrónico, que ella no estaba haciendo eso, que mil disculpas a todos los que habían sido destinatarios de esa situación, porque aquí que es lo grave, lo grave por un lado, obviamente, es que suplanten tu identidad, hay derechos afectados ¿cierto?, pero más grave aún es cuando a partir de ese delito generas daños a terceros, y ese tercero piensa que soy yo, que también soy víctima. Por eso en este proyecto se contempla precisamente una agravante y además multa en el caso, que eso es la novedad, porque este delito no contempla multa, entonces lo que se intenta es que tenga un efecto más bien disuasivo, en términos que hoy día esto, en la actualidad queda en nada, o sea, quien suplante la identidad como en este caso o quien suplante el perfil del Facebook finalmente, por un tema de prueba también, queda absolutamente en cero. Entonces, lo que nosotros pretendemos con este proyecto, lo que pretende la diputada, es que al menos, primero esté contemplado en la legislación, porque hoy día cada vez es más la comisión de estos delitos a través de las redes sociales, ha crecido de manera exponencial, porque es mucho más fácil, y el engaño, o fraude, estafa … los puristas dicen “bueno si es delito de estafa que apliquemos la pena de la

estafa" y quedan en eso, pero nosotros creemos que hoy día es tan simple acceder al perfil de otro, o hackear el perfil de un tercero y a través de ese perfil, de ese engaño, de esa estafa cometer otro delito y a su vez, generar daños a terceros, que creemos que eso tiene que ser tipificado y en eso creemos que la legislación actual está como un poco obsoleta, no recoge esa realidad.

Nosotras: Si bien lo que expuso está dentro del que preguntaremos, ahora haremos una serie de preguntas más ordenadas.

1. ¿Cuál es la motivación detrás del proyecto? ¿Es la falta de regulación?

- A nuestro juicio, hay una falta de regulación en esta materia, por lo mismo, o sea, todos los delitos que hoy día se cometen a través de las redes sociales de alguna forma no están tipificados, y al aplicarse el delito por así decirlo base la penalidad es muy baja. Entonces la motivación de esto, y sobre todo a la hora de incluir la multa como parte de la sanción es precisamente generar un efecto disuasivo respecto de quien comete ese delito.

2. Entendiendo que el delito en la actualidad es conocido como "usurpación de nombre" y ustedes en el proyecto lo denominan "suplantación de identidad", ¿qué entienden por identidad? Porque hay quienes lo entienden como sólo el nombre.

- Acá puede ser, cuando estamos hablando de identidad podemos estar hablando de una persona natural, estamos hablando de una persona jurídica incluso, no necesariamente sólo del nombre, porque la identidad va más allá de sólo el nombre, o sea, nosotras no nos conocemos, por ejemplo el mail que les mandé, claro tenía otros fines ¿cierto?, pero yo les mando y ustedes ven en el pie de firma que es "María Angélica Silva Troncoso", ustedes creen que yo soy la asesora parlamentaria, legislativa de la Diputada Hoffmann y resulta que nos conocemos y yo les digo "pero cuando si yo no les mandé un mail", quizás en ese caso no hay una consecuencia mayor, porque el contenido del mail era la coordinación de una reunión. Pero si yo les digo, hubiese puesto ahí "mira sí, pero esta reunión… no sé, tiene un

cobro o tiene un costo de honorarios" y ustedes después le dicen a la Diputada "oiga Diputada nos escribió su asesora, pero nos está cobrando fíjese", y después llega la Diputada y me dice "oye ¿y cómo que estás cobrando?, te volviste loca." … "oye pero si yo nunca mandé ese mail, no fui yo". Entonces, hay ahí un tema y… ¿quién lo regula?

Nosotras: Entonces si usted pudiera definir identidad, ¿cómo la definiría?

- Identidad. Lo han definido varios. Yo no sé si aquí (mirando el proyecto) nosotros lo definimos.

Nosotras: No, en el proyecto no.

- (Pausa) La identidad, o sea, a ver … desde el punto de vista nuestro va más allá del nombre y contiene todos los atributos de la personalidad, ya sea persona natural o jurídica. O sea con domicilio, el nombre, o sea, todo lo que conlleva los atributos de la personalidad.

Nosotras: O sea, la imagen, la voz, también serían distintos elementos de la identidad para ustedes.

- Sí, claro.

3. ¿Qué abarcaría la suplantación de identidad? En otras palabras, ¿cuáles serían los aspectos de la identidad que se verían protegidos por la norma? El nombre, fotografías, la voz, etc.

- Claro, en el fondo lo que nosotros estamos tratando ... eso está aquí en el proyecto, lo que nosotros queremos salvaguardar, a diferencia, incluso, de lo que establece unos delitos informáticos, que no sé si ustedes lo vieron, que ahí lo que se protege es el contenido de la información, o sea, lo que se sanciona es más bien la vulneración de los contenido.

Nosotras: Como las bases de datos.

- Claro, pero no se está, en definitiva, protegiendo a la persona o la identidad.

Nosotras: Entonces, por ejemplo en un caso concreto, si a alguien le roban sólo las fotos, pero no el nombre, ¿también sería un caso de usurpación de identidad?

- Es mi imagen, sí, claro. Lo que pasa es que hay distintas … o sea, pueden haber situaciones unas más graves que otras ¿me entienden?. Ocupar solamente el nombre del perfil o la imagen u ocupar incluso el nombre y la imagen, pero no causar daños a terceros, porque aquí lo grave es cuando tú además con eso le causas un daño a un otro y donde el tercero cree que soy yo la que está estafando y resulta que yo soy tan víctima como ese tercero de la suplantación, primero porque suplantaron mi nombre o mi imagen, mi identidad digamos, pero además hay un tercero afectado, por ejemplo, por un delito de estafa que cree que fui yo y que cree que yo soy la estafadora y me podría incluso demandar a mí. Y resulta que yo aquí no tengo arte ni parte, hay un otro que hizo, cometió el engaño para que ese tercero creyera que fui yo, y ese tercero, incluso, vio afectado su patrimonio por ejemplo, porque fue estafado ¿te fijas?. Y hay uno que se enriqueció a costa mía y de ese tercero.

4. En el contexto de las redes sociales ¿esto se extendería a los datos sensibles que proporcionan las personas? Por ejemplo, las contraseñas.

- Lo que pasa es que hoy día las contraseñas son posibles de ser hackeadas, entonces esas personas acceden al perfil completo de uno y también a la privacidad de uno, a la intimidad de uno, porque de repente hay cosas que uno … el correo electrónico, ustedes tienen su propio correo, ustedes interactúan y llega alguien que da con la contraseña de ustedes, ingresan al perfil de ustedes, a los correos de ustedes y a quienes con quien han interactuado. Eso también es parte de la vulneración.

5. ¿Qué se busca proteger con el inciso segundo propuesto por el proyecto? ¿Persigue amparar el mismo bien jurídico –a nuestro parecer el derecho a la identidad personal- que establece el artículo 214 o uno nuevo y distinto?

- Lo que nosotros queremos es proteger la identidad de la persona, más allá del nombre, y a su vez protegerlo de delitos que podrían cometer terceros a esa persona, por eso el inciso segundo habla de que en caso que "dicha suplantación se realizare a través de Internet, redes sociales o cualquier otro medio, ocasionando daños a terceros, será castigado con presidio menor en su grado medio y multa de 5 a 30 UTM." O sea, hay un aumento en un grado más la multa. Y la multa, bueno, ese rango… a ver, la penalidad, uno querría también a ratos sancionarlo con una multa mucho más alta, pero en materia penal las multas no puede uno aplicarlas en forma antojadiza, o sea, por ejemplo colocar 100 UTM, porque está eso definido en el Código Penal, la gradualidad de las multas. Entonces revisando más menos estas multas que se establecieron, las sacamos homologando un poco al delito de estafa, a fin de poder innovar en una sanción aumentando el grado, pero también generando la multa, que podría ser un elemento disuasivo.

