EDITORIAL ASTREA

*Las redes del delito**

La sociedad de la información y sus crímenes

Por Roberto M. Ambrosis

1. Introducción

Es de público y notorio conocimiento que los avances de la tecnología y de la comunicación social a través de las redes sociales, no escapan de ninguna manera a los fenómenos de la delincuencia y del delito.

Considero oportuno trazar una somera aproximación de los delitos informáticos, como aquellas acciones típicas, antijurídicas y culpables cometidas a través de los medios relacionados con la informática, y en particular por medio de las denominadas "redes sociales", que no son más que las conocidas masivamente, como Facebook, Twitter, Instagram, YouTube, entre otros.

Estos desarrollos informáticos o medios modernos de comunicación generan verdaderas sociedades cibernéticas de las que hoy en día acabamos formando parte. Las redes sociales pueden ser utilizadas para publicar las fotos vacacionales, mostrarse en forma seductora al sexo opuesto, como perfil profesional a modo de currículum, con la finalidad de exhibirse públicamente o hasta para asechar a un niño con el motivo de satisfacer los más bajos instintos sexuales.

Sin dudas, las llamadas "redes sociales", impactan en la sociedad de la información, funcionan como un escaparate exhibicionista para mostrarle al mundo algo personal. Estas verdaderas "vidrieras infinitas", se muestran como una perfecta y sencilla estructura capaz de comunicar entre sí a personas o instituciones en cuestión de segundos. A través de Internet se pueden establecer relaciones que creen grupos o asociaciones casuales, con intereses comunes o sociales, tanto lícitos como ilícitos.

Ello supone un contacto ilimitado y a tiempo real. Esto se consigue gracias a la interactividad, uno de sus rasgos más distintivos y novedosos del Internet.

Asimismo, las redes permiten establecer un contacto mutuo entre emisor y receptor. Ahora mismo un artículo colgado en un periódico digital no se considera terminado hasta que los receptores han añadido sus reflexiones al original, por lo que algunos autores que estudian el fenómeno de la comunicación y de la economía hablan de los llamados "prosumidores"[1], que implica, ni más ni menos que la aparición

---

* Ernesto E. Domenech (supervisor). Mariano Refi (colaborador). Bibliografía recomendada.

[1] Toffler Alvin acuñó el término "prosumidor" cuando hizo predicciones sobre los roles de los productores y los consumidores, aunque ya se había referido al tema desde 1970 en su libro *Future Shock*. Toffler preveía un mercado altamente saturado de producción en masa de productos estandarizados para satisfacer las demandas básicas de los consumidores, en el cual, para mantener

de nuevas herramientas complejas pero que a su vez son de fácil uso o de tecnologías amigables (cámaras de video, cortadoras de pasto, etc.) que han incentivado el traspaso de actividades antes realizadas por terceros de forma remunerada, hacia la actividad prosumidora y el trabajo llevado a cabo por uno mismo; esto supone una actividad voluntaria que requiere compromiso, esfuerzo y tiempo.

a. La sociedad de la información

La aparición de Internet ha dado un nuevo énfasis a la sociedad, potenciando el trabajo del consumidor y productor al mismo tiempo; a través de redes de colaboración, que agregan valor de manera colectiva, incentivando la innovación y compartiendo conocimientos que aceleran los ciclos económicos y tecnológicos. Su aparición se liga con los cambios en las formas de producción de tipo fordista a las postfordistas, que producen cada vez más en base a las demandas específicas de los usuarios y ellos participan sugiriendo usos, tendencias y formas de diseño de las redes sociales que generan cambios sustanciales en nuestro entramado social.

Redes como Facebook o Twitter ofrecen servicios que garantizan un contacto instantáneo, por ejemplo, si una niña sube a una red social fotografías sobre lo que hizo un día por la tarde, al segundo toda su lista de amigos, que posiblemente esa niña no conozca en su totalidad puede tener acceso a ellas, y así ella casi sin darse cuenta ignora que está ingresando a una zona de riesgos infinitos.

Esto sucede porque Internet y las redes sociales se están convirtiendo en un pasatiempo para los niños y adultos, los cuales a través de éstas comparten las actividades llevadas a cabo tanto en espacios de ocio como de otros planos de la vida.

Así se puede encontrar a personas utilizando dichas redes mientras ven la televisión, mientras caminan por la calle, mientras conducen un automóvil e incluso cuando se comparten momentos en persona, por ello es necesario entender que el contacto cibernético amenaza las relaciones sociales tradicionales, tal cual las concebimos.

Ahora bien, el fenómeno descripto desde el inicio de este trabajo traza un paralelo que denota que, en la actualidad, el fenómeno de la globalización como manifestación, ha tenido un avance significativo, el cual no solo ha dado beneficios, sino también ha contribuido a la masificación de esta clase de delitos y tecnificado a otra clase, los denominados “delitos informáticos”.

Las redes sociales son servicios prestados a través de Internet que permiten a los usuarios generar un perfil público, en el que se plasman información y datos personales, disponiendo de herramientas que permiten interactuar con el resto de usuarios afines o no al perfil público.

---

el crecimiento de las ganancias, las empresas podrían iniciar un proceso de “*mass customization*” (personalización en masa), refiriéndose a la producción a gran escala de productos personalizados, y describiendo la evolución de los consumidores, involucrados en el diseño y manufactura de los productos. Además, Toffler argumentó que cada individuo tendría el control de los bienes y servicios que sean de su consumo, una vez que la era industrial termine.

Estas interacciones no son más que relaciones interpersonales que se gestan a través de la web y son amplificadas por ella a los amigos de los amigos, los conocidos, los compañeros de trabajo, etcétera; son personas que suelen estar relacionadas en formatos estáticos: agendas de papel, memorias de teléfonos móviles básicos y otros directorios similares.

Las redes sociales posibilitan llevar estas listas de conocidos a la web, donde cada nombre deja de ser una cadena de letras, sin más posibilidades, y pasa a ser un enlace que permite acceder a una página nueva, donde va a aparecer toda clase de información sobre el individuo, en toda clase de formatos multimedia: fotografías, audio, vídeo, enlaces a sus webs favoritas, y hasta existen aplicaciones que permiten grabar en vivo fragmentos de la vida de las personas.

Este fenómeno se visualiza de manera más práctica, fundamentalmente por dos grandes razones:

- El primer fundamento reside en que se ha generalizado y naturalizado el uso de medios e instrumentos informáticos por medio de la sociedad y hoy en día aceptamos cada vez más en nuestra vida cotidiana este medio de comunicación, que suple y limita en muchos casos a la comunicación real. En esta nueva forma de comunicarnos se combina el ocio, el esparcimiento, el arte, el consumo, la ansiedad, la búsqueda de conocimientos con las pulsiones sexuales, satisfacer los más bajos instintos que, según el caso, terminan facilitando oportunidades en las cuales determinadas personas logran sacar ventaja, con la finalidad de despojar a los incautos de sus bienes o irrumpir en la vida privada de estos causándole un daño.

- En el segundo fundamento, es donde se produce una paradoja muy grande, por un lado nuestra moral social nos conduce a cuidar nuestra intimidad como un valor de nuestra dignidad, aunque por el otro lado consumimos con habitual voracidad información de la vida privada de las personas famosas o mediáticamente expuestas, con una voracidad inusitada.

- Considero que el tercer fundamento está dado en que la razón de que la sociedad en su conjunto, se asume como productora y consumidora, ya se encuentra alertada en su mayoría de la verdadera jauría de lobos disfrazados con piel de cordero, piel que ya no es real, si no es que un artilugio; pese a ello nos sentimos encantados y fascinados por la comunicación virtual, que nos permite comunicarnos a grandes distancias viéndonos la caras, aunque encierre grandes peligros para nuestros más preciados bienes.

La investigación de los delitos informáticos se asemeja a una moneda de dos caras. Uno de sus lados, parece indicar que la mayoría de los actores sociales tienen la sensación de que las actividades criminales realizadas por medios informáticos garantizan una mayor forma de impunidad de los acechadores o de los delincuentes que utilizan estos medios y se camuflan en sus redes para cometer delitos de forma elegante y además este modo, parece ser la mejor forma de engañar a las víctimas y los investigadores, si es que se tiene un básico conocimiento de la informática.

El otro lado de esta moneda, implica para quien utiliza las redes y los elementos informáticos para cometer delitos, el dejar marcas y señales que permiten seguir al delincuente, como sucedía en un conocido cuento infantil en el cual dos niños, “Hanzel y Gretel” dejaban pedazos de pan para recordar el camino y no perderse, para luego, al emprender la vuelta recolectar esos trozos de pan o marcas que va dejando la comisión del delito, siendo esta la tarea que realizarán los investigadores para poder descubrir y castigar a los autores de los ilícitos que dejan los restos de pan como en el cuento infantil, quienes utilizan ordenadores que tienen establecidos números de IP, que es un acrónimo que significa (Internet Protocol) y consiste en una serie de números que se le asigna a cada ordenador conectado a Internet, estas generalmente se corresponden con los números de dominio de Internet, pudiendo cambiar en tanto los nombres de dominio no varían por que el servidor DNS los hace concordar con las direcciones IP y poder identificar una computadora conectada a una red que corre este protocolo, pudiendo verificar con alto grado de certeza, de que computadora se realizó alguna maniobra delictiva con una sencilla operación.

Lo mismo ocurre con los equipos de telefonía celular que poseen el llamado IMEI; una sigla que proviene del inglés “International Mobile Equipment Identity”, lo que traducido al español significa “Identidad Internacional de Equipo Móvil”, y su propósito es proporcionarle al teléfono celular una identidad única en todo el mundo.

Asimismo, algunos autores determinaron que estos tipos de delitos virtuales se asimilan a los delitos de guante blanco, porque no dejaban rastro de su realización, aunque hoy con una investigación adecuada, rastreando la huella digital impresa en un delito cometido hace posible descubrir su autoría, dejando de lado que las redes sociales dan una cierta impunidad para cometer delitos.

Finalmente esta manifestación social también alcanza y atraviesa a la familia y a las cuestiones vinculadas a la comunicación de niños y adolescentes donde existen diferencias entre el manejo y la familiaridad del uso de las nuevas tecnologías y las redes sociales, entre ellos y sus padres, que generalmente no emplean las redes sociales o las emplean con otra destreza distinta a la que los niños y adolescentes manejan; es allí donde se da una situación de real asimetría entre grandes y chicos, dentro de la familia .

Dicho esto, para arrojar mayor claridad a lo expuesto corresponde incorporar y tratar el concepto de la llamada “brecha digital”, según “Wikipedia Enciclopedia libre on-line”[2]. “Se entiende por brecha digital la distancia en el acceso, uso y apropiación de las tecnologías tanto a nivel geográfico, a nivel socioeconómico (entre quintiles de ingreso) y también en las dimensiones de género, en articulación con otras desigualdades culturales, etcétera. Cabe destacar que la brecha digital está en relación con la calidad de la infraestructura tecnológica, los dispositivos y conexiones, el desconocimiento del uso de la herramienta, pero sobre todo, con el capital cultural para transformar la información circulante en conocimiento relevante”.

Está claro que las condiciones generacionales, tienen que ver con el acceso y uso a las tecnologías de información. Ello puede tener tres planos para analizar. El

[2] https://es.wikipedia.org/wiki/Brecha_digital.

primero tiene que ver con la infraestructura tecnológica y redes disponibles. El segundo plano tiene que ver con la accesibilidad a los servicios que ofrece la tecnología. Y el tercer plano, que considero el más importante, en la relación de padres e hijos, es la de poseer habilidades y conocimientos prácticos para hacer un uso adecuado de las redes y sus novedades.

Esto hace, que al mismo tiempo las redes sociales, sean un caldo de cultivo para eludir los controles parentales de cómo y con quién se comunican estos niños y adolescentes, que también buscan cierta independencia de sus progenitores.

En este caso la sociedad de la información, impacta de lleno en la familia y la hace vulnerable a los ataques externos, traspasando el control que se puede llevar a cabo, con problemas vinculados a la comunicación de padres e hijos niños y adolescentes, nuestras familias y el futuro de nuestros hijos se va con ello.

b. ¿Qué es el "el ojo absoluto"?

En estos tiempos de lo virtual, según Wacjman, se erige en torno a la comunicación humana el llamado de muro de las pantallas, "el muro de imágenes se está convirtiendo en el objeto del siglo"[3].

A este fenómeno según el autor no se lo puede cuantificar en cantidad y dimensión, es por ello que se habla de un verdadero muro que opera como una trasmutación hipodérmica del mismo, por el que el espesor opaco del muro se transforma como por arte de magia en una ventana transparente que dota al ojo humano de una visión de 360 grados, de lo que podríamos hablar, siguiendo a este autor, de un verdadero ojo universal, al respecto manifiesta "El muro encarna la *full visión*, la ambición del discurso de la ciencia de ver todo. Afirma la voluntad de la omnipotencia de la mirada. El muro de imágenes no tiene más rival que la mirada de Dios… El mundo no es una aldea global, porque ahora un mercado único, también esta globalizado por la mirada que lo abraza".

