revista pensamiento penal

La cuenta pendiente en nuestro País: Difusión de imágenes íntimas sin consentimiento y Suplantación de la identidad.

Nicole Jones Romero[1]

Resumen:

En el presente ensayo, la autora desarrolla la necesidad e importancia de modificar el Código Penal, incorporando distintas modalidades delictivas vinculadas con los sistemas informáticos. También analiza, la legislación comparada y cómo algunos de estos delitos, visualizados con perspectiva de género, califican como Violencia de Género Digital.

Palabras clave: *delito informático, ciber criminalidad, violencia de género digital, suplantación de identidad, pornovenganza, difusión de imágenes íntimas sin consentimiento, ciber identidad, derechos digitales.*

Sumario

[1] Profesora adjunta de Litigación Oral Penal de la Universidad Nacional del Nordeste. Especializada en Derecho Penal UAM. Cursando la Maestría de derecho penal de la UNNE.

I. Nuevos contextos sociales adaptados a la tecnología:

El contexto en el que vivimos, atravesando la pandemia por COVID19, nos ha obligado a transformarnos y a adaptarnos a toda esta tecnología. Y debido al aumento de su uso en todos los ámbitos, afecta tanto a adultos como jóvenes, ya sea en el home office y hasta las clases de colegios, con clases virtuales de todos los niveles, jardines, primarios y hasta universitarios.

Los niños en la actualidad, son los llamados "nativos digitales" porque desde que son muy pequeños aprenden a utilizar todos estos medios tecnológicos. Los "pandemials" término utilizado para llamar a los bebés que nacieron durante este contexto de COVID, de seguro que aprenden a utilizar herramientas digitales antes que a caminar.

Las redes sociales, videos de Youtube, Facebook, Snapchat, Instagram y Tik tok, también juegos como Amung us y Fornite se vuelven cada vez más virales, e interactivos ya que los niños y adolescentes, son los usuarios predilectos, y si no actúan con cuidado, también las víctimas predilectas. Si bien existen en algunas plataformas, barreras parentales o virtuales para niños, hay muchas que no tienen ni siquiera estas barreras y se vuelven muy peligrosas.

La inteligencia artificial también avanza a pasos gigantescos, los nuevos medios de billeteras virtuales, Homebanking, Mercado pago y hasta Criptomonedas. Y con todo este crecimiento y desarrollo, ha aumentado de manera desproporcionada y preocupante la actividad delictiva o los comúnmente llamados Ciberdelitos. Los intentos de estafas virtuales, casos de phishing, conocido como "El proceso fraudulento de la rama de la ingeniería social cuyo objetivo es adquirir información sensible como nombres de usuario, claves o datos de cuentas o tarjetas de crédito, a través de una comunicación electrónica, con un anzuelo que podría ser un link, formulario o documento, fingiendo ser una entidad de confianza, tal como un banco o una entidad gubernamental". "*Este tipo de delitos aumentaron un 3000% entre 2019 y 2020 según datos de UFECI*". afirma el Fiscal de la Unidad Especializada de Ciberdelincuencia, Horacio Azzolin.

Entonces este exponencial progreso de la tecnología en el mundo, nos está obligando a adaptarnos y por eso es sumamente necesario que establezcamos las estrategias y pasos a seguir para luchar contra estos nuevos desafíos que presenta la cibercriminalidad. Actualmente vivimos en la llamada "Era digital" y esta multiplicidad de fenómenos delictivos que surgieron por el mal uso de la tecnología

ha dejado al descubierto distintas lagunas de punición en el ordenamiento penal que los legisladores no pueden seguir ignorando. El protagonismo adquirido por el acoso, el hostigamiento, y la violencia cibernética, han evidenciado la necesidad de una política criminal clara de perseguir estas conductas y para ello, introducir en los códigos penales figuras penales específicas para reprimir estos atentados contra la libertad digital, como un derecho esencial, que tenemos aún detrás de una pantalla, como humanos y usuarios cibernéticos. Aunque en realidad dicha manifestación de conductas socialmente desvaloradas no hace más que reflejar el status quo del flujo de la violencia en nuestras modernas sociedades, en especial, respecto de la violencia de género, donde aquí lo único nuevo o diferente, es el medio por el cual se realiza la hipótesis fáctica, pero esto es algo que analizaremos con más profundidad más adelante.

II. Derecho Penal en jaque:

"Es innegable que el legislador que elaboró el Código Penal promulgado por el presidente Hipólito Yrigoyen el 29 de octubre de 1921 no podía prever los desarrollos tecnológicos que ocurrirían en los más de ochenta años posteriores, ni el impacto que ellos tendrían en los sistemas jurídicos."(1) [1] No están contempladas en muchos casos porque el Código Penal fue escrito para otra época en la que l[2]a información no era la materia prima del comercio y las actuales tecnologías de comunicación y almacenamiento y tratamiento de datos personales sólo eran objeto de relatos de ciencia ficción.

Es una regla constitucional del derecho penal moderno que no existe delito sin ley previa (art. 18, CN). Asimismo, tampoco es posible la interpretación penal por analogía. Lo cierto es que las nuevas tecnologías dejaron y seguirán dejando obsoletas muchas normas jurídicas. En materia de nuevas tecnologías, esa obsolescencia llevó, en muchos casos, a declarar la atipicidad de conductas disvaliosas que claramente merecían la protección penal, o a "estirar" la interpretación acotada que debe formular el juez del fuero. La reforma que se hizo en el año 2008 en la Argentina llegó tarde si se la compara con la evolución de la

(2) art. cit. 2011, Gustavo A. Arocena." La regulación de los delitos informáticos en el Código Penal argentino. Introducción a la Ley Nacional núm. 26.388"

legislación del delito informático a nivel internacional. Los países más avanzados en esta materia han reformado sus códigos penales en varias ocasiones a la fecha, tal el caso de Alemania o los Estados Unidos. Queda mucho por hacer en materia de criminalidad informática aún luego de la reforma del Código Penal en el año 2008 en materia de delitos informáticos (ley 26.388).