Nosotras: Entonces sería un bien jurídico distinto. ¿o uno complementario?

- Más bien complementario.

6. Si se busca modificar el artículo 214, que tradicionalmente se cree protege el nombre, pero a nuestro parecer protege el derecho a la identidad, ¿por qué dentro de los argumentos del proyecto se estima que el bien jurídico protegido es la inviolabilidad de las comunicaciones privadas, regulado en el artículo 19 Nº 4 y 5 de la Constitución Política de la República?

- Lo que pasa es que uno de los argumentos es justamente lo que establece la Profesora Ángela Vivanco, porque esa mención viene a reforzar de que aquí estamos frente a un delito, o sea, porque ella dice: "Cuando se invade cualquier tipo de cuenta privada o se usa la imagen sin previo aviso, se viola el artículo 19 números 4 y 5 de la Constitución Política de la República de Chile, es decir, nuestra Constitución establece una inviolabilidad de las comunicaciones privadas. Hacerlo es un delito." Eso es así, o sea, que todos tenemos derecho a nuestra privacidad en relación a las comunicaciones, y cuando esa privacidad se ve menoscabada, se ve violentada o violada, estamos frente a la comisión de un delito. Y eso relacionado a lo que podría

ser una cuenta de correo electrónico, lo que dice relación a una, por ejemplo, página de Facebook o una página web que yo podría tener como María Angélica Silva, donde lo que es público está tal vez en mi perfil, pero lo que yo quiero mantener privado como podría ser la mensajería donde uno interactúa en Facebook que uno lo manda vía privada, ¿cierto? O los correos electrónicos, por eso si te mando un correo electrónico a ti, no es un correo masivo, es un correo dirigido a tu persona, y bajo el alero de una comunicación privada entre nosotras. No lo estoy publicando ni en mi perfil, ni en Twitter, donde cualquier persona lo podría ver, sino que es una interacción entre privados, eso está protegido.

Nosotras: Pero, por ejemplo, en el caso delas cuentas que son creadas falsas, ahí no existiría ese problema, porque si yo me creo una cuenta con un nombre determinado, pero con la foto de otra persona, sin que corresponda tanto nombre como imagen al mismo individuo, en ese caso no habría inviolabilidad de las comunicaciones privadas, porque no hay una comunicación.

- Depende, porque si la verdadera persona ve su foto asociado al nombre de otro diría "oye pero si esa soy yo" y podría reclamar que hay usurpación de identidad.

Nosotras: Pero no inviolabilidad de las comunicaciones privadas, porque son bienes jurídicos distintos.

- Claro, son bienes jurídicos distintos, pero por eso acá lo que nosotros estamos protegiendo son dos cosas: una, la identidad de las personas que va mucho más allá del nombre; y también las comunicaciones privadas, porque, vuelvo a insistir, el perfil de un Facebook, un correo electrónico, por ejemplo, imagínate lo que le sucede a la Ministra Rincón, le hackean su mail, aparece ella pidiendo plata, y más encima se configura el objetivo, porque le depositan plata. Entonces, tú dices "oye momentito", o sea, ella se entera porque hay gente que después la empieza llamar y le dice "oye te transferí". Y resulta que ella nunca pidió esa plata obviamente, y tuvo que hacer toda esta aclaración, hizo la denuncia a la Fiscalía y esta situación fue hace poco, habrá sido en el verano, así que ustedes busquen en las redes y se van a encontrar con el caso de ella.

Hay dos parlamentarias acá que también les pasó lo mismo, Andrea Molina creo que fue una y Camila Vallejo otra. Y también un empresario, no me acuerdo cuál.

Nosotras: Luksic, a través de Twitter.

- También. Fue un Twitter, tienen toda la razón. Y ahí también quedó en nada.

Nosotras: Pero ahí fue otro caso y fue una sentencia absolutoria, era inocente quien creo la cuenta falsa, porque se consideró que no era una usurpación de identidad, sino que era una cuenta burlesca, porque la cuenta era de los Luksic, pero la foto era dinero cayendo del cielo. Entonces la persona firmaba como Luksic, pero el Tribunal consideró que no se podía estimar como una cuenta falsa, ya que nadie en su sano juicio podía considerar que eso era verdadero.

- Claro. Pero, bueno, hay unas situaciones que son más complejas que otras, esa en el fondo, el Tribunal determinó no sancionar, pero hay otras donde hoy día … por ejemplo, el tema de pedir plata o de estafar a alguien vía redes sociales o página o Facebook o correo es súper común … crear una página pornográfica con la cara de mujeres y el cuerpo de otras y eso publicarlo, o sea, tú lo subes a la red y está ahí en el ciberespacio a vista y paciencia de todo el mundo, y eso no puede quedar en la impunidad.

7. Si el aumento de las denuncias por usurpación de nombre no es alarmante, por cuanto el incremento porcentual (en cifras del proyecto, considerando los años 2012 y 2013, fue de un 14% a un 49%) de ellas es alto, mas en la realidad no son muchas los reclamos que se realizan por este ilícito, ¿por qué requerir una modificación del Código Penal en su artículo 214 cuando ésta no es una norma muy utilizada?

- Nosotros creemos que sí, obviamente, por algo hicimos el proyecto. A ver, el artículo 214 la penalidad que tiene es súper baja, es de presidio menor en su grado mínimo, eso al final con suerte es firma en la práctica, pese a que dice “sin perjuicio de la pena que pudiere corresponderle a

consecuencia del daño que en su fama o intereses ocasionare a la persona cuyo nombre ha usurpado." Cómo me afecta a mí que alguien haya ocupado mi nombre ¿cierto?, o mi imagen, mi identidad. Pero nosotros qué creemos, que esto justamente obedece a que esta forma de cometer delitos es bastante posterior a la ley, porque en esa época ninguna posibilidad de que esa comisión de delitos estuviese contemplada en la ley, o sea, era como muy futurista. Y te digo, nosotros creemos que en general todo lo que dice relación con las redes… mira hubo otro proyecto, nada que ver con esto, que decía relación con los medios de comunicación social, que iba dirigida a los diarios electrónicos, y que también fue iniciativa de la diputada, mira se tergiversó de una manera nada que ver, porque al final los diarios electrónicos están todos apoyando ese proyecto. Se dijo que aquí iban a tener que pagar, que había una vulneración a la libertad de expresión, absolutamente lejano a esto, porque lo que ese proyecto pretendía, y que tampoco estaba contemplado en la legislación, es que los diarios electrónicos que pretendieran o quisieran serlo, iban a ser reconocidos como diarios. La Ley de Prensa define lo que es diario, y lo único que hicimos a través de ese proyecto es permitir que los diarios electrónicos, porque todo el mundo hablaba de medios electrónicos, tuviesen la posibilidad de ser considerados diarios para todos los efectos legales. Porque actualmente, uno de los pocos diarios electrónicos que son considerados "diario" es El Mostrador, que ya está como a la altura de La Tercera, El Mercurio, La Segunda, que pueden hacer avisajes legales, comerciales, y así se financia. No cualquier diario electrónico lo puede hacer. Entonces lo que nosotros pretendíamos con ese proyecto, que aquel diario electrónico que quiera ser considerado diario, cumpliendo obviamente con la normativa, pudiese acceder a los mismos beneficios que un diario convencional. Una cuestión que parece súper simple, pero que la Ley no lo contempla tampoco, porque los diarios electrónicos tampoco en esa época existían. Entonces hay mucho vacío en relación al uso de las Tecnologías o de las Web en nuestra legislación y yo creo que en eso estamos al debe, no solamente desde el punto de vista penal sino que desde todo punto de vista. Porque hoy día cada vez se va a utilizar menos el papel y va a ser todo vía electrónica, entonces, incluso los sistemas de seguridad es un tema también. Piensen ustedes, por ejemplo, en el tema de la firma electrónica, o sea, como que a uno le da un poco de nervio, porque y si de repente aparezco firmando un documento que nada que ver, ahí como que falta profundizar más y yo creo

que estos proyectos pueden aportar, pueden ser un aporte, pero no es la solución tampoco, porque no está abordando el tema de manera integral ¿te fijas?.