Según este nuevo orden se impone un nuevo régimen de la mirada, donde a su vez se suprimen todos los muros, marcos y límites de todas las ventanas, lo que supone para este pensador que el espacio "hipermoderno", es el de un sujeto sin lugar, sin domicilio y sin interior, lo que debe hacernos pensar sobre una nueva idea de privacidad o esfera de lo privado que sin dudas también supone un serio replanteo de nuestras normas jurídicas, sociales y estructuras familiares que deberán adecuarse a este nuevo fenómeno, que supone una visión sin límites y medir o cuantificar que es lo que entraña esa ausencia de reglas, lo que en la modernidad puede resumirse como daños colaterales y lo genera el goce de nuestra sociedad de mirar y ser mirado.

Esta nueva transparencia supone que el espacio de lo visible se ha extendido, se ha vuelto global, supone que se disolvieron los límites y las fronteras, al sujeto y al mundo se los acerca considerablemente, lo íntimo y lo interior, como una ideología de querer verlo todo, al respecto dice Wajcman "en la oscuridad de la habitación cerrada,

[3] Wacjman, Gerard, *El ojo absoluto*, Bs. As., Manantial, 2011.

el muro de imágenes de mil pantallas sería, en resumen, el interior del cráneo del mundo, el cerebro de nuestro mundo onmnivideníe".

Es interesante como este autor también define la zona de la delincuencia y como la sociedad misma pasó a ser una colonia de alta seguridad, en la que todos estamos inmersos, diferenciándose con la cárcel en que de ella se pude salir. En nuestra opinión el enemigo sigue estando entre nosotros, solo que es más difícil identificarlo, por qué es íntimo, porque todos y cada uno de nosotros como parte de la sociedad y de nosotros mismos al mismo tiempo estamos conectados, no solo cuidándonos de las acciones de terceros sino también controlando nuestra actividad.

Es decir, entonces, que muchas veces tenemos que defendernos de nosotros mismos y de nuestros hábitos, como por ejemplo exhibir nuestra vida en la redes y es allí donde nace una gran paradoja, por una lado esta nueva modernidad nos hace vulnerables, y por otro en nuestro interior donde yacen y crecen los nuevos delincuentes, los asociales y los criminales, sobre todo si se piensa en estos muros de pantallas sin límites, están nuestros niños observando estos cambios con avidez y curiosidad, sobre todo disfrutando y escapando con astucia de los límites impuestos por los roles parentales.

En estos tiempos es común observar que los niños y adolescentes, migran de redes sociales habituales como Facebook o Twitter y eligen otras que son de poco entendimiento, comprensión y control de sus padres como los son Snapchat, Instragram o Phhhoto, que tienen una lógica de códigos comunes y facilitan eludir los controles de los padres.

Por ejemplo, la aplicación Snapchat permite subir fotos que se borran automáticamente en 24 horas, fotos enviadas en privado con mensajes que se borran al ser vistas. O en el caso de red social Kiwi que se inicia el contacto con el otro con una pregunta personal que se puede hacer. Snapchat, a diferencia de otras redes, se basa en la fugacidad de los mensajes que cada usuario cuelga. No hace falta perseguir la belleza ni ser divinos como en Instagram, sino que se puede decir lo que se quiera, sea en texto, foto, vídeo o gráfico, que desaparecerá como máximo a las 24 horas de efectuar la publicación. Pero la red alienta el intercambio constante de mensajes, que duran entre 1 y 10 segundos, para no perder el "estar en racha", es decir, activo en la red social y no perder puntos, que la red asigna según el nivel de actividad.

Snapchat se basa en el uso del móvil y sobre todo de la cámara frontal, la que se usa para el "selfie". A la foto propia se le puede añadir filtros como cambiar la cara con otra persona, encuadres, máscaras, gráficos, hasta se puede dibujar encima. Todo vale, pero para fotos de paisaje ya está Instagram.

Una foto o un video se pueden ver durante un máximo de 10 segundos, aunque se puede pedir una repetición gratuita pero solo una vez al día. Si quieres más, las pagas. Se puede capturar la imagen con la opción de captura de pantalla del móvil, pero entonces llega icono a quien lo envió avisándole de que lo has hecho. También se pueden hacer chats de video, grabar mensajes de voz o realizar llamadas de voz, pero esto es casi una anécdota para una generación que ya no usa el teléfono para llamar.

Otro punto diferencial es que se pueden comentar los “snaps” dentro del propio “snap” y no en un espacio aparte como ocurre en Facebook. Hay un sistema de pagos dentro de la aplicación para poder transferir fondos, pagar por contenido de la aplicación (repeticiones, por ejemplo) o cualquier cosa que en el futuro a los propietarios se les ocurra, dando cuenta que las nuevas generaciones de niños son las generaciones del consumo sin límites.

Una página aparte merece las aplicaciones para buscar parejas. Una de las más populares es Tinder, aplicación a través de la cual con una serie de fotos se puede lograr clikeando un corazón, en rango determinado de distancia, establecer un contacto con alguien que puede volcar en su presentación información que puede ser verdadera o falsa, con finalidades delictivas, como puede ser cualquiera de las figuras contempladas por el art. 119.

En el caso de la aplicación Hapnn, esta sin dudas promete ayudar a encontrar a las personas con las que te has cruzado, que te gustaron y que te encantaría volver a encontrar. Para lograrlo se vale de la geolocalización y, en tiempo real, te notifica y envía el perfil de usuarios cercanos de este programa. Indica el número de veces que se han cruzado y para volver a encontrarlo sólo basta con presionar la cruz. Además los usuarios pueden presionar el corazón si alguna persona con la que te cruzaste te gusta y, sólo en caso de que la otra persona también indique que le gustas, le avisará a ambas. Se puede descargar, gratis, desde el App Store, Play Store o Windows Store.

Esta aplicación puede lograr en buenas manos encontrar una pareja a nuestra medida y en las manos equivocadas puede ser un instrumento de mucha utilidad para un ciber asechador o un pedófilo, ya que indica a modo de un halcón en las viejas épocas, la distancia de la presa, si nos ha cruzado o está cerca nuestro.

Además, las aplicaciones Tinder y Hapnn, se convierten en verdaderos catálogos humanos, que deshumanizan las relaciones humanas y las vuelven notablemente materialistas y consumistas, basándose ellas solo en la imagen. Tomar la postura de conocer una persona de la misma forma que se elige un viaje, o se compra un auto o indumentaria, sin dudas cosifica de alguna forma a las relaciones humanas.

Es entonces interesante analizar un escenario como lo plantea Pavón como una era del deseo transparente, adonde el goce de la exhibición trasciende las pantallas y como esta tendencia social, modifica las pautas sociales como el erotismo y la forma de conocer personas.

El interrogante aquí, también es filosófico en cuanto a que la intimidad de nuestros cuerpos no es tal, es un espectáculo que está allí y habla sin ser preguntado y también nos viene a decir que las reglas del erotismo deben ser rescritas, las de la comunicación reiniciadas y nuestras reglas sociales y jurídicas repensadas.

Por ejemplo, es posible pensar según Pavón que “desde su nombre el Facebook, es una galería de semblantes. La imagen cuerpo, digitalizado, la voz, la palabra escrita funcionan como un anzuelo para atrapar el deseo del otro. Los intercambios virtuales crean las condiciones para el encuentro (o bien precipitan la caída de la escena: una frase desafortunada puede ser letal). El supuesto exhibicionismo del mundo virtual es más bien una construcción donde cada ser hablante da forma a un relato sobre la propia persona y tal construcción encuentra en las nuevas tecnologías un escenario…

los semblantes construidos en las redes sociales buscan en ocasiones consistencia a la posición sexuada de los partenaires: las cincuenta y cuatro opciones que ofrece Facebook a la hora de definir el género del usuario hablan por sí solas… En la era de los deseos expuestos, las preguntas por el goce, no logran una respuesta satisfactoria, pero el cuerpo –afortunadamente– habla"[4].

Para entender este fenómeno es fundamental tener en cuenta las palabras del fundador de Facebook Mark Zukerberg en cuanto a que dijo "hay que romper los lazos entre lo secreto y lo íntimo, porque eso es una herencia obsoleta del pasado" o lo dicho por Eric Schmidt gerente comercial de Google "la preocupación por preservar la vida privada ya no era de todos modos una realidad más que para los criminales".

Ahora bien, se puede decir, que estos nuevos gurús de las tecnologías pregonan el avenimiento de la era de la transparencia, pero obviamente, este mensaje no es ni más ni menos que un mensaje para favorecer sus prósperos negocios, pero al mismo tiempo se puede colegir en estos discursos paradigmáticos primero un mensaje encubierto perverso y en segundo lugar otro muy equivocado e ingenuo.

El mensaje perverso radica en que se publicita con alegría la pérdida de un atributo de la persona humana como lo es la intimidad y la vida privada, atributo de la personalidad este que se encuentra reconocido por los ordenamientos jurídicos locales e internacionales, y es consagrado como un verdadero derecho humano, el cual no podemos dejar de tener o perder por los avances de las nuevas tecnologías.

También de esta pretendida transparencia social surge un mensaje equivocado e ingenuo, de la idea de pensar que la vida privada es una preocupación solo para los delincuentes, si no que se puede pensar todo lo contrario y se puede decir que los delincuentes se hallan muy a gusto en la era de la transparencia. Para ellos Internet se convierte en un campo plagado de oportunidades para quebrantar la propiedad la sexualidad y la intimidad de las personas.

Por más bondadosa que puede ser el uso de las tecnologías las sociedades modernas que se presumen como tales, no pueden fundarse en la idea de que Internet, se ha convertido desgraciadamente para los pedófilos en una mina de oro, ya que estas conductas desviadas perjudican la sexualidad de los niños (que en el pasado fundaron sus lazos entre ellos funcionando como redes clandestinas de intercambio de material como las fotografías o los videos); hoy en día esta perversa actividad usa la intimidad vulnerada de niños y adolescentes para ganar cifras millonarias con la exhibición, distribución y difusión de imágenes pornográficas obtenidas mediante las redes sociales, ello nos hace pensar que este mensaje que anuncia una nueva idea de transparencia, es ingenuo y equivocado y nos debe poner alerta como sociedad ante las nuevas redes del delito.

Para filósofos sociales como Byung-Chul Han "la sociedad de la transparencia valora la exposición". Cada sujeto "es su propio objeto de publicidad. Todo se mide en su valor de exposición. La sociedad expuesta es una sociedad pornográfica". "Vivimos en un mundo que tiende a la hipervisibilidad, un espacio sin secretos ni misterios ocultos. A la sociedad de la transparencia toda distancia le parece una negatividad

[4] Pavón, Héctor, *La era del deseo transparente*, "Revista Ñ", Clarín, 9/6/16.

que hay que eliminar: constituye un obstáculo para la aceleración de los ciclos de la comunicación y del capital"[5].

Es entonces necesario pensar que es hora de adecuar nuestros ordenamientos legales, para responder a estos flagelos, haciendo necesario adecuar los códigos penales y procesales para responder adecuadamente a estos fenómenos, ya que por ejemplo nuestro Código Penal dentro de los delitos que protegen la intimidad de las personas; tendría que incorporar a modo de sugerencia una figura penal que contemple la conducta de la porno-venganza, de la que nos ocuparemos más delante en este trabajo, cuando nos aboquemos a conductas socialmente disvaliosas no tipificadas.#

2. ¿Una definición de delitos informáticos?

Desde hace algunos años los llamados "delitos informáticos" adquirieron una nueva dimensión en el ámbito del derecho, fundamentalmente a partir de la incorporación masiva de computadoras y dispositivos electrónicos en la vida cotidiana de las personas y el valor que adquirió la información como bien jurídico a proteger.

Si bien en la actualidad no existe una única definición sobre el cibercrimen –como también se conoce a este tipo de ilícitos– el significado más generalizado es aquel que describe a este tipo de delitos como aquellas conductas indebidas e ilegales donde interviene un dispositivo informático como medio para cometer un ilícito o como fin u objeto del delito mismo.

En ambos casos se le asigna una importancia condicionante al lugar que ocupa la tecnología en el hecho más que a la naturaleza delictiva del acto mismo. Pero fue con la expansión global de Internet a mediados de la década de 1990 donde la preocupación de los Estados por este tipo de conductas se incrementó ante la cantidad de delitos en línea relacionados con computadoras.

Si bien no todos los delitos se relacionan con la red, es a partir de la popularización de Internet que adquiere una nueva dimensión. Así, los mismos poseen ciertas características propias desarrolladas por el medio en el que se cometen.

En primera instancia, la mayoría de los delitos informáticos son anónimos, en tanto que la red permite a sus usuarios la creación de identidades ficticias. Asimismo son transnacionales, ya que se puede cometer desde una computadora y afectar a varios dispositivos en distintos puntos del planeta. Por último, Internet acorta las barreras del tiempo y el espacio por la instantaneidad de las comunicaciones, lo que transforma a este tipo de conductas en inmediatos en cuanto a su emisión-comisión.

Pero en términos judiciales, la principal característica de este tipo de delitos es el bajo nivel de denuncia ya sea por el desconocimiento por parte de los usuarios de que están siendo víctimas de un delito informático; como también por la ausencia de legislación que incluya determinado tipo de conductas; la baja resolución judicial de este tipo de casos por la falta de capacitación de los funcionarios, peritos y asesores legales especializados en el tema; el temor de las empresas privadas ante la

[5] Han, Byung-Chul, *Psicopolítica. Ensayo*, Barcelona, Herder, 2014, p. 75.

posibilidad de ver afectada su imagen y reputación al ponerse en evidencia de fallos de seguridad de sus sistemas y redes; entre otras.