Ya en los tiempos del correo electrónico y las redes sociales, pero antes de la reforma, el art. 153, Cód. Penal, se hablaba de "despacho telegráfico o telefónico". El hurto del art. 162, Cód. Penal, era sólo de cosas muebles (aún sigue redactado igual). El delito de daño. La estafa recaía únicamente sobre personas y no sobre máquinas. Desde esos tiempos, el Código Penal no había sido actualizado por una reforma que diera una solución integral al problema de los delitos informáticos. (2)[3]

Que no exista aún legislación para la delincuencia informática es una circunstancia importante para poder determinar la eventual idoneidad de los tipos penales vigentes que utilizamos actualmente para acoger a estas conductas. Al aumentar significativamente estos casos, también aumenta la complejidad para investigarlos y al tiempo que crecen en cantidad y variedad, es notorio que cada vez existen más lagunas legales, donde el Derecho Penal aún no está preparado.

Sobre este tema particular, muchos especialistas desaconsejan la procedencia de reformas parciales y la importancia de una reforma general del Código Penal en la materia, se sumaban las características de los delitos informáticos, que justifican un tratamiento especializado. Entre otras características cabe resaltar la magnitud de los daños, la cada vez más frecuente naturaleza global e internacional de esta clase de delitos; la facilidad para cometerlos; y las dificultades para la investigación, que ha llevado a la necesidad cada vez mayor de la cooperación entre fuerzas de seguridad y el sector privado por la necesidad de preservar datos en el tráfico de ISP, servidores y, finalmente, las empresas de hosting y numerosas reconfiguraciones de los esquemas tradicionales con los cuales se concibe el derecho penal. Pese a ello, en general, se ha considerado que una gran cantidad de artículos del Código Penal resultan aplicables a las actividades desarrolladas en internet que veremos a continuación.(3)[4]

(3) Veáse PABLO A. PALAZZI “Los Delitos Informáticos en el Código Penal. Análisis de la ley 26.388”, 2016, pág 11.

(4) art. cit. PABLO A. PALAZZI “Los Delitos Informáticos en el Código Penal. Análisis de la ley 26.388”, 2016, pág 13.

Existen cada vez más variadas y complejas conductas disvaliosas que podríamos encuadrar en distintas figuras penales, por ejemplo, la difusión no autorizada de imágenes íntimas no está penada actualmente en el Código Penal. Sólo existe el art 71 bis del Código Contravencional de la Ciudad de Buenos Aires, con una pena muy baja, ya que, al ser una pena contravencional, es menor que un delito.

Por lo que es cierto afirmar que, frente a estos nuevos escenarios, la población en general, y también muchos letrados y magistrados, no tienen conocimiento de cómo encuadrarlos y proceder frente a estos nuevos tipos de violencia digital.

También él hostigamiento y el acoso en redes, es muy frecuente. Y a esto se suman otras nuevas modalidades como el "Doxing" que es la publicación de información personal en internet (teléfonos, domicilio), con el fin de vulnerar la privacidad de la persona. También el robo de identidad digital, con la creación de perfiles falsos, apócrifos de una persona.

Muchos de los problemas o dudas que plantea la reforma, requieren comprender el contexto tecnológico en el cual se desarrolla la hipótesis fáctica. Por ello va a ser necesario que los jueces, fiscales y abogados que intervendrán en estos casos conozcan y entiendan el funcionamiento de la tecnología, que se los capacite intensamente en estas temáticas, porque muchas veces la solución pasará por comprender cómo funciona un sistema de correo electrónico, una intranet o un portal, o cómo se accede internamente a un sitio de internet, por citar algunos ejemplos.

III. El sistema jurídico penal está incompleto: La necesidad de tipificar.

Desde hace más de dos décadas se viene discutiendo en distintos niveles académicos, legislativos y hasta judiciales la necesidad de una actualización del Código Penal. Ninguno de los numerosos proyectos presentados tanto por legisladores como por el Ministerio de Justicia habían tenido tratamiento legislativo.

Si analizamos la cuestión de fondo, en el derecho penal, por el principio de "intervención mínima" sólo son legítimas las penas necesarias: el arraigo demuestra, precisamente, que no hay discrepancias a la hora de proponer una reducción de los mecanismos punitivos del Estado al "mínimo necesario". Podríamos decir que la tipificación penal de las conductas indeseadas que plantean las nuevas tecnologías sólo parecerá legitimada, en la medida en que contribuya a aportar una reducción de la violencia social informal imposible de lograr mediante otros instrumentos del sistema jurídico, como los que pueden propiciar el derecho civil y el derecho administrativo. (4)[5]

A la hora de determinar la eventual idoneidad de los tipos penales vigentes para acoger la delincuencia informática. Debemos tener en cuenta que no sólo la existencia de hipótesis fácticas de imposible subsunción en las figuras penales existentes justifica la construcción de nuevas figuras delictivas, también la constatación de que la posible subsunción de un supuesto fáctico novedoso en un tipo penal existente obtiene del sistema normativo una respuesta impropia.

Esta respuesta impropia de los tipos penales sería una pena cuya naturaleza no corresponda al contenido del injusto del hecho atrapado en el tipo penal. Es necesario entonces que la respuesta punitiva sea acorde con el contenido del injusto de estas nuevas realidades.