Nosotras: Es que es nuevo al final todo lo que es electrónico, computacional, Internet. Siempre van haber nuevos desafíos.

- Claro, y cada vez unos se empieza a dar cuenta que hay tras formas de ir vulnerando los sistemas, o sea, se han metido hasta en los sistemas de seguridad de la Casa Blanca, y que se suponen que son como lo más seguro, y ahí están los más capos, cabezones, hasta los hackers están ahí, y han sido vulnerados, entonces uno dice "chuta, tenemos que sentarnos a trabajar en estos temas", no esperar a que quede una embarrada para decir "ahora vamos a legislar". Que es lo que está pasando hoy en el contexto nacional, con el financiamiento de las campañas, está la escoba, "chuta, ahora es el momento de corregir". Para qué vamos a esperar a que quede una hecatombe para … o sea, porque no empezamos a generar proyectos y que además cuenten con el respaldo del ejecutivo para que tengan la urgencia que corresponde, porque finalmente esto es mucho más común que el escándalo que tenemos en el país por el tema político, y es mucho más cercano a la gente, están mucho más expuestos a la comunidad, y son cosas que de repente generan frustración en las personas, porque nosotros conocemos los casos que por el nombre del afectado salen a la luz pública, pero esto es más común de lo que uno cree y genera frustración que una situación como esa quede en la impunidad o que ni siquiera le signifique una multa, o sea, por ultimo tuvo que pagar 30 UTM de multa, aunque esa plata no vaya para mí, pero no importa, o sea, el tipo no se la llevó gratis, le significó, hubo ahí una sanción.

8. En relación a las querellas por el delito de usurpación de nombre y en virtud de información que obtuvimos del ministerio público, por la ley de transparencia, podemos establecer que entre los años 2013 y 2014, de 106 querellas ingresadas, sólo 3 arribaron a una sentencia definitiva condenatoria -habiendo algunas vigentes-, mientras que la mayoría concluyeron en término facultativo o salidas alternativas.
   Entonces, si la mayoría de los imputados no terminan cumpliendo una pena privativa de libertad como estipula actualmente el artículo

214, ¿es necesario aumentar en un grado la sanción? Porque el aumento de pena que ustedes proponen calza dentro de los requisitos para por lo menos optar por alguna salida alternativa.

- Sí, lo que pasa acá es que el mérito del inciso segundo va dirigido, o sea coloca el énfasis en el hecho de que a partir de esta usurpación de identidad se cause daños a terceros como por ejemplo que a través de esa usurpación se genere otro delito que es la estafa, o sea ahí estamos aplicando un grado más y la multa porque hoy día en el sistema no está contemplada la multa, entonces más allá de las salidas alternativas lo que nosotros queremos generar un efecto disuasivo en relación a estos casos. Imagínate los que han llegado a término: 6.

Nosotras: No, 3 condenatorias.

- Entonces es bajísimo. Por eso, tal vez la multa permita que sin aplicar el presidio menor en su grado medio si pudiese contemplarse la multa como parte de la condena y eso ya es un avance.

Nosotras: O sea que la intención al final es la multa.

- Si tú me preguntas, yo creo que ese es el aporte o el mérito del proyecto, contemplar una multa que hasta el día de hoy no está consagrada en lo que dice relación a la usurpación de identidad.

Nosotras: Las dos siguientes preguntas tienen relación entre sí, por lo que vamos a hacer juntas la 9 y la 10.

9. Primero, ¿por qué razón se persigue aumentar la pena en un grado cuando la suplantación de identidad se de en el contexto de Internet y las redes sociales?, ¿Es por eso?, o bien,

10. En cuanto al inciso segundo que se quiere agregar al artículo 214, ¿a qué se refieren con la frase “ocasionando daños a terceros”? Porque por lo que hemos hablado ese es el motivo, no es sea por las redes sociales, sino que el motivo al final es porque ocasione daños a terceros, más que sea en el contexto de las redes sociales.

- No, y también por el medio de comisión, absolutamente, porque en el fondo es mucho más fácil acceder a la comisión de este delito vía redes sociales porque el sistema es más vulnerable, lo que lo hace mucho más grave. Pareciera contradictorio, pero precisamente por la facilidad, porque no sé, de repente tal vez el falsificar una cédula de identidad -que podría ser falsificación de instrumento público-, o yo ocupo la cédula de otro, eso tal vez el modus operandi podría ser más difícil de realizar en términos de que quede perfecto y sea creíble, pero acá vía redes como no tienes a la persona al frente, aquí opera la confianza y la buena fe. O sea por ejemplo nosotras compartimos un correo y tú crees que soy yo y yo creo que eres tú y no necesariamente… ¿Cuántas veces se le ha quedado a alguien abierto el correo y llega otro y empieza a escribir tonteras? Por molestar, por broma. Y la persona que recibe dice ¡oye, pero como me escribiste eso!, pero ¿cuándo?, yo no te he escrito jamás eso.

Claro, eso no da para delito, puede ser una broma de mal gusto si ustedes quieren, pero es mucho más fácil. Entonces hoy día hackear una cuenta o llegar a la clave o contraseña de un blog, de un Facebook no cuesta nada, o sea los tipos que saben, lo hacen.

Entonces, el nombre, la imagen, la fama de una persona tiene valor, aunque sea el barrendero de la esquina, tiene un valor y no tiene por qué ser vulnerado. Entonces que alguien vía red social, vía electrónica vulnere esa identidad, mi identidad, algo que es tan propio por una red… y a eso sumado que cause daño a un tercero, porque es copulativo, a nuestro juicio es más grave.

Nosotras: entonces ocasionando daños a terceros, significa que ¿la tercera persona crea algo de quien se le está suplantando la identidad? o ¿se le ocasione un daño por ejemplo patrimonial, como que haya una estafa de por medio?

- Claro, un daño patrimonial porque en el fondo acá hay tres actores: el que suplanta, el suplantado, que es la primera víctima, y además este tercero que se ve “estafado” o “engañado” por este suplantado, porque ese es el mérito. El suplantador está saliendo libre de polvo y paja y para el tercero

soy yo, la suplantada, la que estoy cometiendo el delito. Soy yo la que lo está estafando, soy yo la que lo está engañando, soy yo la que le está cobrando X cosa que no corresponde. Él no se va a dirigir al suplantador, se va a dirigir a mí porque para él soy yo la que lo estafó, entonces yo soy la doble víctima, porque yo a su vez tengo que probar que hay un suplantador que es el que maquinó todo y que hizo que tanto yo como el tercero fuéramos víctimas del suplantador. Eso a nuestro juicio es…

Nosotras: entonces en caso de que se realizara sólo a través de internet o redes sociales, ¿de igual manera se aumentaría un grado en la pena? porque si dice que es copulativo…

- (Leyendo el proyecto) Dice: En caso que dicha suplantación se realizare a través de internet, redes sociales o cualquier otro medio, ocasionando daños a terceros…

Nosotras: Entonces ¿es copulativo?