Por último, existe en el imaginario social la idea que los delitos informáticos son cometidos únicamente por hackers o profesionales con alto conocimiento en programación y sistemas capaces de vulnerar los sistemas de seguridad de redes de organismos gubernamentales o bancos o de colapsar el funcionamiento de servicios públicos de millones de personas.

En los inicios de Internet, cuando la red no era pública, los usuarios de computadoras eran profesionales con amplios conocimientos en el área de informática que se desempeñaban en laboratorios de investigación en empresas o universidades norteamericanas.

Con el paso del tiempo, el desarrollo de entornos gráficos, mouses, tecnologías "touch" y la popularización de uso a través de Internet, cualquier persona con conocimientos básicos en computación y acceso a la red puede cometer un delito informático.

a. El derecho informático

La delincuencia informática se encuadra dentro de lo que se conoce como "derecho informático". Este es el conjunto de normas jurídicas que regulan la utilización de los bienes y servicios informáticos en la sociedad, incluyendo como objeto de estudio: *1*) el régimen jurídico del software; *2*) el derecho de las redes de transmisión de datos; *3*) los documentos electrónicos; *4*) los contratos electrónicos; *5*) el régimen jurídico de las bases de datos; *6*) el derecho de la privacidad; *7*) los delitos informáticos, y *8*) otras conductas nacidas del uso de los ordenadores y de las redes de transmisión de datos.

En lugar de crear una nueva rama del derecho dedicada exclusivamente al estudio de estos aspectos, podría haberse abordado la regulación o estudio de cuanto concierne al ámbito de digitalización del mundo empresarial, administrativo e incluso personal desde un análisis por cada una de las ramas del ordenamiento jurídico ya existentes, en las que habría que encajar estas nuevas realidades en función del aspecto concreto a analizar. Así, de los contratos electrónicos se ocuparía el derecho civil o mercantil, de las conductas ilícitas vinculadas a las nuevas tecnologías el derecho penal, etcétera.

Sin embargo, la complejidad de las relaciones informáticas, su crecimiento desmesurado o el hecho de que en el estudio de estas nuevas relaciones se transite de una rama del ordenamiento jurídico a la otra constantemente (administrativa, civil, laboral o penal) ha favorecido que por motivos pragmáticos desde algunos sectores se haya reclamado la consideración de una nueva rama del ordenamiento jurídico que regularía las relaciones, cualesquiera, vinculadas con la informática que tendría como característica, precisamente, el hecho de que en la disciplina confluyan normas administrativas, civiles, laborales, penales, etcétera.

b. Delito informático

Desde esta perspectiva, estimo de suma importancia destacar lo que tradicionalmente se ha denominado "delito informático", es decir, los ilícitos cometidos a través de la informática, relativos –entre otros– a la intimidad, la libertad, la indemnidad sexual, etcétera.

En este segundo ámbito es donde Internet es el instrumento que justifica desde una perspectiva político-criminal un tratamiento diferenciado, tanto por el derecho penal material como por el procesal.

1) *Marco conceptual del delito informático*. Una de las primeras dificultades a la hora de afrontar el análisis de los delitos informáticos es su conceptualización. No resulta fácil considerar qué debe entenderse por delito informático y qué conductas pueden considerarse incluidas en él; de hecho, ni siquiera la doctrina encuentra un concepto unitario de delito informático y las discrepancias en torno a éste han llegado incluso a propiciar que algunos autores admitan la imposibilidad de darle una definición y renuncien a ello[6].

La doctrina ha debatido durante años si en estos casos nos encontramos ante una categoría que pueda denominarse "delito informático" o si, por el contrario, se deben utilizar expresiones para definir la misma realidad que carezcan de un matiz jurídico-positivo y que hagan alusión, más bien, a categorías criminológicas: así las expresiones delincuencia informática, criminalidad informática o delitos informáticos, ésta no en cuanto concepto, sino en cuanto realidad de características concretas**.**

Los avances de la tecnología informática y su influencia en casi todas las áreas de la vida social como lo indicamos más arriba, han provocado una serie de comportamientos disvaliosos que antes eran impensables y en algunos casos de difícil tipificación en las normas penales tradicionales, sin recurrir a aplicaciones analógicas prohibidas por el principio de legalidad.

Parte de este problema proviene de la vertiginosa velocidad con la que evolucionan las nuevas tecnologías y el consiguiente constante cambio y desarrollo, también extremadamente rápido, de las conductas delictivas vinculadas a aquéllas**.**

Estos constantes adelantos tecnológicos inciden y alteran sin dudas al alcance de un concepto que la doctrina quiere trazar, pero parece que los adelantos técnicos siempre están un paso por delante de los esfuerzos de la doctrina para definir esta clase de delitos. Es por ello que es de gran dificultad arribar a un concepto único o

---

[6] Por ejemplo, Luis Camacho Llosa consideró que podía definirse como delito informático "toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor aun 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" (*Delitos informáticos*, p. 25).

Autores como Carlos A. Ferreyros Soto propicia prescindir de una conceptuación, y propone enunciar alguna de particularidades que presenta el conjunto de comportamientos a que puede venir referida la expresión delitos informáticos y destaca solo algunas notas salientes que no considera suficientes como para erigir un concepto unívoco de esa expresión (*Aspectos metodológicos del delito informático*, "Informática y Derecho" n° 9, 10 y 11, UNED, Centro Regional de Extremadura, Mérida, 1996, p. 407 y siguientes).

que pueda bastarse a sí mismo, ya que a medida que estas conceptualizaciones van surgiendo la tecnología avanza y va mutando en forma vertiginosa.

No obstante, se han ensayado algunos intentos de conceptualización del delito informático. Así, corresponde indicar que los delitos de informática, son producto de la criminalidad evolutiva, la cual nace concomitantemente con las nuevas tecnologías informáticas y telemáticas y el delito informático es aquel que se comete con el empleo de computadoras o equipos electromagnéticos que transmiten datos o informaciones. En este sentido, los delitos informáticos, según Tiedemann, "aluden a todos los actos, antijurídicos según la ley penal vigente (o socialmente perjudiciales y por eso penalizables en el futuro), realizados con el empleo de un equipo automático de datos"[7].

Otra definición fue la aportada por Parker, que precisó los abusos informáticos como "cualquier incidente asociado con la tecnología de los ordenadores en el que la víctima sufrió o pudo haber sufrido un daño y el autor, intencionadamente, obtuvo o pudo haber obtenido un beneficio"[8]. Este autor no se limitó a describir las conductas relevantes para el ámbito penal sino que reconoce que se trata de un amplio abanico de comportamientos entre los que se incluyen, además de conductas de naturaleza penal, otras de relevancia civil y meros incidentes sin trascendencia jurídica.

Por su parte, Camacho Losa consideró que, no habiendo una definición de delito informático plenamente satisfactoria, debía considerarse delito informático "toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor aun 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"[9].

En uno de los ejemplos, podemos observar que Gómez Perals define a los delitos informáticos, como "el conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos"[10].

En otro sentido, Ruiz Vadillo (1996) recoge la definición que adopta el mercado de la OCDE en la recomendación n° R (81) 12 del Consejo de Europa que indica que el abuso informático "es todo comportamiento ilegal o contrario a la ética o no autorizado que concierne a un tratamiento automático de datos y/o transferencia adecuada y rápida y, por tanto, es necesario llevar a cabo una armonización más

---

[7] Mario Rodrigo Morabito indicó que "podríamos ensayar definiciones de delito informático propuestas por otros autores; no obstante, habré de compartir la definición formulada por Tiedemann, quien previó en la misma ella –a pesar de su generalidad– a todos los hechos ilícitos cometidos a través de un equipo informático". Tiedemann, Klauss, *Poder económico y delito*, Barcelona, 1985.

[8] Parker, D. B., *Crime by computer*, New York, 1976.

[9] Camacho Losa, Luis, *El delito informático*, Madrid, 1987.

[10] Gómez Perals, Miguel, *Los delitos informáticos en el derecho español*, "Informática y Derecho" n° 4, UNED, Centro Regional de Extremadura, III Congreso Iberoamericano de Informática y Derecho 21-25 septiembre 1992, Mérida, Aranzadi, 1994.

intensa de la legislación y de la práctica entre todos los países respecto a la delincuencia relacionada con el computador".

Por su parte, Davára Rodríguez define al delito informático como, "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software"[11].

A su turno con acierto, Téllez Valdés conceptualiza al delito informático en forma típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin"[12].

Como se puede ver no siempre se alude en estas definiciones a acciones típicas, es decir descriptas en figuras delictivas, pues se involucran a acciones inmorales o abusivas, o a acciones no típicas, pero se enfatiza el empleo de medios informáticos en la realización de esas acciones (tipificadas o tipificadas en la legislación). De modo entonces que lo relevante es el medio informático de realización de la acción.

Ahora bien ¿Es indispensable una definición de delito informático como herramienta teórica para el análisis de estos fenómenos de la criminalidad contemporánea, o pueden adoptarse otras estrategias para pensar y analizar estos problemas?

No siempre son claros los propósitos con los cuales se adopta una definición en la teoría jurídica, ya que estas pueden ser utilizadas de diversas maneras. A veces con un propósito informativo, otras como un criterio para resolver un problema de interpretación de la ley, otras para señalar ciertas condiciones de punibilidad. De esta manera introducir una definición de delito informático sin determinar adecuadamente para qué se formula no es útil ni necesario.

En este sentido estimo útil discriminar. Aquellas figuras delictivas en las que el medio informático aparece textualmente referido, como el "grooming" o el "ciber-acoso".

Las que contienen conceptos legalmente definidos que incluyan aspectos informáticos. Tal es el caso de la firma digital, de las palabras documento, firma digital, suscripción, instrumento privado y certificado contenidos en el art. 77 del Cód. Penal.

Y por último se debe tener en muy en cuenta; que otros delitos del Código Penal pueden ser cometidos a través de medios informáticos, o sobre objetos informáticos.

También es posible meritar aquellas acciones no adecuadamente previstas en la legislación penal, por cuestiones de política criminal, pero capaces de provocar daños a las personas o sus bienes.

---

[11] Davára Rodríguez, Miguel Á., *Manual de derecho informático*, Pamplona, Aranzadi, 1997.

[12] Téllez Valdés, Julio, *Los delitos informáticos. Situación en México*, "Informática y Derecho" n° 9, 10 y 11, UNED, Centro Regional de Extremadura, Mérida, 1996, p. 461 a 474.

Los problemas que suscita la informática en el campo jurídico penal, no se agotan de ninguna manera en las discriminaciones que se han realizado. La informática es una herramienta criminalística de gran valor en la investigación criminal, no sólo por los hallazgos que permitan descubrir en forma directa, sino por su uso a través de otras disciplinas criminalísticas que se valgan de ella.

En este sentido la poca visibilidad de muchas acciones dañinas a través de medios informáticos, encuentra en la propia informática una manera de visibilizarla.

2) *Elementos del delito informático*. A pesar de los diversos conceptos que se han propuesto sobre el delito informático y la discusión existente acerca de su naturaleza, lo cierto es que, en todos ellos, encontramos elementos comunes. Veamos:

a) Conducta fraudulenta o engañosa: uso indebido o fraudulento de elementos informáticos a través de la introducción o manipulación de datos falsos.

b) Instrumento: presencia de los componentes físicos y/o lógicos del sistema informático.

c) Finalidad: obtención de un beneficio ilícito, directo o indirecto, no necesariamente patrimonial.

d) Resultado: perjuicio, no necesariamente patrimonial, de tercero o de la colectividad.

Estos habrán de ser los elementos comunes de lo que se denomina “delito informático”, sin perjuicio de que ante nuevas conceptualizaciones, puedan adicionarse otros componentes que resulten de suma utilidad para la práctica forense.

3) *En el derecho internacional. El convenio de ciber-criminalidad como “soft law” interesante en la materia*. En materia de *soft law*, cabe destacar la reciente adhesión a la Convención de Budapest sobre Ciberdelito del Consejo de Europa (ETS n° 185) adoptado en Budapest, Hungría, el 23 de noviembre de 2001, mediante ley 27.441, sancionada en fecha 22 de noviembre de 2017. Este convenio contiene prescripciones que son de sumo interés.

Cabe destacar previo a adentrarnos en el análisis correspondiente del Convenio que su objetivo principal es la cooperación entre los Estado parte. Este se compone de cuatro capítulos y refiere tanto a normativa de fondo como de forma.

El Título III del Convenio trata las infracciones relacionadas con el contenido; más precisamente en el art. 9 “Infracciones relativas a la pornografía infantil”, apartado primero, se ocupa de regular la obligación para los Estados partes de adoptar las medidas legislativas o de otro tipo que estimen necesarias para prever en su derecho interno como infracción penal las conductas que detalla en sus respectivos incisos cuando sean cometidas dolosamente y sin autorización. Estas conductas son: *a*) la producción de pornografía infantil con la intención de difundirla a través de un sistema informático; *b*) el ofrecimiento o la puesta a disposición de pornografía infantil a través de un sistema informático; *c*) la difusión o la transmisión de pornografía infantil a través de un sistema informático; *d*) el hecho de procurarse o de procurar a otro pornografía infantil a través de un sistema informático; *e*) la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.