Actualmente existe en la ciudad de Buenos Aires la UFECI, "Unidad Fiscal Especializada en Ciberdelincuencia" proveniente del Ministerio Público Fiscal, quienes, en estos casos, tratan de encuadrar según sea el caso, calificaciones como:

1. Acceso ilegítimo a un sistema informático, si las imágenes fueron extraídas del dispositivo de la víctima (tras robo o por uso compartido de teléfonos o computadoras)

2. Daño informático, si para acceder a las imágenes se alteraron o borraron datos del dispositivo (se usó algún software para acceder ilegítimamente o se modificó la contraseña de acceso a una cuenta desde la que se extrajeron luego las imágenes)

[5] art. cit. 2011, Gustavo A. Arocena." La regulación de los delitos informáticos en el Código Penal argentino. Introducción a la Ley Nacional núm. 26.388"

3. Comunicación o publicación de una comunicación electrónica para el caso de que las imágenes hayan sido compartidas por la víctima por este medio y el receptor, luego las haya re-transmitido sin autorización.

4. Inserción ilegítima de datos, cuando se trata de la publicación de esas imágenes en webs que pueden ser consideradas archivos o bases de datos.

Estas calificaciones, permiten ingresar al sistema penal un puñado de casos, pero no llegan a dimensionar adecuadamente el fenómeno, ni desde la descripción de la conducta, ni desde su sanción." afirma el Fiscal de la Unidad Especializada de Ciberdelincuencia, Horacio Azzolin.

Un rasgo saliente de la infracción informática es su extraterritorialidad y su intemporalidad. La caída de las fronteras, por las características de la delincuencia moderna, que es transnacional y el fenómeno de lo global, surgido del uso de Internet por un operador situado en cualquier lugar, valiéndose de una computadora, un teléfono, un módem y un proveedor del servicio, hacen los ejemplos tradicionales de "casos difíciles" sobre la determinación de la ley aplicable en el espacio, y nos colocan ante una fantástica serie de situaciones de colisión de derechos penales nacionales frente a un mismo supuesto de hecho. Incluso, podría también resultar insuficiente si no se trabaja de modo simultáneo en una construcción supranacional relativamente homogénea del sistema del derecho penal, de los conceptos y categorías de la teoría jurídica del delito, y de los principios y garantías político-criminales fundamentales. (4)

Hay que entender lo complejo del ecosistema digital, no sólo para resguardar nuestra privacidad sino también para exigir leyes que puedan protegernos y la capacitación específica de los Poderes del estado de estas nuevas conductas, que se regulen procedimientos y fiscalías especializadas, comisarías instruidas en cómo investigar y proceder ante estos casos. La tipificación en el Código Penal sería lo ideal para darle alcance federal y la entidad que merecen estas conductas. Necesitamos que esta reforma sea delimitada, con perspectiva de género y contemple además los posibles agravantes y las distintas variantes que pueden suponer.

III.II. **¿Qué es la pornovenganza? ¿Es delito?**

Este es un término jurídicamente incorrecto, ya que ni el porno, ni la venganza, son delitos. Quizás podrían ser considerados una infracción moral o social, pero no por ello, un delito.

Difundir imágenes sexuales sin consentimiento, no es "porno", y si el fin es la venganza, tampoco debería sernos relevante, además que la motivación del ofensor, no siempre consiste en "venganza". Este es un término injurioso para la víctima.

Es cierto que este no es un delito en sí, sino una clase de conducta. Aunque muchas de estas conductas pueden abordarse en otros delitos, como analizamos anteriormente.

Pero no hay hoy en día tipificado un delito específico que abarque estrictamente esta clase de conducta. Claramente que comprenderlo en distintas figuras, no puede alcanzar, ni ser suficiente. No dimensiona que hay muchas otras conductas quedan fuera de este procedimiento, por no poder ser calificado con estos otros delitos, ya que ese no es el fin con el que se creó esta norma.

Encuadrarlo en otros delitos es un procedimiento necesario para no dejar impune a estos delincuentes, pero lo mejor para nuestra seguridad jurídica y para nuestro ordenamiento, teniendo en cuenta además la masividad de denuncias y casos que se presentan en la actualidad, es la tipificación propia, con la conducta clara, el tipo objetivo, subjetivo, bien jurídico protegido, agravantes. Es decir, reconocerlo, como un problema y darle la entidad que necesita, por las consecuencias tan dañinas que produce o puede producir. Para no dejar desprotegida a nuestra sociedad, con una marcada política criminal y directrices claras, aunque, así y todo, no bastaría únicamente con esto.

Debemos lograr la eficiencia y eficacia en la investigación de las causas penales mediante la utilización de medios modernos de obtención de pruebas basados en tecnología informática y de las telecomunicaciones, garantizando que su utilización se rija por normas respetuosas de los derechos fundamentales de los ciudadanos. Y la capacitación necesaria de quienes conforman tanto la investigación, como el proceso jurídico.

Con esta corriente nace en el 2012 la resolución 501 del Ministerio Público de la Ciudad Autónoma de Buenos Aires, creando una fiscalía especializada en delitos informáticos. Se trata de la primera unidad especializada a nivel judicial creada en la Argentina.

En el año 2015 la Procuración General de la Nación creó la Unidad Fiscal especializada en Ciberdelincuencia (res. PGN 3743/2015) a cargo del Dr. Horacio J. Azzolin.

La resolución 69/2016 (BO 18/03/2016) del Ministerio de Justicia crea el Programa Nacional contra la Criminalidad Informática en la órbita de dicho Ministerio.

Este ambicioso plan de actividades del programa incluye, entre otros, los siguientes aspectos:

— Reformas que resulten necesarias en la legislación penal y procesal penal.

— Proyectos normativos de cooperación judicial entre la nación y las provincias a fin de mejorar la

eficiencia en la persecución de los delitos informáticos como en todo lo atinente a la cooperación interjurisdiccional en la obtención de evidencia digital.

— Capacitación de los operadores del sistema penal tanto federal como provincial sobre la materia.

— Coordinación de acciones con organismos nacionales e internacionales.

— Promover la cooperación entre sector público — sector privado para el mejoramiento de las investigaciones que involucren la necesidad de obtener evidencia digital en la que sea necesaria la colaboración de los proveedores de servicios de internet u otros entes con acceso a datos informáticos que puedan resultar de interés para las investigaciones.