- Claro, es copulativo.

Nosotras: o sea si falta cualquiera de los dos no se aumenta la pena

- Ojo acá porque dice "cualquier otro medio", podría ser no vía redes sociales.

Nosotras: Pero cuando falte cualquiera de los dos se penaría por el inciso primero del artículo 214. O sea que si se produce este delito por redes sociales se castiga por el inciso primero, sin multa.

Bueno, la pregunta once ya ha sido respondida a lo largo de la conversación, pero dice:

11. ¿Es el perjuicio que se le provoca a terceros la razón por la cual se busca una sanción más estricta o sólo la circunstancia que la usurpación de identidad se dé en una plataforma virtual?

Nosotras: Bueno, ahora entendimos que es copulativo, porque de la lectura del proyecto, se entiende que sólo es porque la usurpación sea por medio de

una plataforma virtual, en el proyecto no se explica que es copulativo el requisito. El “ocasionando daños a terceros” no se explica, por lo que se entiende que se sanciona con mayor pena porque se da en internet.

- Y porque ocasiona daños a terceros.

Nosotras: claro, ahora nos queda claro esto.
Pregunta doce, en caso de ser…

- Perdón, porque en el inciso primero, en el que está dice: “el que usurpare el nombre de otro será castigado con presidio menor en su grado mínimo, sin perjuicio de la pena que pudiere corresponderle a consecuencia del daño que en su fama o intereses ocasionare a la persona cuyo nombre ha usurpado”. Eso es el tipo que me usurpa o se hace un perfil con mi nombre y me muestra desnuda o me estafa. Ahí se aplica el inciso primero.

El problema es cuando yo aparezco usurpada y “cometiendo un delito” afectando a un tercero, porque no es el usurpador el que lo comete, sino que es el usurpado. En el fondo es doble víctima, porque es usurpado como lo establece el inciso primero, pero además soy delincuente, porque no sé, estafé a alguien.

12. En caso de ser el daño a terceros, como bien lo hemos establecido, el fundamento del aumento de la pena, ¿es aquella razón suficiente para proporcionar una mayor sanción, cuando si un tercero es afectado tendrá mejores recursos para amparar sus derechos que el artículo 214 que claramente busca proteger sólo a quien es víctima de una suplantación de identidad?

- Sí, claro, el tendrá mejores derechos, pero ¿y yo? ¿qué pasa conmigo? Porque en el fondo lo que yo quiero es que ese tipo, el usurpador, por el hecho de haber cometido un delito, porque al final el estafador es él, me ocupa a mí, pero el estafador es él, yo quiero que por eso, a él, la pena sea más alta.

Nosotras: O sea se mira desde el punto de vista de la víctima, de la primera víctima, no de la segunda.

- Sí, claro.

13. Si se aumenta en un grado el presidio que se aplica, ¿cuál es el fundamento detrás de la multa? En el proyecto se habla del "carácter disuasivo de la multa" ¿qué quisieron decir con esto? De todas maneras ya lo hemos hablado durante la conversación.

- En el fondo, en nuestro sistema tenemos claro que esta penalidad, que lamentablemente desde el punto de vista de… o sea, uno no podría… es súper complicado cuando uno revisa el código penal, porque nace naturalmente el ser más duro con las sanciones, pero tiene que haber una cierta coherencia y una cierta proporcionalidad en relación a otros delitos. Voy a decir una aberración, pero esto no podría tener una penalidad mayor que la violación por decir algo, por el sólo hecho de que no queremos que se cometa, porque además tampoco va a generar ese efecto. Pero sí lo que se pretende es dar una señal, contemplar una situación que a nuestro juicio no está contemplada en nuestra legislación, que es la comisión de este delito de usurpación o suplantación de identidad con daños a terceros. Entonces la multa efectivamente tiene un efecto disuasivo porque podría quedar con firma quincenal o firma mensual el tipo y le sigue costando cero peso. En el fondo lo que queremos es que… a una persona natural, 30 UTM no es tan poca plata, ¿te fijas?, entonces que le duela el bolsillo, porque hoy día incluso estas personas, que son hacker es casi una entretención el lograr la vulneración del sistema aunque no hagan nada, o sea, hoy día hay algunos que llegan a eso, o sea, como un mérito casi personal: ¡lo logré, lo hice!
No generan el daño, llegan hasta ahí. Quizá el duelo del perfil nunca se enteró, pero el tipo queda con la satisfacción de que lo logró, pero el otro, que finalmente va más allá y a su vez comete el delito ¿cómo se las va a llevar gratis?, ¿con una firma mensual?, porque no da ni siquiera para arraigo este asunto.
Entonces, uno dice bueno, cuando ya a las personas les empieza a afectar el bolsillo lo piensan o toman sus resguardos.

Nosotras: ¿Y no pensaron por ejemplo en agregar la multa pero no subir en un grado el presidio? Porque si la multa es disuasiva, no entendemos por qué se sube además el presidio.

- Lo pensamos en su minuto, pero no es lo mismo que tu usurpes la identidad de una persona a que tú la usurpes, si además a propósito de esa usurpación le causas un daño a un tercero, eso es más grave todavía. Y vuelvo a insistir, esto es una trilogía, el usurpador, el usurpado y la víctima en este caso del usurpador y del "usurpado", porque la víctima final del delito de estafa está seguro que fui yo, y yo a él le digo: "pero si no fui yo, a mí me usurparon la identidad, se hicieron pasar por mí, no fui yo la que te estafó". Eso para mí tiene una carga adicional en materia de prueba, yo tengo que probar además que efectivamente no fui, sino que hubo otro que lo hizo precisamente con ese fin, por lo que ahí el dolo está clarísimo, porque en el fondo la persona no lo hace directamente, sino que lo hace a través del usurpado, por lo que es más grave, porque el tipo maquina la situación, de cómo hacerlo, qué modus operandi va a usar para que ese crea que fue esta otra persona, que no fui yo. Por lo que hay más elaboración en la forma de cometer el delito.

14. Esta última pregunta ha ya sido respondida a lo largo de la entrevista, pero según su opinión, ¿cuál es el beneficio que conllevaría la inclusión del inciso segundo en el artículo 214? ¿Cuál es el aporte del mismo, que supuestamente hoy no es satisfecho con el precepto mencionado?

- Bueno, un poco lo que hemos hablado todo este rato, es que aquí se tienen que dar los requisitos de manera copulativa, o sea acá tiene que generarse de partida una forma de comisión de la usurpación de identidad ya sea vía redes sociales o cualquier otro más el daño a terceros. Nosotros consideramos que el sólo artículo 214 en su inciso primero o único inciso como es actualmente no contempla la situación de que a partir de esta usurpación de identidad se genere un daño a terceras personas, y también creemos que desde el punto de vista de la persona que es usurpada el daño es aún mayor, porque entre medio, mientras se está dando todo… coloquémonos en una situación real, esta víctima que fue estafada piensa que soy yo y supongamos que lo publica en un medio de comunicación, porque esa persona genuinamente cree que yo fui, y tiene las pruebas, porque es mi perfil, es mi cara o efectivamente era mi correo y dice: ¡oye, María Angélica Silva es una sinvergüenza! Y lo publica en televisión, en

radio, en Twitter, etc. ¿Qué pasa conmigo? Yo soy tan víctima como ella, ¿y el daño que me hicieron a mí? En mi imagen, en mi honra, en mi fama, me puede costar el trabajo, puede afectar la imagen de mis hijos, los pueden molestar en el colegio, ¿te fijas? Esa es la realidad que se da hoy día con las redes sociales como están a nadie le cuesta nada subir una foto y hacerte de otra, si esta cuestión es demasiado simultaneo e inmediato. Por eso consideramos que es tan grave, porque en el desarrollo del juicio que estamos probando o desde que se inicia el juicio la persona me pudo haber hecho… Cuánta gente incluso prefiere en vez de recurrir a la justicia mandar una carta al diario, publicarlo porque siente que es mucho efectivo y que siente que de esa forma sí se está haciendo justicia, pasa mucho. Contemos sobre todo –que no tiene nada que ver contesto- cuando ha habido abuso con las tiendas, con Entel, Movistar, lo que sea: ¡son unos ladrones!, etc., y ahí aparecen las empresas a resolver los problemas, pero una vez que salió en los medios, porque se viralizó en las redes sociales o salió en televisión, y es así. Y se ahorraron el juicio, los meses, o años de pagos de los abogados y lo resolvieron de esa manera.