Por otra parte, en el apartado segundo –siempre del art. 9– el Convenio se ocupa de definir a la pornografía infantil afirmando que esta última comprende cualquier material pornográfico que represente de manera visual: *a*) un menor adoptando un comportamiento sexualmente explícito; *b*) una persona que aparece como un menor adoptando un comportamiento sexualmente explícito; *c*) unas imágenes realistas que representen un menor adoptando un comportamiento sexualmente explícito.

Como se podrá advertir, es necesaria una pronta adhesión al Convenio en razón de que su importancia ha sido destacada por importantes juristas. No obstante, soy de la opinión, que en la práctica forense sus disposiciones pueden ser consultadas como guía para la resolución de un caso en concreto.

Es de destacar que Argentina ha efectuado cuatro reservas a este instrumento internacional que versan sobre diversos puntos, la reserva que encuentro más significativa y la que guarda mayor relación a la materia abordada es la efectuada en razón de los arts. 9.1.d., 9.2.b. y 9.2.c.

Como ya vimos anteriormente, el art. 9 refiere a los delitos relacionados con la pornografía infantil y ciertas definiciones; por ejemplo, la relativa a incorporar en la definición de “pornografía” al material que incluya a adultos simulando ser niños/as (art. 9.2.b), o a aquellas que incluya representaciones “realistas” de un menor adoptando un comportamiento explícito (art. 9.2.c).

Ahora bien, la mayor discusión pasa por la mera tenencia de pornografía infantil en dispositivos informáticos (art. 9.1e), si bien al sancionarse la ley 27.441 se hizo reserva parcial en el presente artículo estableciendo: “*El mismo sólo es aplicable de acuerdo a legislación penal vigente hasta la fecha, cuando la posesión allí referida fuera cometida con inequívocos fines de distribución o comercialización*”; en la actualidad, mediante ley 27.436 de fecha 23 de abril de 2018, se modificó el art. 128 del Código Penal, quedando su redacción de la siguiente manera:

“*Será reprimido con prisión de tres a seis años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.*

Será reprimido con prisión de cuatro meses a un año el que a sabiendas tuviere en su poder representaciones de las descriptas en el párrafo anterior.

Será reprimido con prisión de seis meses a dos años el que tuviere en su poder representaciones de las descriptas en el primer párrafo con fines inequívocos de distribución o comercialización.

Será reprimido con prisión de un mes a tres años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce años.

Todas las escalas penales previstas en este artículo se elevarán en un tercio en su mínimo y en su máximo cuando la víctima fuere menor de trece años”.

Por lo que es de destacar que la legislación interna incriminó con la condición de que la tenencia sea a *sabiendas* de que dicho material tiene una representación de un

menor de dieciocho años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores, más allá de la realización de las acciones de producir, financiar, ofrecer, comerciar, publicar, facilitar, divulgar o distribuir.

Aquí el legislador, dejó atrás la discusión que existía en cuanto incriminar la mera tenencia de material pornográfico, con una pena menor que la de la figura originaria, con la condición de que le tenencia sea con el pleno conocimiento que el material que se posee tiene las condiciones estipuladas en el párrafo que le antecede. Lo que parece razonable y un acierto del legislador.

3. Figuras delictivas en las que el medio informático aparece textualmente referido

En este caso podremos hablar de delitos típicamente informáticos y en nuestro Código encontramos los siguientes casos:

a) Art. 131: "ciber-acoso"

"*Será penado con prisión de seis meses a cuatro años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma*" (artículo incorporado por art. 1° de la ley 26.904, BO, 11/12/13).

b) Art. 153 bis: "acceso no autorizado de datos informáticos"

"*Será reprimido con prisión de quince días a seis meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido*".

"*La pena será de un mes a un año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros*" (artículo incorporado por art. 5° de la ley 26.388, BO, 25/6/08).

c) Art. 173, inc. 16: "estafa informática"

"*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" (inciso incorporado por art. 9° de la ley 26.388, BO, 25/6/08).

d) Art. 183, párr. 2°: "daño informático"

"*En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños*" (párrafo incorporado por art. 10 de la ley 26.388, BO, 25/6/08).

4. Figuras delictivas que contienen conceptos legalmente definidos que incluyen aspectos informáticos

Esta categoría se construye principalmente por la asimilación legal efectuada por el art. 77 del Cód. Penal que transcribiré: "*Para la inteligencia del texto de este Código se tendrán presente las siguientes reglas:… El término 'documento' comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión. Los términos 'firma' y 'suscripción' comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos 'instrumento privado' y 'certificado' comprenden el documento digital firmado digitalmente. El término 'información privilegiada' comprende toda información no disponible para el público cuya divulgación podría tener significativa influencia en el mercado de valores*" (artículo sustituido por art. 1° de la ley 26.733, BO, 28/12/11).

Figuras delictivas que contienen palabras especificadas en el art. 77 del Cód. Penal

Artículo	Delito
Art. 153	Violación de secretos
Art. 155	Publicación indebida de datos
Art. 157	Revelación de secretos
Art. 167 quater	Abigeato agravado
Art. 168	Extorsión
Art. 173	Defraudación
Art. 174	Defraudaciones agravadas
Art. 175	Abuso de confianza
Art. 183	Daño primera parte
Art. 184	Daño agravado
Art. 255	Destrucción y alteración de documentos
Art. 289	Falsificación de marcas, sellos y firmas
Art. 292	Falsificación de documentos
Art. 293	Falsificación de instrumento público
Art. 293 bis	Expedición negligente de certificados
Art. 294	Supresión o destrucción de documentos
Art. 295	Expedición de certificado falso
Art. 296	Uso de documento falso
Art. 297	Falsificación de documentos equiparados a los públicos
Art. 309	Agiotaje
Art. 310	Intermediación financiera sin autorización

5. Otros delitos del Código Penal pueden ser cometidos a través de medios informáticos o sobre objetos informáticos

#Es necesario entender que hoy en día cada vez más bienes jurídicos protegidos por el Código Penal pueden ser atacados por medios informáticos y parece que es importante no encasillarse en viejos preconceptos e imaginar un escenario más amplio que aquel que se tenía en el derecho penal tradicional, por lo que ha modo de ejemplo haré un repaso somero de algunos delitos del Código Penal, imaginando formas de comisión a través de medios informáticos.

Por ejemplo, como hemos mencionado, se puede instigar o determinar a matar a alguien por medio de Facebook, Messenger o email, por lo que es posible atentar contra la vida de una persona a través de un medio informático, poniendo en peligro a la vida como bien jurídico tutelado.

Asimismo, de forma más directa, podría sabotearse o introducir un virus informático en un instrumento médico que se encuentra informatizado, el cual suministra aire a un paciente que se encuentra con asistencia respiratoria y deliberadamente hacer que el instrumento deje de funcionar, provocando así la muerte del sujeto.

Como en este ejemplo se ilustra una sutil forma de terminar con la vida de una persona en la cual los medios informáticos toman un papel principal y excluyente.

Otro ejemplo podría ser el de un mecánico aeronáutico que por negligencia o impericia o incumplimiento de procedimientos, no carga o actualiza los datos de navegación del piloto automático de una avión y por defecto de éste se produce un accidente, lo que puede terminar en homicidio culposo, contemplado en el art. 84 del Cód. Penal, o un estrago culposo, normado en el art. 189 del mismo digesto.

Similar situación sucede en el caso de que una persona, con intenciones de deformar el rostro de otra de forma permanente descalibre un bisturí laser que va a ser utilizado para una cirugía laser introduciéndole datos erróneos para producir la deformación permanente del rostro a un viejo enemigo. Este tipo de conducta podría verse tipificada en el delito de lesiones gravísimas (art. 91, Cód. Penal).

Hasta se podría llegar a incurrir en un abandono de persona, conducta tipificada en el art. 106 del Cód. Penal, en el supuesto en el que a una persona le piden auxilio a través de un medio de mensajería informático, y este, quien recibe y lee el mensaje asume, automáticamente, la obligación de socorrer, pero lejos de ello, responde a quién sufre la situación de peligro que se arreglara o lo resolviera por sus medios, que este no podía.

Capítulo aparte merecen los delitos contra el honor, ubicados en el título II del Código Penal.

Tanto las calumnias, las injurias y la difamación pueden llevarse a cabo por la inserción de estas en alguna red social, como Facebook, Twitter, entre otros. Podríamos decir entonces que estas redes son los medios a través de los cuales podría quedar alguna conducta comprendida en la figura típica recién mencionada.

A medida que el tiempo fue avanzando se hicieron más frecuentes este tipo de acciones delictivas llevadas a cabo a través de redes sociales, y ya no sólo a personas

con una vida pública o con determinada exposición, tales como deportistas, personas del mundo del espectáculo o la política, sino también a cualquier persona que utilice estas redes o medios, naturalizándose este proceder siendo considerado como una conducta no delictual y aceptado como algo habitual en la web.

Hasta hace una década parecía imposible que se pudieran cometer delitos contra la integridad sexual por medios informáticos, pero en la actualidad son usuales las figuras de corrupción simples y agravadas previstas en el art. 125 del Cód. Penal.

Art. 125: "*El que promoviere o facilitare la corrupción de menores de dieciocho años, aunque mediare el consentimiento de la víctima será reprimido con reclusión o prisión de tres a diez años.*

La pena será de seis a quince años de reclusión o prisión cuando la víctima fuera menor de trece años.

Cualquiera que fuese la edad de la víctima, la pena será de reclusión o prisión de diez a quince años, cuando mediare engaño, violencia, amenaza, abuso de autoridad o cualquier otro medio de intimidación o coerción, como también si el autor fuera ascendiente, cónyuge, hermano, tutor o persona conviviente o encargada de su educación o guarda".

También es posible realizar la figura de los arts. 125 bis, 126 y 127, que penan la facilitación y promoción de la constitución que es habitual que se haga por medios informáticos.

Art. 125 bis: "*El que promoviere o facilitare la prostitución de una persona será penado con prisión de cuatro a seis años de prisión, aunque mediare el consentimiento de la víctima*".

Art. 126: "*En el caso del artículo anterior, la pena será de cinco a diez años de prisión, si concurriere alguna de las siguientes circunstancias:*

1. Mediare engaño, fraude, violencia, amenaza o cualquier otro medio de intimidación o coerción, abuso de autoridad o de una situación de vulnerabilidad, o concesión o recepción de pagos o beneficios para obtener el consentimiento de una persona que tenga autoridad sobre la víctima.

2. El autor fuere ascendiente, descendiente, cónyuge, afín en línea recta, colateral o conviviente, tutor, curador, autoridad o ministro de cualquier culto reconocido o no, o encargado de la educación o de la guarda de la víctima.

3. El autor fuere funcionario público o miembro de una fuerza de seguridad, policial o penitenciaria.

Cuando la víctima fuere menor de dieciocho años la pena será de diez a quince años de prisión".

Art. 127: "*Será reprimido con prisión de cuatro a seis años, el que explotare económicamente el ejercicio de la prostitución de una persona, aunque mediare el consentimiento de la víctima.*

La pena será de cinco a diez años de prisión, si concurriere alguna de las siguientes circunstancias:

1. Mediare engaño, fraude, violencia, amenaza o cualquier otro medio de intimidación o coerción, abuso de autoridad o de una situación de vulnerabilidad, o concesión o recepción de pagos o beneficios para obtener el consentimiento de una persona que tenga autoridad sobre la víctima.

2. El autor fuere ascendiente, descendiente, cónyuge, afín en línea recta, colateral o conviviente, tutor, curador, autoridad o ministro de cualquier culto reconocido o no, o encargado de la educación o de la guarda de la víctima.

3. El autor fuere funcionario público o miembro de una fuerza de seguridad, policial o penitenciaria.

Cuando la víctima fuere menor de dieciocho años la pena será de diez a quince años de prisión".

Del mismo modo son propias de ser cometidas por medios informáticos las figuras de los arts. 128 y 129, que tienen que ver con penar a quien produzca, financie, publique, divulgué o distribuya actividades sexuales explícitas de menores de edad o quien tenga en su poder este material para su comercialización.

Art. 128: "*Será reprimido con prisión de seis meses a cuatro años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.*

Será reprimido con prisión de cuatro meses a dos años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización.

Será reprimido con prisión de un mes a tres años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce años".

Art. 129: "*Será reprimido con multa de mil a quince mil pesos el que ejecutare o hiciese ejecutar por otros actos de exhibiciones obscenas expuestas a ser vistas involuntariamente por terceros.*

Si los afectados fueren menores de dieciocho años la pena será de prisión de seis meses a cuatro años. Lo mismo valdrá, con independencia de la voluntad del afectado, cuando se tratare de un menor de trece años".

Asimismo es posible, sabiendo que el estado cuanta con medios informatizados para certificar el estado de las personas, alterarlos o suprimir estos registros por medios informáticos y llevar a cabo las conductas de los arts. 138, 139 y 139 bis.