— Propiciar la participación de Argentina en los foros internacionales y en las Convenciones y mecanismos internacionales de Cooperación sobre la materia que resulten convenientes para nuestro país.

La mencionada norma es un paso importante que demuestra el interés del Estado en combatir el delito informático y en actualizar las normas procesales penales en la materia.

Además, contamos con una guía recientemente aprobada sobre prueba informática. Con fecha 31 de marzo de 2016 la Procuración General de la Nación emitió la resolución 756/2016 mediante la cual se aprueba la guía para la obtención, preservación y tratamiento de evidencia digital, fruto de la discusión de estos temas a nivel Mercosur.

Se trata de un protocolo que, si bien no es vinculante, aborda detalladamente el modo en el cual se debe obtener, conservar y tratarla evidencia digital para mejorar los niveles de eficiencia en materia de persecución penal. La guía no pretende abarcar todos los procedimientos a tener en cuenta, sino que busca sistematizar y brindar recomendaciones utilizadas a nivel mundial para incautar, analizar y preservar evidencia digital que debe ser considerada por los operadores judiciales.

Se debe señalar que la evidencia digital está cada vez más presente, no sólo en casos de delitos informáticos sino también en casos de delitos no informáticos. Por eso no ha de ser un hecho relevante la aprobación de la primera guía en el país, para que los miembros del Ministerio Público Fiscal pueden usar para sus investigaciones que son cada más frecuentes. (5)[6]

IV. Legislación comparada:

En los últimos tiempos se desarrollaron normativas a nivel internacional y regional tales como el Convenio del Ciberdelito de Budapest, elaborado por el Consejo de Europa, su protocolo adicional contra la Xenofobia en internet, el Protocolo relativo a la venta de niños, la prostitución infantil y la utilización de los niños en la pornografía, que complementa la Convención de las Naciones Unidas sobre los Derechos del Niño; la Decisión Marco 2005/222/JAI del Consejo de la Unión Europea de 24/02/2005 sobre acceso ilegítimo a sistemas informáticos y las guías

[6] art. cit. 2016, PABLO A. PALAZZI "Los Delitos Informáticos en el Código Penal. Análisis de la ley 26.388", 2016, pág 6

internacionales de cooperación entre fuerzas de seguridad e ISP elaboradas en el marco del Consejo de Europa.

La gran cantidad de normativa en el derecho comparado que ha actualizado los códigos penales para legislar toda clase de infracciones informáticas, y las recientes reformas especiales a normas procesales. Estos cambios legislativos obedecen a la necesidad de lograr que las herramientas legales de investigación de delitos cometidos a través de internet sean eficientes. No sólo la mayoría de los códigos penales modernos del mundo han contemplado alguna forma de criminalidad relacionada con la informática, sino que hasta existe una convención internacional sobre la materia y varias normas de nivel regional de la cual son parte más de cuarenta países desarrollados, y que se encuentra en vías de ser implementada en varios de los países que la aprobaron.

Es que el delito informático ya no puede seguir siendo ignorado por el legislador: su realidad y su presencia son incontrolables y los efectos devastadores que puede causar resultan enormes. Basta citar los millones de dólares en daños y pérdidas que ocasionan los virus informáticos, o las estafas por esa vía o, para citar un fenómeno más común, el ataque mediante denegación de servicios que lleva incluso a práctica sextorsivas de ofrecimiento de servicios de seguridad a empresas en internet.

El acto de hackear se ha vuelto algo tan común que cualquiera puede realizarlo fácilmente, justamente este es uno de los motivos que vuelve tan peligrosas estas conductas y así la masividad con exponencial crecimiento como el que tenemos actualmente.

En materia de acuerdos internacionales, son notorias las recientes tendencias en las Naciones Unidas sobre esta temática, y el interés de este organismo internacional en crear un nuevo estándar en tratados sobre ciberdelincuencia que reemplace al Convenio de Budapest. (6)[7]

La República Argentina ha adherido en 2010 al Convenio sobre Cibercriminalidad de Budapest (de noviembre de 2001), que incluye una disposición general que establece: "Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para instaurar los poderes y procedimientos previstos en la presente sección a los efectos de investigación o de procedimientos penales específicos" (artículo 14.1) y reglas específicas que indican que las partes sancionarán

[7] art. cit. PABLO A. PALAZZI "Los Delitos Informáticos en el Código Penal. Análisis de la ley 26.388", 2016, pág 8

tales medidas para la conservación inmediata de datos informáticos almacenados (artículo 16), la conservación y divulgación inmediata de los datos de tráfico (artículo 17), el registro y decomiso de datos informáticos almacenados (artículo 19), la recogida en tiempo real de datos de tráfico (artículo 20) y la interceptación de datos relativos al contenido (artículo 21).

Ahora bien, sería correcto decir que existen dos opciones a la hora de pergeñar esta normativa particular. Por un lado, puede sancionarse una ley específica, complementaria del Código Penal. Es la opción por la que se han inclinado, por ejemplo, Venezuela —que sancionó su Ley Especial contra los Delitos Informáticos el 30 de octubre de 2001—, Chile —que hizo lo propio mediante ley núm. 19.223, del 28 de mayo de 1993) y Alemania —que el 15 de mayo de 1986 adoptó la Segunda Ley contra la Criminalidad Económica, que se ocupa casi excluyentemente de la ciberdelincuencia, pero atrapa igualmente algunas figuras ajenas a ella, como, por caso, la utilización abusiva de cheques—.