Entonces hoy día es tan fácil que la honra, la fama, la imagen de una persona se vea expuesta frente a situaciones como esta, no cuesta nada. Esa es la razón por la cual nos motivamos a sancionar un grado más, que tampoco es mucho al ser honesta, al menos cuando estamos hablando de presidio menor. Nos motivó incluso a innovar con el tema de la multa, porque es un delito que finalmente no lo considera y creemos que podría ser un elemento disuasivo, aparte que tampoco queremos –si esto fuera pena efectiva- tampoco queremos gente en la cárcel por una situación como esta, tiene que haber proporcionalidad, ¿cierto? Este tipo con suerte va a tener firma mensual, lo que es casi lo mismo que nada, o sea, no me inhibe a no hacerlo nuevamente. Entonces aplicamos la multa y dice: “me sancionaron” a no sé, el tope que es 30 UTM, ya 15, 10 UTM, igual duele el bolsillo, porque estamos hablando de que esto se empezó a masificar, a hacer más común en un nivel o perfil de gente que no está pensando una gran estafa como para decir que “30 UTM son nada”, es otro perfil. Son tipos especializados en informática o que andan con poco dinero y por eso quieren estafar, porque necesitan el dinero.

ANEXO 4.

Entrevista a Natalia Alviña, Asesora legislativa del Diputado Ramón Farías. Martes 28 de Abril, 2015.

1. ¿Cuál es la motivación detrás del proyecto?

- Este proyecto tenemos que saber primero que es de autoría propia de otro diputado, que si no me equivoco es la diputada Hoffmann, la cual ustedes saben cómo se inician las mociones parlamentarias que finalmente es un autor y necesita el patrocinio de no más de diez diputados, hasta diez ¿cierto? El diputado cuando la diputada le ofreció poder ser patrocinante, le interesó mucho, pero no sólo porque sea del tema de la usurpación de identidad, sino que a él (diputado Farías) le interesa todo lo que esté ligado con Internet y cómo se controla hoy día el tema de Internet. Se ha descubierto y hemos descubierto a lo largo de varios estudios y situaciones que no siempre está regulado, tenemos una Ley que es la Ley que ahora rige todos estos delitos informáticos, pero es muy breve tiene sólo cuatro artículos, por tanto, cuando se le propuso, esto a él le gustó, porque él (diputado Farías), tanto incluso tenemos Ministros u otras personas de la cámara de diputados han estado involucrados en esto. Ellos, obviamente, y hasta nosotros yo creo que alguna vez nos han hackeado algo, se han hecho pasar por nosotros, en un mail o en Facebook, alguien ha tenido la oportunidad, entonces es de proteger en este sentido a las personas, porque la Ley que tenemos ahora protege la información que está en Internet, protege los datos, pero no tenemos una que proteja a la persona, a su identidad ni a ella misma, y eso es lo que le motiva a él (diputado Farías) a colaborar y a patrocinar este proyecto.

2. Entendiendo que el delito en la actualidad es conocido como "usurpación de nombre" y ustedes en el proyecto lo denominan "suplantación de identidad", ¿qué entienden por identidad?

- Claramente ahí nosotros lo conversamos con el diputado, existe un pequeño, al no ser los autores, pero sí patrocinantes, problema yo creo de términos ¿ya?, porque la sanción, o sea, el tipo penal es la usurpación, "suplantación" no existe o no está tipificado dentro de la parte penal, sí existe en el ámbito público, sí en el área administrativa se habla de suplantación, pero no se habla en el ámbito penal. Correctamente la

utilización debería ser, la palabra exacta debería ser “usurpación”, sobre todo como va un inciso segundo del artículo señalado, pero nosotros no notamos ese detalle, entonces ¿qué entendemos por identidad? Me imagino, o sea es que les puedo dar una definición quizás más mía. A ver, tratando de enfocar cómo lo ve el diputado… la identidad sería como pasar por la persona de uno, digámoslo en palabras, para que no hablemos tan técnico, es ponerse o hacerse pasar por uno y tomar conductas, posiciones y comentarios a nombre mío, es simplemente como tomar… quiero decirlo simple…

Nosotras: En realidad la pregunta va más dirigida a qué es “identidad”, más allá de la usurpación de la identidad o de la suplantación de la identidad. Cómo definirías “identidad”? Sólo identidad.

- ¿Cómo definiría identidad? Pienso yo, podría ser como mi nombre, mi persona, mis actos y cómo yo me veo frente al resto. Podría ser algo así, tratando de orientarlo al proyecto en cuestión.

3. ¿Qué abarcaría la suplantación de identidad? En otras palabras, ¿cuáles serían los aspectos de la identidad que se verían protegidos por la norma? El nombre, fotografías, la voz, etc.

- El nombre, la imagen, el uso de los datos, de todos los datos, o sea, todos los datos que sean personales, que sean privados. Quizás ahí esté la diferencia, quizás que me afecten un mail, que me roben la información del mail quizás ya está cubierto por la Ley, lo que buscamos o lo que buscan los diputados, por lo menos, lo que logro que el diputado patrocinara es cuidar la imagen de uno, a eso como a la identidad, la imagen mía y cómo se relaciona todo lo que puedan hacer, sean delitos o no delitos, cómo afectan mi imagen, mi vida personal y cómo yo me veo ante la sociedad.

Nosotras: O sea, el diputado lo relaciona directamente con la reputación de la persona.

-Exactamente. Por ejemplo, tenemos el caso, no sé si ustedes vieron a una Ministra, que se metieron a su mail.

Nosotras: Sí, la Ministra Rincón.

- Le hackearon el mail, bueno quizás mandan mails, pero era pidiendo plata para fondos y todo, entonces hay dos cosas distintas, estamos atacando primero "oye violaste mi mail, mi información, tomaste mis contactos", ya te metiste en mi área privada, todo lo que quieras. Pero después de eso, la dejan su imagen como, a ver, su comportamiento ético o moral frente al resto, porque claro está no había campaña y todo, entonces se puede, se afecta la imagen de ella como persona.

4. En el contexto de las redes sociales ¿esto se extendería a los datos sensibles que proporcionan las personas? Por ejemplo, las contraseñas.

- Bueno, el proyecto… o sea para poder acceder a un medio que sea tuyo, el mail, Twitter, el Facebook, obviamente el primer paso es a través de las contraseñas, no sé si la pregunta va quizás también sacando como para otros medios, como mi contraseña del banco, pero es como la fase inicial entiendo. O sea, yo creo que para poder acceder, y por lo que nosotros sabemos para poder acceder a cualquier tipo de… o sea, puede estar la suplantación, o sea, la usurpación, puede ser creando algo nuevo, como también accediendo a lo mío, por ejemplo a mi cuenta de Facebook, o a la cuenta del Diputado, que también les ha pasado que han tratado de hackearle su cuenta y que va a través de este robo de claves por ejemplo. Pero también puede suceder que le saquen fotos, que donde él tiene fotos tanto en los medios y creen, por ejemplo, un Facebook nuevo y también se comete el mismo … en este caso pretendemos que haya como una misma sanción para que sea el mismo delito, que tiene distintas vías, pero estamos llegando al fin que es como proteger la imagen y a la persona.