Art. 138: "*Se aplicará prisión de 1 a 4 años al que, por un acto cualquiera, hiciere incierto, alterare o suprimiere el estado civil de otro*".

Art. 139: "*Se impondrá prisión de 2 a 6 años:*

1. A la mujer que fingiere preñez o parto para dar a su supuesto hijo derechos que no le correspondan.

2. Al que, por un acto cualquiera, hiciere incierto, alterare o suprimiere la identidad de un menor de 10 años, y el que lo retuviere u ocultare".

Art. 139 bis: "*Será reprimido con reclusión o prisión de 3 a 10 años, el que facilitare, promoviere o de cualquier modo intermediare en la perpetración de los delitos comprendidos en este Capítulo, haya mediado o no precio o promesa remuneratoria o ejercido amenaza o abuso de autoridad.*

Incurrirán en las penas establecidas en el párrafo anterior y sufrirán, además, inhabilitación especial por doble tiempo que el de la condena, el funcionario público o profesional de la salud que cometa alguna de las conductas previstas en este Capítulo".

Del mismo modo, por ejemplo, es posible realizar la conducta típica de la privación ilegal de la libertad, en el caso de un funcionario del Servicio Penitenciario que recibe, a través de una notificación electrónica al mail una orden de libertad sobre una persona que se encuentra detenida a su disposición, por medio del sistema de firma digital, orden enviada por otro funcionario de la órbita judicial, y pese a recibir el mail y leerlo no hace que se disponga la misma (art. 143, inc. 1, Cód. Penal).

Art. 141: "*Será reprimido con prisión o reclusión de seis meses a tres años; el que ilegalmente privare a otro de su libertad personal*".

Asimismo, se puede realizar la figura prevista en el art. 148 del Cód. Penal, por ejemplo, cuando una persona le escribe un mensaje de Facebook a un menor de diez años para que se fugue del hogar.

Art. 148: "*Será reprimido con prisión de un mes a un año, el que indujere a un mayor de diez años y menor de quince, a fugar de casa de sus padres, guardadores o encargados de su persona*".

Es notorio el cambio que han tenido los medios informáticos en la reforma efectuada en el capítulo III del título V: Delitos contra la Libertad, que se tituló "Violación de secretos y de la privacidad", en la cual la ley 26.388, introdujo cambios notorios en las figuras del art. 153 e incorporó las nuevas figuras de los arts. 153 bis y 157 bis, que los erigen también típicos delitos informáticos por sí mismos.

Art. 153: "*Será reprimido con prisión de quince días a seis meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.*

En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.

La pena será de prisión de un mes a un año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.

Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena".

Art. 153 bis: "*Será reprimido con prisión de quince días a seis meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.*

La pena será de un mes a un año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros".

Art. 157 bis: "*Será reprimido con la pena de prisión de un mes a dos años el que:*

1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.

3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años".

La propiedad, como bien jurídico protegido también puede ser atacado por medios informáticos, como puede pasar en la figura del art. 168, la extorsión, siendo que alguna de las acciones típicas puede ser llevada a cabo a través de un mensaje de texto, por mensaje de Facebook o bien un mail.

Art. 168: "*Será reprimido con reclusión o prisión de cinco a diez años, el que con intimidación o simulando autoridad pública o falsa orden de la misma, obligue a otro a entregar, enviar, depositar o poner a su disposición o a la de un tercero, cosas, dinero o documentos que produzcan efectos jurídicos.*

Incurrirá en la misma pena el que por los mismos medios o con violencia, obligue a otro a suscribir o destruir documentos de obligación o de crédito".

Pueden ser cometidos por medios informáticos algunas de las modalidades de estafa previstas en el art. 172, ello adquiere mayor certeza con las nuevas figuras incorporadas por los incs. 15 y 16 del art. 173, sobre todo el último inciso que se refiere a la defraudación mediante cualquier técnica de manipulación informática, que altere el normal funcionamiento de un sistema informático o de transmisión de datos.

Art. 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*".

Art. 173: "*Sin perjuicio de la disposición general del artículo precedente, se considerarán casos especiales de defraudación y sufrirán la pena que él establece:…*

15. El que defraudare mediante el uso de una tarjeta de compra, crédito o débito, cuando la misma hubiere sido falsificada, adulterada, hurtada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos, aunque lo hiciere por medio de una operación automática.

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".

Incluso pueden los medios informáticos facilitar el delito previsto en el art. 174 inc. 5, en el cual los funcionarios públicos pueden defraudar a la Administración pública por medios informáticos, como lo es por ejemplo en los casos que los funcionarios públicos tengan un procedimiento informático para modificar o borrar la deuda fiscal que se tiene en el sistema y la usen sin ajustarse a los procedimientos, modificando montos o haciendo desaparecer la deuda fiscal del sistema para su propio provecho perjudicando al erario público.

Art. 174: "*Sufrirá prisión de dos a seis años:*

…5. El que cometiere fraude en perjuicio de alguna Administración pública".

Los delitos previstos contra la seguridad del tránsito y los medios de transporte y comunicación pueden ser cometidos a través de medios informáticos.

Como ya hemos mencionado, muchos de los dispositivos del transporte, ya sea aéreo, terrestre o marítimo, son controlados a través de sistemas informáticos, entablando comunicaciones a través de estos medios y trazando trayectos o rutas de viaje, piénsese como ejemplo que alguien alterase un sistema de estos, cambiando rutas aéreas hackeando el sistema operativo de una base de mando de un aeropuerto, o incluso algo mucho más simple, ingresando en el sistema que controla las luces de los semáforos y modificarla de forma intencional, para generar un estrago conforme lo previsto por el art. 190 y siguientes.

Los medios informáticos resultan idóneos a su vez para cometer los delitos previstos contra el orden público, ya que Internet, y los incontables medios de comunicación que este facilita, resultan un medio propicio para llevar a cabo la conducta típica de instigación a cometer delitos, conforme lo contempla el art. 209 del Cód. Penal.

La intimidación pública es un delito que puede ser cometido por medios informáticos, impartiendo temor a la población desde una red social, cumpliendo con los medios comisivos que la figura prevé, siendo que el medio informático resulta idóneo como medio masivo para infundir temor público, suscitar tumultos o desordenes, hiciere señales o voces de alarma, etcétera.

Finalmente y modo de ejemplo también es posible cometer los delitos de falsificación, previstos en los arts. 292 a 296, por medios informáticos, ya que la definición de documento en conformidad a lo normado por el art. 77 del Cód. Penal, alcanza a "*toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión*" al igual que deja comprendidos "*los términos 'firma' y 'suscripción' comprenden la firma digital, la creación de una firma digital o firmar digitalmente*". Asimismo, el citado artículo va a establecer que los términos instrumento público y certificado digital comprenden el documento digital firmado digitalmente, definiciones estas que permiten ser aplicadas en las falsedades de documentos digitales, situaciones que se dan de manera muy frecuente en la actualidad, ampliando los medios comisivos y así el universo de delitos que pueden ser cometidos por medios informáticos, algo que de plantearlo veinte años atrás sonaría descabellado.

Si bien el art. 77 del Cód. Penal, en su última parte menciona "*Los términos 'instrumento privado' y 'certificado' comprenden el documento digital firmado digitalmente*" (párrafo incorporado por art. 1° de la ley 26.388, BO, 25/6/08) y aunque solo hace referencia a documentos privados, no es posible pensar que se ha excluido como bien jurídico digno de protección a los documentos públicos, ya que una interpretación armónica del Código Penal, no parece que quisiera dejar impune un hecho de falsificación de un documento público firmado digitalmente, sobre todos si se toma la idea primera del artículo la asimilación establecida en la palabra "documento", como posible de comprender toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión, sea documento o instrumento público.

6. El "grooming" o el "ciber-acoso"

Los delitos contra menores se ven facilitados en todos sus aspectos por Internet, cuya creciente utilización en los últimos años ha conducido a un enorme aumento de tal actividad delictiva. Los delincuentes no solo pueden distribuir y consultar con mayor facilidad material relacionado con el abuso sexual de menores, sino que también pueden establecer un contacto directo con niños, a través de salas de chat y sitios web de redes sociales.

También, cada vez más, se cometen delitos de contenido sexual, por personas adultas que, amparándose en el anonimato o haciéndose pasar por menores de edad, tras configurar algún tipo de juego, llegan a captar imágenes de menores, a través de la webcam, y a solicitar fotografías de los menores en situaciones de desnudez o videos con contenido sexual explícito, para su posterior ramificación en la web, llegando a ser un auténtico delito de posesión y distribución de pornografía infantil, o lo que se conoce como "grooming", acoso o extorsión de carácter sexual.

Ahora bien, se podría referir que la palabra "grooming", proveniente del idioma inglés, es una acción que refiere a preparación o acicalamiento de algo, también utilizada en la actualidad para hablar de acoso virtual, siendo por otro lado sinónimo de la palabra novio.

Autores como Buompadre sostiene que se habla de "grooming", cuando una "acción encaminada a establecer una vinculación y control emocional sobre un niño/a, cuya finalidad última es la de mantener una relación sexual con dicho menor"[13].

Morabito define al *grooming* como "el conjunto de estrategias que una persona adulta desarrolla para ganarse la confianza del menor a través de Internet con el fin último de obtener concesiones de índole sexual"[14]. Se trata, básicamente, de un abuso sexual virtual.

---

[13] Buompadre, Jorge, *Grooming*, "Revista Pensamiento Penal", Doctrina 40272, 2014.

[14] Morabito, Mario R., *La regulación de los "delitos informáticos" en el Código Penal argentino. Nuevas tendencias criminológicas en el ámbito de los delitos contra la integridad sexual y la problemática de persecución penal*, Bs. As., La Ley, 2011.

A su vez, Rovira del Canto indica que es posible esquematizar el acoso sexual infantil o *child grooming* en una serie de fases sucesivas, a saber: *a*) fase de amistad; *b*) toma de contacto, gustos, preferencias, confianza; *c*) fase de relación; *d*) confesiones personales e íntimas, consolidación; *e*) componente sexual; *f*) participación de actos de naturaleza sexual, fotografías, webcam; *g*) extorsión; *h*) escalada de peticiones; *i*) ¿agresión?[15].

He de preferir a diferencia del resto de la doctrina, tratar a esta conducta que ha tipificado ley argentina como "ciber-acoso" o "acoso informático", ya que traer una definición de una figura local con un significado en el idioma inglés, puede derivar en dificultades de interpretación y de la comprensión de los lectores y de toda la comunidad; sobre todo teniendo en cuenta que esta figura penal, no tiene arraigo local ni correlación con otras legislaciones, por lo que entiendo que debemos ponerle a esta conducta un nombre "criollo", y es entonces que propongo denominar esta acción típica, como "ciber-acoso" o "acoso informático".

1) *El artículo 131 del Código Penal, su génesis*. El legislador argentino ha decidido poner un freno a la actividad llevada a cabo por pedófilos y pervertidos sexuales, esto lo realizó con la creación de una nueva figura típica, el ya descripto "ciber-acoso", incorporado por la reforma de la ley 26.904 del 11/12/13, que en su art. 131, pena la conducta o acción llamada "acoso cibernético", un delito que solo puede cometido por medios informáticos como vimos más atrás.

Poco antes de su sanción legislativa con fecha (5/6/13), el Tribunal en lo Criminal n° 1 de Necochea, en los autos "F., L. N. s/corrupción de menores agravada" (expte. T.C. n° 4924-0244), donde se condenó al autor del hecho a la pena de 10 años de prisión por el delito de corrupción de menores, agravada por tratarse la víctima de una persona menor de doce años de edad y por el engaño como medio comisivo y en los fundamentos del fallo se determinaba cuáles eran las notas típicas de las maniobras del "*grooming*"; fallo del cual transcribiré algunas consideraciones del fallo al tratar la calificación penal del hecho, con consideraciones sumamente interesantes que transcribiré; ya que solo después de seis meses del fallo surgió el tipo penal que analizaremos.

"En el transcurso de las audiencias del debate se acudió al anglicismo 'grooming' para señalar una suerte de hilo conductor o marco aglutinante de las diversas actividades que realizaba Leandro Nicolás Fragosa. Lejos de endilgar una conducta atípica al nombrado o de vulnerar el principio de legalidad como deslizara la defensa al referirse al 'grooming', en el caso, esta actividad desplegada por Leandro Nicolás Fragosa, subsume perfectamente en el tipo objetivo y subjetivo de la norma del art. 125, párrafos segundo y tercero, del Código Penal, pues ellos son los actos corruptores de la menor de 8 años de edad, L.M. De esta manera, es importante deslindar que el 'grooming' corruptor de la menor realizado por Fragosa, es un concepto compuesto por un abanico más o menos acotado de conductas realizadas por un sujeto contra un menor de edad".

---

[15] Rovira del Canto, Enrique, *Ciberdelincuencia intrusiva: hacking y grooming*, conferencia, Barcelona, 2010, p. 6.