Por el otro, puede preferirse una reforma del Código Penal, ya agregando un nuevo título que contemple las nuevas ilicitudes no tipificadas, o ubicando éstas en los distintos títulos del digesto, conforme los diversos bienes jurídicos que pretendan tutelarse. Entre otros países, ha legislado sobre los delitos informáticos en su Código Penal, mediante la creación de un capítulo específicamente dedicados a ellos, Bolivia: en su libro segundo, el título XII —destinado a los delitos contra la propiedad— incorpora el capítulo XI, que tipifica los delitos informáticos. En cambio, ha preferido regular los ciberdelitos en su Código Penal, esparciendo las diversas figuras en distintos pasajes de su articulado, Paraguay, España y Francia, por ejemplo.

En nuestro país, en el desarrollo histórico de la legislación penal más reciente, encontramos ejemplos de cada una de estas dos grandes alternativas, aunque la normativa vigente decide incluir la cibercriminalidad en su Código Penal en forma desconcentrada, esto es, incluyendo los distintos tipos legales en los diversos títulos del libro segundo del digesto, conforme los variados objetos jurídicos que se desea tutelar.(1)[8]

El anteproyecto que inspiró al proyecto de Código Penal fue elaborado por una comisión designada en conjunto por los Ministerios de Justicia y Relaciones Exteriores en el año 2005. La Procuración General de la

[8] art. cit. 2011, Gustavo A. Arocena." La regulación de los delitos informáticos en el Código Penal argentino. Introducción a la Ley Nacional núm. 26.388"

Nació designó también un representante. La Secretaría de Política Criminal del Ministerio de Justicia elevó este anteproyecto a la Comisión de Reforma Integral del Código Penal para su consideración. Por ende, dicho proyecto no tuvo vida propia. Si bien el anteproyecto no tuvo, por ello, estado parlamentario, constituyó la expresión oficial de dos ministerios sobre la necesidad de penalizar las conductas relacionadas con la informática. El anteproyecto no tenía exposición de motivos. Pero este adoptaba la postura de modificar los tipos penales existentes en el Código Penal y no la de aprobar una ley especial en la materia.

En mayo del año 2006 se presentó en consulta pública el Anteproyecto de Ley de Reforma y Actualización integral del Código Penal. El Ministerio de Justicia y Derechos Humanos de la Nación creó la "Comisión para la Elaboración del Anteproyecto de Ley de Reforma y Actualización Integral del Código Penal". Este anteproyecto de reforma contempló numerosos cambios en materia de tecnología.

*IV.*II. La ciudad de Buenos Aires en su Código Contravencional:

CAPÍTULO V

IDENTIDAD DIGITAL DE LAS PERSONAS

"Artículo 71 bis - Difusión no autorizada de imágenes o grabaciones íntimas. Quien difunda, publique, distribuya, facilite, ceda y/o entregue a terceros imágenes, grabaciones y/o filmaciones de carácter íntimo sin el consentimiento de la persona y a través de cualquier tipo de comunicación electrónica, de transmisión de datos, páginas web y/o a través de cualquier otro medio de comunicación, siempre que el hecho no constituya delito, es sancionado con una multa de cuatrocientas (400) a mil novecientas cincuenta (1950) unidades fijas o cinco (5) a quince (15) días de trabajo de utilidad pública o con tres (3) a diez (10) días de arresto. El consentimiento de la víctima para la difusión, siendo menor de 18 años, no será considerado válido.

Tampoco podrá alegarse el consentimiento de la víctima en la generación del contenido como defensa a la realización de la presente conducta.

Acción dependiente de instancia privada con excepción de los casos donde la víctima sea menor de 18 años de edad.

No configura contravención el ejercicio del derecho a la libertad de expresión."

"**Artículo 71 ter. - Hostigamiento digital.** Quien intimide u hostigue a otro mediante el uso de cualquier medio digital, siempre que el hecho no constituya delito, es sancionado con multa de ciento sesenta (160) a ochocientas (800) unidades fijas, tres (3) a diez (10) días de trabajo de utilidad pública, o uno (1) a cinco (5) días de arresto.

Acción será dependiente de instancia privada con excepción de los casos donde la víctima fuese menor de 18 años de edad.

No configura hostigamiento digital el ejercicio del derecho a la libertad de expresión."

Artículo 71 quarter. Agravantes: En las conductas descriptas en los artículos 71 bis y 71 ter, las sanciones se elevan al doble cuando son realizadas:

1. Cuando la víctima fuera menor de 18 años, mayor de 70 años, o con discapacidad.

2. Cuando la contravención se cometa con el concurso de dos (2) o más personas.

3. Cuando la contravención sea cometida por el/la jefe, promotor u organizador de un evento o su representante artístico.

4. Cuando la contravención sea cometida por el/la cónyuge, ex cónyuge, o a la persona con quien mantiene o ha mantenido una relación de pareja, mediare o no convivencia.

5. Cuando la contravención sea cometida por un familiar en el 4to. grado de consanguinidad o 2do. grado de afinidad.

6. Cuando la contravención se cometa con información que no habría sido develada sin que medie el engaño.

7. Cuando la contravención sea cometida mediante la utilización de identidades falsas o anónimas o mediando la suplantación de la identidad de otra persona humana o jurídica."

"**Artículo 71 quinquies. Suplantación digital de la Identidad:** Quien utiliza la imagen y/o datos filiatorios de una persona o crea una identidad falsa con la imagen y/o datos filiatorios de una persona mediante la utilización de cualquier tipo de comunicación electrónica, transmisión de datos, página web y/o cualquier otro medio y se haya realizado sin mediar consentimiento de la víctima, siempre que el hecho no constituya delito, es sancionado con una multa de Ciento sesenta (160) a cuatrocientas (400) unidades fijas o uno (1) a cinco (5) días de trabajo de utilidad pública o de uno (1) a cinco (5) días de arresto.