5. ¿Qué se busca proteger con el inciso segundo propuesto por el proyecto? ¿Persigue amparar el mismo bien jurídico –a nuestro parecer el derecho a la identidad personal- que establece el artículo 214 o uno nuevo y distinto?

- Es el mismo, mira por lo menos como nosotros lo vimos, y en la propuesta que nosotros analizamos, recordando claro está que él (diputado Farías) es

patrocinante y no autor. Es una intención, lamentablemente nuestro Código Penal tiene muchos años ¿cierto? La materia de la usurpación viene hace más de treinta, sólo unas pequeñas modificaciones algunos años atrás, si son como veinte o treinta años atrás que hubo alguna pequeña modificación que se ha discutido sobre el tema, pero claro está que tiene, yo creo, que un cierto el mismo objetivo ¿o no? que es proteger a la persona, su identidad, sus datos, su imagen, pero ahora extenderlo a algo que no existía hacia años atrás. El Código Penal tiene 170 años, esta materia de la usurpación se ha ido tratando con más profundidad desde como hace veinte o treinta años atrás, como que nos ha interesado un poquito más y es extenderlo a lo que tenemos hoy e ir actualizándolo conforme a la modernidad. Hace diez años atrás no teníamos Facebook como lo tenemos ahora, no existía el Twitter, y así como avanza la tecnología también se está avanzando y se propicia, se dan los elementos para aquellas personas que quieran hacer alguna de estas acciones tan dañinas a través de estos medios, entonces lo que se pretende o lo que se busca es ampliar como a la modernidad, ¿por qué es más grave?, porque establece una sanción distinta o por lo menos sube en un grado la pena y viene dado por la accesibilidad también que tiene Internet ¿ya? Por la masividad que tiene, no es lo mismo que yo, no sé, lo diga en el diario local de un pueblito en el sur a que lo escriba en una red social, porque tiene mayor alcance, incluso, no sólo nacional, sino que tiene alcance mundial.

6. Si se busca modificar el artículo 214, que tradicionalmente se cree protege el nombre, pero a nuestro parecer protege el derecho a la identidad, ¿por qué dentro de los argumentos del proyecto se estima que el bien jurídico protegido es la inviolabilidad de las comunicaciones privadas, regulado en el artículo 19 Nº 4 y 5 de la Constitución Política de la República?

- Sí, lo nombran como argumento citando, si no me equivoco, a una abogada.

Nosotras: Sí, la profesora Vivanco de la Universidad Católica.

- Sí, están citando a esta profesora. Realmente más como se consideraron los fundamentos del proyecto, como les dije la autoría es de otro, se comparte un poco en el sentido de la honra, porque acuérdense que en estos

artículos igual se habla sobre la vida privada y la honra de las personas, si no me equivoco que es el 4 ¿cierto? Pero también citan a otro profesor...

Nosotras: Sí, Hernán Corral.

- Pero lo que motiva en este caso al diputado Farías a firmar viene más allá incluso del trasfondo, porque él tiene como un pensamiento quizás más amplio que no lo puedo plasmar, porque no lo escribió él, pero sí… no podría decirte por qué justo citan a esa persona, se puede entender un poco, si tú me lo preguntas como a mí por el tema legal quizás se puede entender un poco, tratar de encontrar el fundamento y un apoyo legal.
¿Cuál es el fundamento del diputado de firmar?

Nosotras: No fue por el fundamento, sino que fue por la solicitud.

- Exacto, por la idea general, para marcar el punto y poder legislar sobre el tema, si esto se acoge a tramitación en teoría se aprueba en general, se tendrían que recibir audiencias, y es poner un tema súper importante en la palestra y hacerlo crecer, porque nosotros podemos tener un pensamiento, pero al recibir audiencias de gente que esté interesada en la materia o que sepa de la materia, se puede llegar a legislar incluso puede ser el artículo que ustedes ven puede variar completamente a través de las indicaciones, pero es el trasfondo, la idea, el fin el que al diputado le llama la atención y lo que él quiere ayudar a legislar sobre eso, entonces por eso accedió a patrocinar el proyecto.

7. Si el aumento de las denuncias por usurpación de nombre no es alarmante, por cuanto el incremento porcentual (el cambio en cifras del proyecto, considerando los años 2012 y 2013, fue de un 14% a un 49%) de ellas es alto, más en la realidad no son muchas los reclamos que se realizan por este ilícito, ¿por qué requerir una modificación del Código Penal en su artículo 214 cuando ésta no es una norma muy utilizada?

- Yo creo que aquí hay un desconocimiento, lo conversamos también con el diputado y creemos que existe una falta de información, precisamente porque hay una falta de regulación, donde no está claro, donde acá vemos

“usurpar” lo que ya tenemos, la usurpación de identidad no sabemos en qué casos aplica o no, y el tema de Internet es más complejo aún, porque si no, como les decía revisamos estos cuatro artículos que tenemos ahora, que casi todo es a la información, a los datos, la gente, yo creo, no sabe que … y porque no está claro tampoco en la ley, sino no estaría la iniciativa del proyecto, no sabe si denunciar o no.
Yo creo que uno está en la casa, y me hackean o alguien crea una cuenta ¿es delito o no es delito? ¿Denuncio o no denuncio? Yo creo que también hay una falta de denuncias, pero si hacemos un sondeo o por lo menos tú hablas o yo hablo con mis conocidos, yo creo que 7 de cada 10 o más, estoy diciendo un número… nos ha pasado algo así, porque a mí me ha pasado, al diputado le ha pasado y yo creo que hasta ustedes les ha pasado.

Nosotras: A nosotras no. Pero en la práctica, lo que pasa es que la gente, por lo general, tiene conocimiento como colectivo casi que el artículo 214 se utiliza para la suplantación de identidad, más allá de que éste tipifica la usurpación de nombre, sólo abarcando el nombre, la gente lo utiliza de forma más amplia. De hecho, gracias a la Brigada del Cibercrimen pudimos constatar esto. Pero los casos que llegan, por ejemplo, a tribunales, e incluso, los casos que terminan en una sentencia son tan pocos que en realidad este aumento se ve alto, pero en la realidad es realmente muy bajo, entonces no entendemos muy bien por qué modificar si en realidad el artículo en sí, no tanto por las denuncias, no se utiliza casi nada.

- Yo creo que va en base a eso, yo creo que la gente no denuncia, porque no sabe que puede denunciar. O sea, es una apreciación que nosotros conversando podemos llegar, pero de que existe la preocupación, existe. Y se nos ha manifestado en varias formas, precisamente porque el diputado está muy interesado en todo lo que es el tema cibernético. Nos llegan muchos correos, él tiene correo y atendemos gente vía correo, o vía teléfono o presencial, y te preguntan o de repente conversando: “y sabe qué, el otro día me pasó esto, y qué hago”, y realmente la gente no sabe que puede configurar un delito, que existe una forma de tratar de frenar, de que se encuentre una sanción, no se conoce y yo creo que también, porque no sólo falta esta modificación, como bien el diputado ha señalado, y si no me equivoco también lo ha señalado la prensa, se necesita una Ley informática nueva, o sea, que abarque todo y dé más atribuciones a la gente de

Cibercrimen, que haga una concordancia con el Código Penal, y que se integren delitos que ahora no están tipificados en la Ley, pero que existen.