"En la exposición de motivos del proyecto de ley para penalizar específicamente el 'grooming', más allá que actualmente el 'grooming', forme parte de actividades abusivas y corruptoras, como en el caso de autos (expte.S n° 2174/11 con media sanción en el Congreso de la Nación) se explica que el 'grooming' consiste en acciones deliberadamente emprendidas por un adulto con el objetivo de ganarse la amistad de un menor de edad, al crearse una conexión emocional con el mismo, con el fin de disminuir las inhibiciones del niño y poder abusar sexualmente de él. Las redes sociales son un factor de riesgo para los menores, ya que no existe claridad respecto la identidad de las personas con quienes conversan o se relacionan".

"Etimológicamente, 'grooming' es una forma verbal de 'groom', vocablo cuyo significado alude a conductas de preparación o acicalamiento de algo, que en el ámbito de la pedofilia suele asociarse a toda acción que tenga por objetivo minar o socavar moral y psicológicamente a un niño, con el fin de conseguir su control a nivel emocional para un posterior abuso sexual. Respecto a su modus operandi, es una figura de 'acoso progresivo' que se verifica en etapas o períodos. Por lo mismo, suele denominársele también como 'acoso sexual infantil'".

"Sus características podrían ser resumidas de la siguiente forma: *a*) las conductas de childgrooming tienen como sujeto pasivo un menor de edad; *b*) progresivamente el acercamiento se transforma en acoso intimidatorio; *c*) se utilizan redes informáticas o telemáticas; *d*) las conductas tienen contenido sexual, sea porque se busque obtener material pornográfico o bien porque se pretenda realizar un abuso sexual físico; *e*) usualmente el agresor recurre a falsear su edad o identidad" (ver al respecto Scheechler Corona, Christian, *El childgrooming en la legislación penal chilena: sobre los cambios al artículo 366 quáter del Código Penal introducidos por la ley 20.526*, "Derecho y Ciencia Política", vol. 3, n° 1, 2012, p. 55 a 78).

"A su vez, el delito de corrupción de menores previsto en el art. 125 del Cód. Penal, en nuestro caso realizado a través de utilización de nuevas tecnologías, genera una variación de criterio en lo que en otras épocas podría haberse exigido la efectiva producción del resultado dañoso. Hoy entiendo que las nuevas posibilidades de interacción, como en autos se ha verificado a través del 'grooming', no requieren del tipo penal la efectiva producción de un resultado corruptor, ya que los verbos típicos de la figura son 'promover' y/o 'facilitar' la corrupción de un menor. Basta, entonces, para su configuración que las acciones sean desplegadas con ese objetivo. No será necesario que la víctima alcance el estado de corrupción para lograr la consumación, bastará la realización de actos tendientes a su logro (De Luca, Javier, *Delitos contra la integridad sexual*, Hammurabi, p. 157)".

Este precedente novedoso, parece ser el antecedente directo del tipo penal en cuestión, en relación a que considero que dio "la alerta", de la ausencia de legislación al respecto y además se describió de manera pormenorizada a esta nueva maniobra comisiva indicando a la sociedad su nocividad; aunque se soslayó la falta de consagración legal, se justificó de una manera razonable porque se resolvió esta cuestión problemática, con la figura del art. 125 del Cód. Penal.

El mencionado art 131 de nuestro Código Penal establece lo siguiente: "*Será penado con prisión de seis meses a cuatro años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito*

contra la integridad sexual de la misma" (artículo incorporado por la reforma de la ley 26.904 del 11/12/13).

Si se comparan las caracterizaciones teóricas del "grooming", con su determinación en el art. 131 del Cód. Penal, las diferencias son notorias. La figura delictiva del art. 131 involucra no sólo a la Internet, sino a otras telecomunicaciones. Relaciona personas con menores de edad, sin rangos preestablecidos de edad, aunque los propósitos del contacto sean similares.

He de coincidir plenamente con Garibaldi, en cuanto a que quien contacte a un menor con propósitos de cometer un delito contra la integridad sexual, pero no lo haga por medios informáticos, no quedaría comprendido en el "grooming", por lo que aquí el medio informático ha de ser un elemento necesario para la configuración del tipo delictual ya referido[16].

2) *Los valores jurídicos protegidos por este tipo penal*. Esta figura tiene como característica principal, crear una conexión emocional con el menor, con el fin de disminuir las inhibiciones del niño y poder abusar sexualmente de algún modo de él, corromperlo aprovechándose de su inmadurez sexual para obtener algo de ellos como fotografías y/o videos de contenido erótico, imágenes pornográficas del menor, incluso como primer paso o aproximación para un encuentro sexual, posiblemente por medio de abusos o con la finalidad de secuestrar al menor para explotarlo sexualmente, mejor conocido como "trata de personas", ya sea para que realizase espectáculos pornográficos o sometiéndolo a toma de fotografías y videos.

Una de las modalidades más comunes empleadas para llevar a cabo este tipo delictual es aquella en la que el sujeto activo trata de elaborar una identidad falsa de una persona de la misma edad y sexo de la que tiene el sujeto pasivo, ensayara temáticas comunes o adolescentes, conforme a la información que va obteniendo del menor, más la que arroja el perfil de sus redes sociales, para poder ganar su confianza; se esconde detrás del anonimato y de cuentas falsas, ya sean de alguna o varias redes sociales como de emails, cuentas que siempre dejan alguna huella si la investigación que se lleva a cabo es la correcta.

A medida que esta "pseudo-amistad" se fortalece, el adulto va obteniendo datos personales y de contacto del menor, comienza a utilizar tácticas como la seducción, la provocación, el envío de imágenes de contenido pornográfico, luego consigue finalmente que el menor se desnude o realice actos de naturaleza sexual frente a la webcam o envíe fotografías de igual tipo, llegando incluso a proponer encuentros disfrazados de juego con fines de secuestro, abuso sexual o posterior explotación sexual.

3) *El comienzo de ejecución*. Son suficientemente conocidas dentro de la teoría de la tentativa las cuatro etapas que se distinguen: ideación, preparación, tentativa y consumación. El punto clave de ese camino que delimita lo punible es el llamado comienzo de ejecución. Se trata de un principio garantista, recibido en gran número de códigos penales que lo mantienen.

---

[16] Garibaldi, Gustavo, *Aspectos dogmáticos del grooming legislado en Argentina*, Doctrina, 8/5/15, SAIJ: NV11208.

Dado que la tentativa solo existe cuando se comienza la ejecución del delito queda excluida la fase de deliberación interna y se consideran punibles como tentativa únicamente los actos externos.

Del principio de ejecución también es posible extraer que no todos los actos externos pueden ser considerados tentativa. Esa fase de la conducta punible se reserva a aquellos dirigidos a la realización del delito. De esta manera, los actos preparatorios son impunes, a menos que el legislador determine lo contrario. En todo caso, se trata de excepciones al principio general de impunidad de la preparación.

El Código Penal argentino recibe el principio vinculado al de legalidad constitucional al definir la tentativa como realización de aquel que "con el fin de cometer un delito determinado comienza su ejecución, pero no lo consuma por circunstancias ajenas a su voluntad" (art. 42).

Los delitos informáticos propios permiten distinguir fases. Es claro que no puede ser punida la ideación (*cogitationis poenam nemo patitur*); así, el problema remite a la etapa de preparación de un acceso no autorizado al castigo estatal.

Tal preparación comienza con la recolección de información sobre el objeto del ataque. El agente traza un perfil del sistema de la víctima (*footprint*), que le permitirá un ataque exitosamente dirigido. Dentro de la preparación, certifica luego los sistemas activos que se pueden alcanzar por Internet. Se trata de una fase de barrido que procura determinar las puertas de acceso y sistema operacional en uso. Evalúa así a la víctima y las probabilidades de éxito del ataque, de modo equiparable al merodeo e inteligencia previa de cualquier delito.

La última fase preparatoria es de enumeración y determinación de fragilidades de la víctima, que consiste en la identificación de las cuentas válidas de usuarios y de los recursos mal protegidos. Luego, el descubrimiento de contraseñas o identificación de puntos débiles es simplemente cuestión de tiempo. El comienzo de la ejecución y la consumación requieren el acceso a los datos y su lectura o ejecución.

Los delitos informáticos impropios comienzan su ejecución cuando tiene inicio la infracción respecto de la que el sistema informático es un medio. He mostrado que en el caso de la ley argentina solo a través de ciertos sistemas de comunicación (electrónico, telecomunicaciones u otra tecnología de transmisión de datos) se puede dar inicio a un intento de contacto típico. Pero además, bastaría con comenzar a contactarse, una acción que solo la buena interpretación permitirá no alejarse desmedidamente del efectivo contacto. En cualquier caso, resulta extraño y poco razonable.

De por sí es problemático especificar cuáles son las características definitorias de una figura legal donde intervienen elementos valorativos, así como también una descripción que sea análoga a la propia definición. Las acciones pueden describirse de distintas maneras, en atención a las propiedades empíricas que presentan e incluyen en la descripción. En cualquier caso, aparecerá el problema de la indeterminación del lenguaje natural.

No se contacta ni se intenta contactar –en un sentido típico– sino quien lo hace con cierta desvalorada ultra-intención. Se contacta y lo intenta quien se contacta o intenta contactar, vale decir, quien establece o intenta establecer contacto o

comunicación con un menor de edad, con una intención mediata, que es menoscabar su integridad sexual.

De esta manera: ¿intenta contactarse quien simplemente llama a quien no atiende por estar ocupado en ese momento?; ¿se contacta quien es atendido, pero no recibe respuesta?; ¿desiste voluntariamente quien no responde a quien atiende o en ese caso, ni se contacta, ni intenta contactarse?

Cualquier modalidad planificada de “acoso informático”, incluye, probablemente, varias fases. Es razonable pensar en la generación de un lazo de amistad con el menor, frecuentemente, fingiendo ser un niño o una niña. Luego, la obtención de información del menor, preparando la fase de afectación. Una etapa que incluye la seducción, procurando conductas con significado sexual y quizá, finalmente, la extorsión para hacerse de pornografía o lograr contacto físico prohibido.

Esto implica un complejo entramado de conductas equiparable, en cierta forma, a la descripción realizada para los delitos informáticos en sentido estricto o propio, donde en todo caso la seducción en busca de ciertas conductas se equipara al acceso a los datos en los delitos propiamente informáticos.

Simplificado por una única acción consistente en contactar (por cierto medio y con cierta inconfesable finalidad), ni siquiera permite su adecuación a la especie de delito informático impropio. Se sanciona la realización de un acto que, cometido personalmente, sería preparatorio de alguna de las especies tradicionalmente legisladas para reprimir afectaciones contra la integridad sexual. Pero además, teniendo en cuenta sus orígenes, se legisla el “ciber-acoso”, previendo su consumación, cuando no hay preparación ni acicalamiento ni acción alguna que tienda a socavar moral o psicológicamente al menor.

Chiara Díaz dice que en el art. 131 del Cód. Penal “se ubicó la figura de hacer proposiciones a niños con fines sexuales”, al considerarse insuficiente para la protección de niños y jóvenes la producción, ofrecimiento, difusión o posesión de pornografía infantil por medio de un sistema informático[17]. Explica que se tuvieron en cuenta, especialmente, las facilidades para enmascarar identidades, crear otras y mantener el anonimato en redes sociales cibernéticas.

Fue para el citado autor una tipificación poco precisa, a su juicio, conseguía márgenes de impunidad respecto de afectaciones a la integridad sexual de los menores que eran inicio al camino del acoso cibernético.

Elogia Chiara Díaz, así que, con auxilio de antecedentes extranjeros notables y la opinión de expertos en la materia, se haya adelantado la franja de punición para comportamientos anteriores a delitos más graves. Llama la atención el elogio, sobre todo si realizó una crítica sobre la precisión de la legislación que adelanta la punición de delitos más graves.

Y digo que también me llama la atención dicho elogio, porque la figura legislada no consiste en “hacer proposiciones a niños”, ya que por lo pronto no lo son todos los

[17] Chiara Díaz, Carlos A., *Incorporación del grooming al Código Penal argentino*, elDial.com CC37BB.

menores de dieciocho años. Además, contactar con cierto propósito no equivale a proponer.

Si algo cabe decir de la tipificación, es que ahora estamos frente a una específicamente poco precisa descripción que no solo admite perseguir acciones ciertamente alejadas del acoso cibernético, sino también de cualquier afectación razonablemente delictiva de la integridad sexual.

El fortalecimiento doctrinario de cualquier decisión o propuesta vinculada a la legislación represiva exige, primero, una legitimación positiva. Restar facilidades a los pederastas –escrupulosos o no– puede ser un objetivo deseable, pero la validación de la amenaza y la sanción penal exigen la configuración de una conducta que se esté facultado a prohibir, convirtiéndola en delito. Solo entonces de esa forma y con esa tipificación, podrá ser cometido el delito y con ello generará un reproche penal.

4) *Los problemas del "acoso informático" en el Código Penal, su análisis, el señalamiento de las diversas dificultades de la figura y posibles soluciones*. Los problemas que plantea esta regla son variados.

A poco tiempo de sancionada esta figura típica en el ámbito del Congreso Nacional (0927-D-2015 trámite parlamentario 11, 16/3/15) firmado por el legislador Manuel Garrido, se planteó su seria necesidad de reforma aduciendo que la redacción de la figura tiene varios problemas.