Las sanciones se elevan al doble cuando:

a. La conducta sea realizada con la finalidad de realizar un banco de datos con la información obtenida.

b. La víctima fuera menor de dieciocho (18) años, mayor de 70 años, o con discapacidad.

c. La contravención sea cometida por el/la cónyuge, ex cónyuge, o a la persona con quien mantiene o ha mantenido una relación de pareja, mediare o no convivencia.

d. La contravención sea cometida por un familiar de hasta el cuarto grado de consanguinidad o segundo grado de afinidad.

e. La contravención sea cometida con el objeto de realizar una oferta de servicios sexuales a través de cualquier medio de comunicación.

El consentimiento de la víctima, siendo menor de 18 años, no será considerado válido.

Acción dependiente de instancia privada con excepción de los casos donde la víctima fuere menor de 18 años de edad.

No configura suplantación de identidad el ejercicio del derecho a la libertad de expresión

Una de las problemáticas asociadas a la protección de datos que más denuncias recibió el Centro de Ciberseguridad del GCBA es la de la suplantación de identidad. En el último año, este tipo de delito aumentó un 50%. Y de acuerdo al Centro de Ciberseguridad de GCBA, en 2020, sólo en CABA, se detectaron 190 denuncias por estos hechos, lo que significa un incremento del 143%.

"La suplantación de identidad está dirigida no sólo a personas físicas, sino también jurídicas, como las empresas. En los casos que se ven habitualmente, el criminal, aprovecha la imagen de una empresa, simulando ser el perfil verdadero con el objetivo de engañar y así obtener datos importantes o el robo de sus tarjetas", indica Luciano Monchiero, titular de la cátedra de Ciberdelitos y director del posgrado de Especialización en Cibercrimen de Universidad Siglo 21.

Una táctica que se vuelve cada vez más habitual es el secuestro de los perfiles de "influencers" en Instagram –una estafa que creció un 500%- para acceder a las cuentas de usuarios legítimos. Usualmente para recuperar la cuenta y los seguidores los atracadores piden un rescate en bitcoins. También la creación de perfiles falsos con datos reales robados a cuentas de "influencers", con el supuesto fin de realizar sorteos y regalos, utilizándolo como gancho perfecto para robar información y datos de tarjetas de crédito de seguidores reales de estos, que caen en la trampa y se genera así la estafa.

Pero entonces, si esta conducta se realiza o tiene efectos en la Ciudad de Buenos Aires, podría ser investigado y calificado por estos artículos del Código Contravencional, donde se hace un buen análisis y una tipificación especifica sobre la descripción de la conducta, el bien jurídico protegido, y sus respectivos agravantes. Aun así, no es un delito, sino una simple contravención y tiene una escala penal muy baja.

Se debe valorar, que por lo menos allí corren con un poco más de suerte, al ser pioneros en al menos tener redactadas y tipificadas estas conductas, con una modalidad, que, aunque no parece suficiente, puede perseguir estas conductas disvaliosas y por lo menos la ciudadanía en algún modo se puede sentir más protegida de su identidad y derechos digitales.

En algunas provincias de Argentina, en cambio, no contamos ni siquiera con este medio de protección. Si se comete esta conducta, no hay ninguna norma específica, ni siquiera contravencional, que describa específicamente la conducta, y entonces ocurre lo que habíamos analizado en los párrafos anteriores, en algunos casos se puede llegar a encontrar la forma de encuadrarlo en otro delito, dándole en todo caso igualmente una respuesta impropia, y en otros casos, dejándolo sin ningún respaldo, como figura atípica, ya que no encuadra con ninguno de los delitos que tenemos tipificados. Dejando completamente desprotegidas a estas víctimas, sin poder darle ninguna solución, revictimizandolas con un Derecho Penal, que no está preparado para protegerlas, dejando impune a estos ciberdelincuentes que por lo tanto no hacen más que aumentar su actividad delictiva.

V. Violencia de Género Digital:

La violencia de género es la misma que existe desde tiempos muy lejanos, el tema ahora es que lo digital es el soporte para realizarla. Lo distintivo sería a través de qué medios se manifiesta. "Puede ser desde una violencia psicológica, como insultos o maltratos a través de medios electrónicos. O puede ser el acoso y hostigamiento, como también la difusión de imágenes sin autorización. Todo eso configura el contexto de la violencia digital", afirma Silvina Lico, abogada y parte del Programa de Atención de Niñez y Adolescencia y Género de la Defensoría del Pueblo de la Ciudad de Buenos Aires.

"Violencia digital: La que afecta la dignidad digital de las mujeres al lesionar alguno o varios de sus bienes y/o derechos digitales como la reputación, la libertad, la existencia, el domicilio, la privacidad y la inclusión digitales, o afecta cualquier otro aspecto de su acceso y desenvolvimiento en el ámbito virtual, el uso de las tecnologías de la información y la comunicación, la seguridad informática de sus equipos y dispositivos y la indemnidad de su identidad digital.".

"Violencia telemática: aquella ejercida con la asistencia o a través del uso de las Tecnologías de la Información y la Comunicación (TIC), como por ejemplo los teléfonos celulares, la Internet, las plataformas de redes sociales o el correo electrónico.".

La Fundación Activismo Feminista Digital se ha expresado firmemente en toda oportunidad, sobre la necesidad de un Estado nacional que atienda mediante políticas públicas acordes y expeditas, a la problemática de la violencia de género digital y telemática. Uno de sus informes recientes, refleja las primeras estadísticas que se han hecho en el país dando lugar a la visibilización del impacto que supone este flagelo en la vida de las mujeres argentinas. El informe 2018 se encuentra ya en ejecución por parte de la Fundación y anticipa un cuadro más preocupante que el del año pasado, lo que ratifica la exigencia al Estado Argentino de aggiornar el marco normativo de Protección Integral hacia las Mujeres, comprendiendo necesariamente el desenvolvimiento digital de éstas como parte del ámbito de tutela planteado en la Ley.