8. En relación a las querellas por el delito de usurpación de nombre y en virtud de información que obtuvimos del ministerio público, por la ley de transparencia, podemos establecer que entre los años 2013 y 2014, de 106 querellas ingresadas, sólo 3 arribaron a una sentencia definitiva condenatoria -habiendo algunas vigentes-, mientras que la mayoría concluyeron en término facultativo o salidas alternativas.

   Entonces, si la mayoría de los imputados no terminan cumpliendo una pena privativa de libertad como estipula actualmente el artículo 214, ¿es necesario aumentar en un grado la sanción? Porque el aumento de pena que ustedes proponen calza dentro de los requisitos para por lo menos optar por alguna salida alternativa.

- Claro, bueno ahí hay que ver cada caso, cada caso es distinto, o sea, hay pocos, primero partamos por esta base que nosotros podemos pensar que no se denuncia tanto como debería, no se llevan, de ahí vienen todo como el archivo, todo lo que podemos encontrar antes de llegar a un juicio, pero yo creo que enfocarlo como al no estar tipificado conforme a estas reglas modernas, que es lo que buscan de cierto modo el artículo, se hace más difícil también a los magistrados y a los jueces a aplicar sanción. Obviamente, si es sólo de identidad a secas, porque si conlleva otro delito ya ahí empiezan las penas y todo, ahí ya podemos encontrar que van a haber sanciones mayores, pero ¿por qué legislarlo a pesar de que haya tan poco? En cifras, porque seguimos creyendo que es necesario, que quizás al haber una regulación, quizás al subir las penas va a ser más disuasivo y a la vez la gente se va a animar al saber que ya está legislado como tal, no hay que inducirlo… "bueno que esto se puede aplicar aquí, no" … que esté como tal, la gente por un lado va a denunciar más y a la vez donde es más masivo, más fácil acceso, estos delitos por eso van a subir la pena, porque en teoría cometer ese delito es mucho más fácil que quizás falsificar un carné, que conlleva otros delitos y todo. Entonces… se me fue la pregunta.

Nosotras: Por el número tan bajo de sentencias condenatorias ¿por qué subir la pena? Más allá del por qué legislar sobre la usurpación de identidad en las redes sociales o Internet, ¿por qué subir la pena?

- Yo creo que ahí van los dos puntos, o sea, dicho todo lo anterior, por un lado que es necesario que se tipifique, que la gente denuncie, y por el otro lado, una sanción donde es de fácil accesibilidad, una sanción que pueda ser un poco, por así decirlo, preventiva quizás, que realmente desincentive la comisión de estos delitos y a la vez obviamente donde puede… no necesita ser un … podría ser cualquier persona el que cayera en este delito ¿cierto? Entonces aumentar o el aumento de pena en teoría se entendiera más como preventivo. Bueno, hay sanciones, y donde más encima concurren un montón de causales, "sabe, bueno ya si lo hago total donde es el mínimo, el menor en grado mínimo, más todas las atenuantes, bueno listo una firmita y estoy listo". No, quizás al haber una sanción mayor, y quizás lo que se busca a través del proyecto es una sanción mayor que nos va a poder incentivar a "bueno oye aunque tenga atenuantes y todo, pero ésta es más alta" y tomar una seriedad conforme al tema.

9. ¿Por qué razón se persigue aumentar la pena en un grado cuando la suplantación de identidad se de en el contexto de Internet y las redes sociales? ¿es sólo por esto?

- Bueno, yo creo que por lo mismo que les decía antes de lo conversado con el equipo, es la masividad, el fácil acceso.

Nosotras: O sea, es por el hecho que se da en un contexto informático.

- Es porque se da en un contexto informático. Precisamente por el tema de accesibilidad, de masividad de las redes.

10. En cuanto al inciso segundo que se quiere agregar al artículo, ¿a qué se refieren con la frase "ocasionando daños a terceros"?

- Voy a leer (mirando el proyecto). Bueno, nosotros teníamos igual sus reparos, marcar el punto, una cosa del reparo por ejemplo del tema

“cualquier otro medio” podría darse bueno para cualquier otro medio… cualquier otro medio quizás debería haber sido, por ejemplo, Internet.
“Ocasionando daños a terceros”, por lo menos, el diputado cuando patrocinó lo entendió como utilizar este medio no sólo obviamente para dañar mi imagen, sino, por ejemplo, me suplantan a mí, no sólo dañan mi imagen, sino que a mi nombre dañan a otro o también me dañan a mí, porque la persona que está suplantando no sólo me está haciendo este daño, sino que está causando daños, por ejemplo, en un caso de que suplantaron la identidad del diputado y le hacen bullying a otra persona. De todas maneras, la redacción es totalmente conversable de hecho nosotros ya tenemos como, en vistos, unos tres más o menos indicaciones que podrían entrar, pero lo importante por ahora era plantear el punto y dejarlo ahí, por eso les digo que él (diputado Farías) patrocinó, no es el autor material, pero si… y poder trabajar y ya entrando y ya empezándose a tramitar esto es totalmente como una plasticina que se puede moldear hasta llegar algo más.

Nosotras: O sea, el “ocasionando daños a terceros” puede ser cualquier otro daño, no tiene que ser solamente patrimonial, puede ser también, por ejemplo, el bullying u otro…

- Sí, exactamente. Cualquier daño.

11. ¿Es el perjuicio que se le provoca a terceros la razón por la cual se busca una sanción más estricta o sólo la circunstancia que la usurpación de identidad se dé en una plataforma virtual?

- O sea, la pena, como les dije antes nosotros buscábamos… o sea, por qué subía más era por este medio que es más masivo y todo, pero, o sea, el hecho de causar daños a terceros y daños a la misma persona es considerable, pero también se podría ver implicada en el artículo como está. Si vemos acá (leyendo): “el que usurpara el nombre de otro… ocasionada a la persona cuyo nombre…”. Ahí el anterior ve en su propio nombre ¿cierto? O sea, el que está. Sí, o sea, busca o buscamos … me estoy tratando en mi mente mientras les hablo buscando las ideas de cuando lo conversamos con él (diputado Farías) y yo estoy tratando de transmitirles las ideas de él … sí, es un poco de los dos: me dañan, ya están en … dañamos y esta plataforma que es tan masiva que generalmente en los casos que nosotros hemos conocido de usurpación o de suplantación … no es la palabra correcta como

lo conversábamos, pero primero es desprestigiar a la persona por quien yo me hago pasar claro está, y a través de la red podemos hacer estafas, podemos hacer un montón de cosas, que son delito, pero no está en la Ley de ninguna manera tipificado el que yo más encima le esté haciendo daño como Luli, por ejemplo, otras personas y en las redes sociales lo que hace más daño viene dado precisamente por el tema de la red social, que no le estoy robando, no le estoy estafando, pero estoy o injuriando o calumniando o infiriendo daño, entonces podría ser una mezcla de los dos. Obviamente, el acento también va en el tema de la masividad de la red social.

12. En caso de ser el daño a terceros el fundamento del aumento de la pena, ¿es aquella razón suficiente para proporcionar una mayor sanción, cuando si un terceros es afectado tendrá mejores recursos para amparar sus derechos que el artículo 214 que claramente busca proteger sólo a quien es víctima de una suplantación de identidad?

Nosotras: Nos estamos poniendo en el caso de que el motivo sea el daño a terceros, y que este tercero como víctima de un delito conexo, como el delito de estafa, por ejemplo, tiene otros recursos judiciales mucho mejores que el artículo 214, con penas, si es que uno quisiera, más altas.