En primer lugar, se menciona que el tipo penal incrimina la conducta de quien "contacte" a una persona menor de edad con el propósito de cometer cualquier delito contra su integridad sexual. Siendo de esta forma, la mera comunicación, comprobada la ultra finalidad exigida, basta para la realización del tipo, penando un acto preparatorio del delito cuya comisión se perseguiría con el contacto, lo que aparece como un adelanto de la punibilidad irracional, que atenta contra los principios rectores del derecho penal.

Luego el otro señalamiento que se da en esta figura es que se exige que el contacto tenga "el propósito" de cometer algún delito de índole sexual. Y conlleva esta redacción el inconveniente o dificultad para probar que ese propósito existió en el caso concreto, porque se requiere para que haya "grooming" debe consolidarse una ultra-finalidad delictiva en la conducta de quien se contacte con el menor de edad.

En tercer lugar, se planteó que la escala penal prevista para el delito de "acoso informático", es igual a la pena del abuso sexual consumado.

Menciona el anteproyecto de ley en este sentido: "art. 131 del Código Penal establece una pena de seis meses a cuatro años, es decir, la misma pena que establece el Código Penal para el abuso sexual en el art. 119" ("*Será reprimido con reclusión o prisión de seis meses a cuatro años el que abusare sexualmente de persona de uno u otro sexo cuando, ésta fuera menor de trece años o cuando mediare violencia, amenaza, abuso coactivo o intimidatorio de una relación de dependencia, de autoridad, o de poder, o aprovechándose de que la víctima por cualquier causa no haya podido consentir libremente la acción*").

De esta manera, el autor del anteproyecto reprocha, que con la misma pena la conducta de quien ejecuta el acto preparatorio de contactarse con el propósito de

cometer el delito de abuso sexual, que la conducta de quien consuma el delito de abuso sexual, lo cual es a todas luces irrazonable.

Por otro lado, señalo que el art. 131 del Cód. Penal no distingue entre las distintas edades de la menor víctima de "grooming", por lo que el sujeto pasivo del delito puede ser cualquier persona menor de dieciocho años, en contradicción con el art. 119 del Cód. Penal, que refiere a personas menores de trece años de edad. Igual crítica merece el tratamiento del sujeto activo del tipo penal, por cuanto se incluye también a los menores de edad. De esta forma, un menor de diecisiete años que se "contacta" con una menor de su edad puede quedar comprendido en integridad sexual. Es evidente que esto puede dar lugar a aplicaciones irracionales del tipo penal.

Por otro lado, el delito previsto por el art. 131 resulta de acción pública, mientras que los delitos comprendidos en los arts. 119, 120 y 130 dependen de instancia privada, con lo cual pueden plantearse complejidades procesales que se evitarían estableciendo que el delito de "grooming" dependa de instancia privada, máxime si tiene en cuenta la reforma producida por la ley 27.206, que entró en vigencia el 10 de noviembre de 2015, por medio de la cual se modifican los arts. 63 y 67 del Cód. Penal, estableciendo que en ciertos delitos contra la integridad sexual y de trata de personas, se suspende la prescripción mientras la víctima sea menor de edad y hasta que habiendo cumplido la mayoría de edad formule por sí la denuncia o ratifique la formulada por sus representantes legales durante su minoría de edad, no incluyendo al delito previsto en el art. 131 como sí lo fueron los delitos sexuales.

También, es cuestionable el art. 131 ya que deja abierto un amplio margen a la arbitrariedad dada su vaguedad y amplitud. Por su parte, la Corte Interamericana de Derechos Humanos en diferentes casos contenciosos sostuvo que es incompatible con la Convención Americana el tipo penal que no es preciso en el establecimiento de la conducta delictiva. En diversas ocasiones sostuvo: "*La Corte entiende que en la elaboración de los tipos penales es preciso utilizar términos estrictos y unívocos, que acoten claramente las conductas punibles, dando pleno sentido al principio de legalidad penal*".

Esto implica una clara definición de la conducta incriminada, que fije sus elementos y permita deslindarla de comportamientos no punibles o conductas ilícitas sancionables con medidas no penales. La ambigüedad en la formulación de los tipos penales genera dudas y abre el campo al arbitrio de la autoridad, particularmente indeseable cuando se trata de establecer la responsabilidad penal de los individuos y sancionarla con penas que afectan severamente bienes fundamentales, como la vida o la libertad.

Estas normas al no delimitar estrictamente las conductas delictuosas, son violatorias del principio de legalidad establecido en el art. 9 de la Convención Americana y al mismo tiempo dejarían impunes muchas conductas que la sociedad considera altamente nocivas y dañosas para los niños.

Es de destacar también que se encuentra en pleno debate un anteproyecto de Código Penal de la Nación que en su art. 133, inc. 2°, considera al delito de "ciber-acoso", un acto preparatorio, estableciendo que "*Será penado con prisión de uno a cinco años el mayor de edad que tomare contacto con un menor de trece años,*

mediante conversaciones o relatos de contenido sexual, con el fin de preparar un delito de este Título".

Considero a mi criterio que el tipo penal propuesto por el Anteproyecto adolece de varios de los problemas que observamos en el actual art. 131. En efecto, el verbo típico que la norma recepta es el de "tomare contacto", lo que sigue dejando abierto un amplio margen para la arbitrariedad, el uso de este verbo no solo no corrige la redacción actual del articulado, sino que también por la forma que está redactado el artículo le quita de manera inexplicable al delito descripto su principal elemento típico que por excelencia lo caracteriza como el requisito necesario para su comisión; los medios de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos.

Por lo que, de este modo, quien tomare contacto mediante conversaciones o relatos con un menor de trece años con el fin de preparar un delito del título contra la integridad sexual puede hacerlo mediante conversaciones o relatos que nos sean cometidos por medios informáticos y en vez de penar el acto preparatorio del delito de "*ciber-acoso*".

En este aspecto considero que se sincera y se argumenta, en la redacción de este anteproyecto, la circunstancia de que se podría penar el acto preparatorio de por ejemplo una corrupción de menores.

Pero a la figura a mi criterio, este contacto con la finalidad de menoscabar la integridad sexual, es lo que se quiere proteger con la figura delictiva, conforme lo establecido en la CDÑ (arts. 3 y 16) y el Protocolo Facultativo de la Convención relativa a la Venta de Niños, Prostitución Infantil y la Utilización de Niños en la Pornografía infantil incorporado por ley 25.763 a nuestra legislación en relación a que dispone "*1. Todo Estado parte adoptará medidas para que, como mínimo, los actos y actividades que a continuación se enumeran queden íntegramente comprendidos en su legislación penal, tanto si se han cometido dentro como fuera de sus fronteras, o si se han perpetrado individual o colectivamente: …c) Producir, distribuir, divulgar, importar, exportar, ofrecer, vender o poseer, con los fines antes señalados, material pornográfico en que se utilicen niños, en el sentido en que se define en el art. 2…. 2. Con sujeción a los preceptos de la legislación de los Estados partes, estas disposiciones se aplicarán también en los casos de tentativa de cometer cualquiera de estos actos y de complicidad o participación en cualquiera de ellos. 3. Todo Estado parte castigará estos delitos con penas adecuadas a su gravedad. 4. Con sujeción a los preceptos de su legislación, los Estados partes adoptarán, cuando proceda, disposiciones que permitan hacer efectiva la responsabilidad de personas jurídicas por los delitos enunciados en el párrafo 1 del presente artículo. Con sujeción a los principios jurídicos aplicables en el Estado parte, la responsabilidad de las personas jurídicas podrá ser penal, civil o administrativa*".

Lo mismo parece suceder con lo normado con el art. 8 del Protocolo, donde se dispone que "*1. Los Estados partes adoptarán medidas adecuadas para proteger en todas las fases del proceso penal los derechos e intereses de los niños víctimas de las prácticas prohibidas por el presente Protocolo y, en particular, deberán: a) Reconocer la vulnerabilidad de los niños víctimas y adaptar los procedimientos de forma que se reconozcan sus necesidades especiales, incluidas las necesidades especiales para declarar como testigos. b) Informar a los niños víctimas de sus*

derechos, su papel, el alcance, las fechas y la marcha de las actuaciones y la resolución de la causa. c) Autorizar la presentación y consideración de las opiniones, necesidades y preocupaciones de los niños víctimas en las actuaciones en que se vean afectados sus intereses personales, de una manera integral…. e) Proteger debidamente la intimidad e identidad de los niños víctimas y adoptar medidas de conformidad con la legislación nacional para evitar la divulgación de información que pueda conducir a su identificación; 3. Los Estados partes velarán por que en el tratamiento por la justicia penal de los niños víctimas de los delitos enunciados en el presente Protocolo la consideración primordial sea el interés superior del niño. 6. Nada de lo dispuesto en el presente artículo se entenderá en perjuicio de los derechos del acusado a un juicio justo e imparcial, ni será incompatible con esos derechos".

Por lo que parece que este instrumento internacional suscripto podría ser incompatible con normativa propuesta como modificatoria del Código Penal.

Situación esta que también existe con la redacción del art. 125 actual de nuestro Código Penal que contempla las modalidades típicas dispuestas en el art. 2, inc. *c* del Protocolo, que castiga las acciones de producir, distribuir, divulgar, importar, exportar, ofrecer, vender o poseer, con los fines antes señalados, material pornográfico en que se utilicen niños y la figura propuesta en el art. 131, inc. 1, del Anteproyecto del Código dispone: "*1. Será reprimido con prisión de uno a seis años, el que por cualquier medio publicare, produjere, comerciare o divulgare imágenes de actividades sexuales explícitas de menores*", situación que parece ser no totalmente compatible con la obligación asumida internacionalmente de penar ciertas conductas para castigar la pornografía infantil que de ser sancionada como norma podría tener responsabilidad para el Estado argentino.

Asimismo y en este caso coincido con Garrido por los argumentos ya señalados, que el texto del anteproyecto mantiene para el acto preparatorio, que se ha elegido conminar con pena, una escala penal que no guarda proporción con los delitos contra la integridad sexual consumados, tales como los previstos en el art. 127 del propio Anteproyecto.

Finalmente la utilización de la expresión para definir los medios comisivos del delito, puede traer inconvenientes, ya que se establece que serían punibles las acciones que se efectuaran mediante "conversaciones o relatos de contenido sexual" que a mi criterio, tiene la dificultad de establecer de antemano, lo que sería una conversación o un relato y que no lo es; porque lo que entiendo que es posible entablar un contacto pernicioso y peligroso para la integridad sexual de un niño sin realizar cabalmente, un relato o una conversación.

Entiendo que habría que recalar como una medida de técnica legislativa en medios comisivos, más generales, para poder contextualizar la acción y no dejar en un segundo plano la finalidad del autor, que sería entonces la voluntad direccionadas para vulnerar la inocencia sexual del niño de cualquier forma con medios informáticos que pueden no tener la forma convencional de relatos o conversaciones (emoticones, fotos, chistes sexuales, envío de links, etcétera).

Por lo que entiendo que cuando el contenido del contacto es de contenido sexual y si el contacto ya se comenzó de una forma seria y consecuente (como explicaremos más adelante) para captar la atención del niño, para vulnerar su sexualidad y se

explicitó de cualquier forma esa intención, quedaría configurado el “ciber-acoso” conforme lo que se le debería exigir el tipo penal.

a) *La escala penal y su significado*. Siendo que el tope de la escala penal es de cuatro años, este tipo delictual puede ser imputado a personas menores de edad, aquellas comprendidas entre los dieciséis a dieciocho años, ello en función de lo establecido en el art. 1 de la ley 22.278. De modo que puede implicar el contacto de un chico de dieciséis años con un niño de mucha menor edad. En suma, el contacto puede llegar a suceder entre personas no adultas y con pocas diferencias de edad.

Tiene una escala penal amplia, ello debido a que su mínimo, seis meses, permite la aplicación de institutos tales como la suspensión del juicio a prueba o la condena de ejecución condicional, siempre y cuando se cumpla con las condiciones que establece la normativa de fondo y forma. Por el otro lado, en su tope de pena máximo, estos beneficios quedan vedados, siendo de aplicación penas privativas de libertad de efectivo cumplimiento.

Esta escala es significativamente menor a la establecida para el delito de corrupción de menores, de modo que permite soluciones paradojales, pues un acto que prepararía una corrupción de menores podría llegar a ser considerado más grave que otro que lo lleve a cabo, no lo que parece lógico.

b) *Algunos problemas semánticos y su importancia*. La expresión “menor de edad” no ha sido definida y su interpretación puede plantear problemas, por ello se propuso ya a muy poco tiempo de la sanción en esta reforma legislativa que evocamos más arriba, derogar el art. 131, e incorporar y modificar la conducta típica estableciendo que el delito de “acoso informático” se configure cuando un sujeto mayor de edad requiera de cualquier modo a una persona menor de trece años que realice actividades sexuales explícitas o actos con connotación sexual o le solicite imágenes de sí misma con contenido sexual. De esta manera el tipo penal se configura cuando un mayor de edad –a diferencia de la actual redacción que admite que el sujeto activo sea un menor de edad– le requiera algún tipo del material de mención.