La dignidad digital y la libertad digital son la base para el reconocimiento del plexo de derechos digitales. Ambos conforman la columna vertebral del cúmulo de derechos a proteger mediante la determinación legal de la "violencia digital".

La reputación digital está estrechamente ligada con la identidad digital ya que es la percepción por terceros en el plano virtual, o sea de la expresión asumida por la internauta para su desenvolvimiento en Internet; en otras palabras, es la consideración pública de la individua que por tal no deviene ni accesoria ni prescindible para comprender al ser en su conjunto. Por ello mismo cualquier afectación a la identidad digital conlleva una vulneración directa a la reputación digital y viceversa, entendiendo como agravante de cualquier forma de violencia digital hacia las mujeres, su carácter de "acumulativa en el tiempo".

No puede negarse la importancia de estos derechos en la dignidad digital de las mujeres; la proyección que cada una realiza de su identidad debe poder ser voluntariamente elegida, dando a conocer sólo aquello que cada una considere pertinente. Los contenidos de la esfera privada de ninguna forma deben ser considerados como información pública sin resultar ello altamente dañoso.

Según una encuesta, el 47% de las personas se han sentido acosadas en alguna red o medio digital. De ellas, el 56% fueron mujeres.

La compañía BTR Consulting realizó una encuesta que descubre el crecimiento de casos de ciberacoso y otros delitos a través de las plataformas online. "Se trata de la agresión psicológica que realiza una persona a través de las nuevas tecnologías como el correo electrónico, sistemas de mensajería como WhatsApp y las redes sociales, de forma sostenida y repetidas en el tiempo con la única finalidad de discriminación, dominación e intromisión sin consentimiento en la privacidad de la víctima", señala el informe titulado "Violencia de Género Digital. El efecto sutil, profundo y anónimo de la tecnología", que además determina que "puede darse por medio del acoso, amenaza, extorsión, suplantación de identidad espionaje y ataque".

Según ese estudio, realizado sobre una muestra de 3.000 personas entre hombres y mujeres, el 47% de las personas encuestadas se han sentido acosadas por un tercero en alguna red social o medio digital. De ese total, el 56% son mujeres mientras que el 44% son hombres. El mismo informe también reveló que cerca del 60% de las mujeres y niñas que usan las redes Facebook, Instagram, Twitter y Tik tok han sufrido abusos.

Asimismo, el 85% de los encuestados que sufrieron el abuso online de su pareja o ex pareja afirmaron que también lo experimentaron de manera real y casi un tercio de los encuestados (el 29%) fue víctima de algún software espía o localizadores GPS en su teléfono o computadora por parte de un socio o tercero.

Otra cifra escalofriante: el 50% de los encuestados que experimentaron abuso online también recibieron amenazas directas para ellos o para alguien que conocían.

"si bien la agresión online puede dirigirse contra cualquier persona, las investigaciones muestran que las experiencias de las mujeres online son cualitativa y cuantitativamente diferentes". Lo aseguran porque según las Naciones Unidas "las mujeres, a nivel mundial, tienen 27 veces más probabilidades de ser atacadas en internet que los hombres y el abuso digital que enfrentan también es específico por su naturaleza".

Y se refieren tanto al acoso online como a la mal denominada "pornovenganza". "Los casos de violencia sexual digital contra mujeres se han disparado y una de las principales causas es la amplia disponibilidad de tecnología". Informe de la consultora manifiesta que todas las conductas de violencia de género que se ejercen mediante las redes sociales e internet pueden englobarse bajo el término violencia de género digital y que las diferentes formas de ejercer el ciberacoso limitan la libertad, sobre todo de la mujer, ya que generan relaciones desiguales y provocan una dominación del acosador sobre la víctima mediante estrategias humillantes que dañan su imagen pública y afectan su privacidad.

"La violencia de género digital está afectando especialmente a grupos tan vulnerables como los adolescentes y los síntomas en las víctimas online son similares a los causados por el abuso sexual y doméstico tales como la depresión, la ansiedad y pérdida de la autoestima". En este contexto, para visibilizar y asistir a las víctimas de violencia de género digital, es necesario que la víctima tenga a quién acudir ante un caso de ciberacoso, donde se sienta protegida y entiendan por lo que está pasando.

El gobierno de la Ciudad de Buenos Aires informó que los casos de violencia de género digital en época de pandemia se triplicaron.

Muchas actividades se trasladaron al ámbito digital. Videollamadas, reuniones virtuales, clases en línea y home office. Mariana Marques directora de Política y Justicia Internacional en Amnistía Internacional Argentina afirma que las redes sociales e internet, en general, son una extensión del debate público y que de la misma manera en la que las mujeres sufren violencia de género en las calles o en sus

casas, la sufren en las redes sociales: "No es un tipo de violencia nueva, sino una forma diferente en la que esa violencia se manifiesta".

Y como se viene repitiendo a través del tiempo, y sea cual sea el medio, la culpa de todo es siempre de la víctima que, por cierto, casi siempre es mujer. Ella es culpable de sacarse las fotos, sin pudor, de enviarlas sin pensar en las consecuencias y también de haber hecho o dicho algo que generó, que se difundan las fotos o vídeos.

VI. Reflexión Final:

En primer instancia como ciudadanos, debemos reconocer y darle la entidad que merecen en la actualidad nuestros derechos digitales y nuestra identidad digital, ya que finalmente aun cuando somos usuarios tecnológicos, seguimos siendo personas, humanos y sujetos de derechos. Que, si somos claros, y logramos delimitar nuestros derechos y obligaciones, desarrollando mecanismos e instituciones que funcionen para defenderlos y garantizarlos en caso de perjuicios o daños, quizás entonces sería posible discutir acerca de una ciudadanía cibernética más segura y justa.