- Claro, podrían ir a concurso de delitos y se podría quedar uno afuera. Mira, como les dije realmente, ya así a tan profundidad yo creo que en su momento no analizamos el punto exacto, yo creo que, mira partiendo nosotros creemos que al tiro "suplantación" tendría que ser por "usurpación", "cualquier otro medio" es peligroso, porque entonces ya no es sólo Internet, redes sociales o cualquier otro medio, tendría que ser otro medio electrónico, buscar la adecuación.

Nosotras: Porque "cualquier otro medio" podría ser el plano físico, y al final eso sí está abarcado por el artículo 214 en su redacción actual. Nosotras hicimos esa lectura después.

- "Ocasionando daños a terceros", no sólo en la mirada del diputado cuando firmó era que yo le cause daños a terceros, sino ya el hecho de hacerlo por la plataforma, utilizar la plataforma para… yo al final entre que me enredo o no, pero prefiero explicarles así como por puntos. Ocasionar este daño a

terceros no es como excluyente, no es como si no ocasiono daños a terceros dejaría de existir, claro, tipificado así sí, nos tendríamos que ir al de arriba (mirando el artículo 214 propuesto por el proyecto, y haciendo alusión a su inciso primero) porque si no hay daños a terceros no existiría el inciso (por el inciso segundo que se pretende incluir con la iniciativa).

Nosotras: De hecho ese es un problema, que el artículo estaba escrito como si fueran, y gracias a una aclaración que nos hizo la asesora legislativa de la Diputada Hoffmann, son requisitos copulativos, entonces si falta uno, ya sea si falta o Internet o un daño a terceros sólo es necesario el inciso primero, o sea, el artículo como está.

Además como dice "cualquier otro medio" también incluye el medio físico, entonces al final lo único que se agrega es el "ocasionando daños a terceros". Nosotras cuando leímos el proyecto, lo hemos leído muchas veces, al final nos dimos cuenta que lo único que se agrega es "ocasionando daños a terceros", porque al decir otro medio incluye el inciso primero, entonces nos pareció muy raro.

- El diputado cuando me dijo que íbamos a firmar un proyecto, me dijo "conversémoslo", y después nos comunicaron ustedes y me dijo "a ya". Por eso lo empecé a leer, quizás me era más fácil para ordenarme de esa manera. Obviamente "suplantación" cambia, "a través de internet, redes sociales o cualquier otro medio" ya deja abierto de nuevo, que puede volver arriba, y el "ocasionando daños a terceros", yo creo, para la mirada del diputado es más el tema no sólo si le causo un daño a terceros, sino que uso esta plataforma que es tan masiva, esta plataforma que es en teoría de fácil acceso, de masividad y que puede causar mucho daño.

Nosotras: De hecho ese es nuestro "pero", que si hubiese sido redactado de esa forma, nosotras habríamos estado un poco más de acuerdo con el artículo propuesto, porque abarcaba internet y redes sociales, pero por el hecho de sólo exigir un daño a terceros, al final mientras no exista lo devuelve al pretendido inciso primero y no es necesario el cambio.

Claro, y al final todo el proyecto, esta conversación y la que tuvimos anteriormente con la asesora de la diputada Hoffmann, todo ha sido

enfocado a la importancia que tiene Internet en nuestras vidas, que todo el mundo ahora usa Internet, la facilidad que da Internet para cometer ilícitos como usurpar la identidad de otra persona, pero al final el proyecto en sí no es viable en la forma que se redactó, ya que sólo se refiere al daño a terceros, entonces es contradictorio.

- Por eso preferí leérselo y quizás ir apuntando … porque, claro, esto está en comisión de constitución, legislación y justicia, pero se pueden hacer llegar indicaciones y claro está que él (diputado Farías) quiere legislar, precisamente por la masividad del medio, pero dando esos … el "suplantación" que lo cambiaríamos por "usurpación" porque el delito está tipificado como "usurpación", el tema del "cualquier otro medio" que para nosotros como que nos abarca demasiado y el tema de que no es sólo para nosotros o no lo entendió él (diputado Farías) al firmarlo no como copulativos, sino que si se le hace a terceros, que terrible, pero más enfocado en la red, en el medio social. Y también sería otra indicación, acomodarlo quizás ahí, no sé si sacarlo, pero quizás hacer referencia que el mismo delito, o sea, el primer inciso se realiza a través de la plataforma, incorporar la plataforma, dada la masividad, la facilidad de acceso y todo eso.

13. Si se aumenta en un grado el presidio que se aplica, ¿cuál es el fundamento detrás de la multa? En el proyecto se habla del carácter disuasivo de la multa, ¿qué quisieron decir con esto?

- Mira, una apreciación como lo que creo que va detrás de poner una multa es precisamente donde les contaba cierto que, pucha ya subimos la escala, no es un delito… porque el delito lo podría cometer cualquiera, entonces empezamos con las atenuantes, por tanto, yo creo que habría gente dispuesta a decir "bueno, si total esto baja, voy a quedar con una firmita, quizás hice la maldad igual, da lo mismo, por que es una firma" o los procesos, lo mismo como ustedes me daban los datos de que muy pocos terminan, ya sea porque se archivan, por principio de oportunidad, todo lo que sea, el tema de imponer una multa y como bien se estableció en el proyecto yo creo que va en base a poder como reforzar, o sea, no sólo de esto me puedo librar, sino también va haber un … algo al bolsillo, y

lamentablemente a la gente la plata le duele. Disuasivo totalmente, lo que veo plasmado ahí.

Nosotras: Claro, el carácter disuasivo de la multa dice relación con que sobreviva la multa, y le duela al bolsillo a la persona que comete el ilícito, entonces al final no debería subirse el presidio, porque el presidio subido en un grado entra igualmente en la posibilidad de que quede en salida alternativa. Entonces al final, si lo único que quieren es que sobreviva la multa, no habría razón para subir el presidio en un grado. Entonces no se entiende cuál es la necesidad de subir el presidio en un grado además de sumarle la multa, si en realidad lo disuasivo es la multa, no es la pena de presidio mayor, porque igual se puede optar por salidas alternativas.

Claro, porque la firma va a quedar igual, si uno dice "bueno, cometo el delito y firmo igual", es lo mismo, sólo que la multa al final es la diferencia.

- No, pero igual podría… aparte de… porque podría ser la multa, pero también estábamos viendo que también podría conjugarse otro delito y no tener alguna salida y ser como por el otro delito.

Nosotras: Pero eso igual se puede en el escenario donde la multa sea más baja, igual pueden haber delitos conexos relacionados con la usurpación de identidad, y ahí habría un concurso ideal y al final se aplicaría la pena del delito con mayor pena, no se sumarían penas, entonces al final sólo estaría penándose con estafa o con calumnies e injurias, pero no se estaría penando como suplantación de identidad, entonces esto no tiene mucho sentido.

- No sé chiquillas, les encuentro razón realmente. Por eso, como les digo, el diputado no es abogado, no sé si ustedes saben, pero es actor, le encanta el tema, encontró que era un tema para apoyar, pero después de analizarlo nosotros y conversarlo, y ahora que ustedes me señalan como esta diferencia, sí me hace bastante sentido.

14. Según su opinión ¿Cuál es el beneficio que conllevaría la inclusión del inciso segundo en el artículo 214 del Código Penal? ¿Cuál es el aporte del mismo, que supuestamente hoy no es satisfecho con el precepto mencionado?

- Claramente y bajo la mirada y como el interés que tiene el diputado es la regulación de Internet.

Nosotras: Actualizar el Código Penal entonces.

- Sí, e incluir y modernizar no sólo esto, sino ellos están trabajando incluso con la propia diputada Hoffmann en Ley de medios y varias más.