Pero regular los ciberdelitos sin pensarlo con un enfoque internacional no es posible. Las redes cibernéticas atraviesan todo el mundo y no tienen en cuenta las fronteras territoriales. Es por ello que resultaba necesario armonizar las legislaciones en materia de delitos informáticos y establecer procedimientos de cooperación para combatirlos. Esta fue la génesis de la Convención del Ciberdelito y de otros proyectos que están actualmente en discusión en foros internacionales.

Y con todo este desarrollo quisiera aclarar, que es de suma importancia, pero no basta ni es suficiente la simple tipificación de estos delitos, debemos tener una política criminal seria para la persecución, el juzgamiento y el eventual castigo del delito informático, no puede ser suficiente la tipificación por más perfecta y clara que sea de las distintas hipótesis o conductas de ciberdelito que deben ser previstas por el legislador penal. Ya que también es imprescindible para que esto funcione, que se creen los mecanismos y procedimientos adecuados para poder acreditar y subsumir estas conductas socialmente disvaliosas en las nuevas figuras delictivas que se tipificaron.

Es que, debemos tener en cuenta las características principales de estos delitos informáticos, como son su extraterritorialidad, su intemporalidad e intangibilidad

para que se construyan métodos de investigación eficientes y eficaces a la hora de perseguirlos.

Si no queremos crear puro derecho penal simbólico, es decir leyes que se promulgan, pero que no se reglamentan, ni se aplican. Debemos corroborar que en el procedimiento se encuentren métodos de constatación probatoria idóneos, como así también la capacitación del personal, los materiales y técnicos suficientes para poder perseguir eficazmente estas conductas.

Otro punto muy importante y necesario, para el correcto funcionamiento y aplicación, es la colaboración internacional y de organismos privados, que necesariamente deben aportar su ayuda, brindando la información necesaria cuando es requerida, y promoviendo una política de ciberseguridad apropiada y estricta.

En materia de violencia de género digital está claro que no podemos seguir revictimizando a las víctimas, que de por sí, ya sufren este contexto social, donde casi siempre las hacen culpables, en vez de culpabilizar al verdadero autor de estas conductas y daños. Debemos encontrar la forma de protegerlas. A través de leyes, que reconozcan sus derechos, como su ciber-identidad, y su derecho a la libertad de auto determinarse cibernéticamente, de poder mostrarse como lo prefiera, sin sufrir abusos, coacciones, o suplantaciones de identidad. Y que, si esto sucede, que existan organismos preparados para recibirlas, apoyarlas y acompañarlas en este proceso, que se pueda investigar eficazmente y someter a un justo proceso penal. Y quizás así logremos, frenar el avance exponencial de estos delincuentes.

Ahora bien, si la Ciudad de Buenos Aires logró realizar esta incorporación de figuras para poder de alguna manera, aunque aún no logremos la incorporación o reforma de nuestro Código Penal, perseguir estas conductas. Me pregunto, por qué no podríamos adaptarlo a las distintas Provincias y jurisdicciones en caso de que se siga dilatando de esta manera la reforma del Código Penal, lo que como ya dijimos sería lo ideal y necesario.

Pero la realidad, es que, por las consecuencias dañosas, las estadísticas formuladas en las investigaciones que ya analizamos, y el exponencial crecimiento de estos delitos, es claro que necesitamos una solución con prisa, ya que existen cada vez más ciberdelincuentes, y más víctimas que se sienten desprotegidas y con razón, de nuestro ordenamiento jurídico aún no está preparado.

Debemos avanzar, y lograr adaptarnos a esta nueva "era digital" en la que vivimos, dejando clara nuestra política criminal, que conductas son socialmente disvaliosas,

como podemos proteger a las víctimas, los procedimientos de incorporación de prueba y evidencia, como perseguir estos delitos e investigarlos. Sino seguiremos atrasados a nivel Internacional, y las consecuencias gravísimas que acarrea el dejar desprotegida de esta manera a la población frente a esta serie de conductas que no hacen más que aumentar.

Bibliografía:

art. cit. 2011, Gustavo A. Arocena." La regulación de los delitos informáticos en el Código Penal argentino. Introducción a la Ley Nacional núm. 26.388"

http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332012000300002

Marcelo Alfredo Riquert, "Algo más sobre la legislación contra la delincuencia informática en Mercosur a propósito de la modificación al código penal argentino por ley 26388"

http://www.ciidpe.com.ar/area2/DELINCUENCIA%20INFORMATICA.RIQUERT.pdf

art. cit. 2016, PABLO A. PALAZZI "Los Delitos Informáticos en el Código Penal. Análisis de la ley 26.388"

https://filadd.com/doc/los-delitos-informaticos-en-el-codigo-penal-pdf

2020, Giuliana Biasotto, Agencia de noticias. Ciencias de la comunicación UBA. "Se triplicaron los casos de violencia de género digital"

http://anccom.sociales.uba.ar/2020/10/21/se-triplicaron-los-casos-de-violencia-de-genero-digital/

2020, Fernando Jara, "Violencia de género digital: cómo detectarla y combatirla"

https://www.infobae.com/sociedad/2020/12/03/violencia-de-genero-digital-como-detectarla-y-combatirla/

2018, MODIFICACIÓN DE LA LEY 26.485 VIOLENCIA DIGITAL.

https://dequesetrata.com.ar/proyecto/camara-de-diputados/5968-D-2018-21575

2018, Código Contravencional de la Ciudad de Buenos Aires (texto consolidad Ley 6017.) http://www2.cedom.gob.ar/es/legislacion/normas/leyes/ley6128.html

2019, Mariano Borinsky, "La porno venganza en el nuevo Código Penal." https://www.infobae.com/opinion/2019/03/08/la-porno-venganza-en-el-nuevo-codigo-penal/

2021, "La suplantación de identidad creció un 50 por ciento en Argentina: así operan los ciberdelincuentes."

https://www.clarin.com/tecnologia/suplantacion-identidad-crecio-50-ciento-argentina-operan-ciberdelincuentes_0_WRq_pT7l4.html