Por otro lado, se ha sugerido el reemplazo del vago concepto de “contacto”, siendo el mismo poco preciso y dificultoso al momento de establecer cuando queda configurado. Otra dificultad, de índole probatoria, surge del término “propósito”, ya sea realizando actividades sexuales explícitas, actos con connotación sexual o solicitando imágenes con contenido sexual, probar la intención o propósito resulta para las partes una gran complejidad, siendo este un elemento psicológico que solo podría ser acreditado a través de pericias de rigor y de la sana critica llevado a cabo por los magistrados al momento de valorar la prueba.

En el segundo párrafo del art. 125 ter propuesto, se prevé el caso de que el sujeto pasivo del requerimiento que configura el delito de “acoso informático” sea una persona comprendida en la franja etaria que va de los trece a los dieciséis años. En ese caso, se configurará el delito cuando la persona mayor de edad engañe, abuse de su autoridad o intimide a la persona menor de edad. De esta forma el tipo penal propuesto es congruente y armónico con el art. 119 del Cód. Penal.

c) *La palabra “contactare” suscita también dificultades*. ¿Cuándo se logra el contacto? ¿Cuándo el menor de edad recibe la comunicación o simplemente cuando se emite? ¿Si el contacto se logra cuando el menor recibe la comunicación cómo

debería considerarse la mera remisión del mensaje? ¿Podría llegar a considerarse como una tentativa? ¿Cuándo comienza a ejecutarse el delito?

El contacto implica una relación entre personas que pueden estar ubicadas en sitios próximos o extremadamente lejanos. ¿Cuál es el lugar en que este contacto se lleva a cabo? Esta información es fundamental para determinar la ley aplicable, y en especial, la jurisdicción que debe intervenir.

La palabra contactar o contactare, según la RAE, es “establecer contacto o comunicación con alguien”, por lo que claramente el contacto debe lograrse y por como está establecido en la figura actual, solo puede hacerse a través de un medio informático, quedando claro que por los menos para que la conducta tenga alguna nota de tipicidad ese contacto debe tener la intención de menoscabar la integridad sexual del menor, por lo que entiendo que una simple presentación o dialogo de chat o intercambio de mail, por más de que la persona mayor tenga una identidad supuesta con el menor, si no genera diálogos intencionados o direccionados a menoscabar su integridad sexual, la conducta no podrá ser típica, circunstancias que me llevan a inclinarme en estos casos a descartar la tentativa.

También considero que no es posible tomar como típico la mera remisión del mensaje, sino que es necesario que ese contacto, tome estado, es decir debe generarse un diálogo o contacto con la intención de menoscabar la integridad sexual del menor o acelerar o desvirtuar su madurez sexual con un engaño realizado de forma virtual. En otras palabras, el tipo penal requiere para quedar configurado el contacto, y para que este se dé, el menor víctima debe haber recibido el material que el sujeto victimario le enviara, caso contrario no podría imputársele la comisión de delito previsto al sujeto activo.

Para interpretar el término contactare debe tenerse en cuenta el funcionamiento de estas herramientas de comunicación virtual como así también las pautas sociales de cómo se establece un contacto, ya sea a través de un chat, en alguna rede social o vía mail, situación que regularmente requiere un ida y vuelta en la comunicación y que debe tener como contenido una intención de menoscabo a la integridad sexual de uno de los intervinientes, por lo que considero que cuando ese contacto debe ser sí o sí (con ida y vuelta).

Es decir que cuando se sugiera o pregunte cuestiones de índole sexual a la víctima o se indague con cuestiones que no tengan que ver a su edad o madurez sexual tendremos el principio de ejecución de este delito.

Lo que parece claro y evidente, que luego para saber si hubo o no contacto va a depender de la prueba que se pueda obtener sobre esos extremos, sobre todo si lo que se juzga en este delito requiere de un extremo u elemento objetivo (el contacto por medios informáticos) y uno subjetivo (que sea con la finalidad de menoscabar la integridad de la víctima).

Considero, para hacer una primera apreciación sobre el tema, que el lugar de contacto para determinar la ley aplicable, y en especial, la jurisdicción que debe intervenir, es donde el sujeto activo realiza el contacto informático con el sujeto pasivo y el lugar de donde se produce el chat o intercambio de mensajes con la finalidad de menoscabar la integridad sexual cuando se consuma la totalidad de la acción típica y ha de tenerse en cuenta para ello también el interés superior del niño (arts. 3, 16

puntos 1 y 2, 19 puntos 1 y 2 de la CIDÑ), para combatir este delito por lo que es necesario tomar como un punto de conexión, impuesto por la convención que nos llama a proteger los derechos de los niños, el domicilio de la víctima de donde se realizó el contacto y allí determinar la ley aplicable y la jurisdicción, para evitar vulnerar normas de derecho convencional.

d) *Un problema que suscita el art. 131 del Cód. Penal es su vinculación con el art. 125*. Como ya adelante, es aquí, donde nos encontramos con una relación asimétrica de figuras, que son las que pueden entablar un hombre o una mujer adulta (sujetos activos) con el propósito de establecer lazos de amistad con un niño o niña (sujetos pasivos del delito) a través de Internet (que obra como un elemento o modo comisivo del tipo).

Consideramos que la conducta típica se consuma cuando el mayor contacta al menor con el único propósito de cometer cualquier delito contra la integridad sexual, y luego puede ser parte o no de maniobra de tipo corruptora para la integridad sexual del niño o la niña.

Ahora bien, al parecer el legislador ha penado una conducta previa o anterior a los otros delitos contra la integridad sexual, lo que puede generar el interrogante de si lo contemplado por el art. 131 del Cód. Penal, queda desplazado o no por otras figuras que puede tener como medio comisivo a las redes sociales, o si por el contrario, se debe entender que el legislador ha creado el “acoso-informático”, como una figura de peligro que no le quita el contenido delictual a la figura, dando así nacimiento a un nuevo interrogante: ¿Cómo debería concurrir esta figura con el resto de las figuras como por ejemplo la contemplada por el art. 125 del Cód. Penal?

En este tópico la diferencia se hace más difusa ya que es complicado deslindar donde termina la acción típica del “ciber-acoso” y donde comienza la de la corrupción de menores, ello puede radicar básicamente en una cuestión probatoria que habrá de desarrollarse en el derecho penal de forma y no de fondo, cuestiones que se suscitan al accionar de las partes y que serán admisibles conforme lo estipule cada ordenamiento adjetivo.

El término corrupción de menores, tal como lo enuncia el art. 125 del Cód. Penal, ha generado crítica por alguna parte de la doctrina en cuanto a la imprecisión y vaguedad del término en sí mismo.

Podríamos definir a esta acción típica como lo ha hecho el Superior Tribunal de la Provincia de Córdoba en el fallo dictado por la Sala I Penal (“P., A. O. y otra p.ss.aa., promoción a la corrupción de menores agravado -Recurso de Casación-” (expte. “P”, 70/10, del 10 de marzo de 2013) que a continuación se transcribe: “La corrupción de menores es una depravación de los modos del acto sexual, por lo perverso, lo prematuro o lo excesivo. Ello puede ocurrir porque el acto sexual sea perverso en sí mismo, en su ejecución; o volviéndose prematuro por su práctica lujuriosa habitual precoz, con menores, que por su edad o desarrollo no alcanzaron aún el grado de madurez física y psíquica que según la naturaleza y la sociedad se requiere para mantener una vida sexual normal, o, finalmente, volviéndose excesivo por su cantidad, como ocurre cuando los abusos son plurales y se ubican en un extenso período de tiempo” y agregó “En orden al bien jurídico protegido por el tipo penal de la promoción a la corrupción de menores, se acepta que se trata de un delito que atenta contra el

derecho de las personas que, en razón de su edad no han alcanzado la plena madurez física, psíquica y sexual, a no ser sometidos a tratos sexuales anormales en sus modos, cuya práctica puede en el futuro impedirles tomar decisiones de índole sexual carentes de deformaciones. Es el derecho que los menores de edad tienen al libre desarrollo de su personalidad, particularmente en el aspecto sexual".

La materialidad ilícita de un caso hipotético. Ahora bien, supongamos que un agresor sexual contacta a una niña de doce años vía Facebook simulando su identidad por la de una niña de la misma edad, mantiene contacto vía chat con ella, y luego de la primera semana comienza a enviar mensajes desde la computadora personal que poseía en su hogar en la ciudad de La Plata, mediante la cuenta de correo electrónico ejemplo1@hotmail.com.

También supongamos que el agresor se hizo pasar por una niña de menor edad y le requirió a una niña menor de edad que se sacara fotos, primero vestida, luego en ropa interior, después desnuda, después tocándose los genitales, o mostrando el ano y desnuda con sus piernas abiertas hacia la cámara, solicitando se las enviara a través de Facebook Messengger.

Y digamos que la niña inicialmente oponía reparos a los requerimientos usando como motivo que su máquina de fotografiar estaba rota, y más tarde, luego de haber cedido tras la insistencia del agresor y sus técnicas de manipulación envió una cantidad importante, aunque imprecisa, de fotografías, imágenes que luego el agresor utilizaba como medio para coaccionarla, indicándole que de no continuar con los envíos, exhibiría las fotos recibidas en las redes sociales, llevándose a cabo este tipo de mensajes por el lapso de un mes.

Conjeturemos que entre las fotos enviadas se cuentan una que la muestra desnuda acostada, con las piernas flexionadas y entreabiertas en dirección a la cámara, otra desnuda con exhibición de los pechos y otra fotografía con la niña en ropa interior.

Además, tengamos como probado que el autor acopiaba, más de cuatro mil fotografías de iguales características, claramente destinadas a su difusión.

e) *El planteo hipotético de un caso y sus dificultades*. Ahora bien, luego de haber establecido previamente una materialidad ilícita hipotética, podrían plantearse los siguientes interrogantes, que a su vez pueden ser herramientas útiles para comprender y analizar esta joven figura penal.

Las preguntas.

1) ¿Cómo deben ser calificados estos hechos y como debo hacerlos concurrir?

2) ¿En este caso quedaría subsumida la figura del "ciber-acoso" en un concurso aparente o son figuras que pueden concurrir en forma ideal o real?

3) ¿Existe una inconsistencia de valor con la figura del art. 125 agravada por amenazas en cuanto la excesiva pena en relación a la figura del art. 119 cuando existe un abuso sexual con penetración y un caso como el planteado?

4) ¿Puede existir doble valoración de una conducta, si en una sentencia se valora como agravante a la forma de lograr contacto con la víctima, siendo las redes sociales

un medio que facilita la comisión del delito y tal circunstancia es aprovechada por el autor?

Habiendo establecido las preguntas, daremos algunas aproximaciones.

Las posibles respuestas a estos interrogantes, con más interrogantes

1) Para responder el primer interrogante, me preguntaré como puedo calificar los hechos y en segundo lugar como los puedo hacer concurrir.

a) ¿Cuáles serían las posibles calificaciones a emplear?

A primera vista, sin dudas podríamos pensar que se encuentra presente según las características del caso el delito de corrupción de menores de trece años con amenazas.

Ya que si pesamos que inducir y obligar a una niña de doce años a tomarse fotografías, en ropa interior, desnuda, con un dedo en la vagina y en el ano o masturbándose, durante un proceso que duró aproximadamente un mes, son acciones que claramente indican la intención de iniciar tempranamente en prácticas sexuales inapropiadas a la niña víctima en este hecho, que carecía de experiencia sexual elemental, que se evidenció en el desconocimiento del funcionamiento de sus genitales. Esa inexperiencia puede ser aprovechada por el acusado al fingir una edad y un sexo capaces de facilitar la maniobra, incluso amenazando a la niña para lograr que esta acceda al envío de más fotografías.

Estas acciones además podrían configuran un adelantamiento inapropiado en la sexualidad de la niña, son maniobras que la someten a una exposición inadecuada de su intimidad, por provocada y sostenida en el tiempo, aún pese a las primeras resistencias de la niña (art. 125, párr. 2°, Cód. Penal).

Haber obligado a la víctima a entregar más fotografías indicándole que de no hacerlo exhibiría las fotografías ya recibidas, a través de mensajes de Facebook y Messenger son acciones inequívocamente intencionales e implican amenazarla para hacer algo contra su voluntad, pues le prometen un mal, una agresión a la identidad y a la intimidad de la niña, con la difusión de sus fotografías desnuda en las posiciones que he descripto. Un mal destinado a vencer su voluntad para que se tome nuevas fotografías y se las remita.

También podría calificarse esta conducta como producción, tenencia y distribución de imágenes con pornografía infantil.

Las acciones desplegadas pueden implicar la producción de imágenes con representaciones de actividades sexuales de niños menores de dieciocho años de edad.

Las imágenes con el tocamiento de la vagina, o la exhibición de ésta, o de los pechos con el pubis, constituyen estas representaciones, que el autor buscó el resultado lesivo y un producto que siempre tuvo la intención de generar.

Se puede pensar aquí que esta producción de fotografías, se pensó y deliberó, ya que se puede indicar a una niña como fotografiarse, con indicaciones claras y precisas para enviarlas a su acechador.

Esta “dirección clara de las tomas fotográficas” puede formar parte de su producción en los términos que indica el tipo penal.

Es importante como elemento de la finalidad, el que puede extraerse de los diálogos con contenido sexual explícito, también puede ser indicador de esta intención, los elogios que el acosador pueda realizar de las fotografías que recibía a la víctima, para en solapar el contenido sexual de la producción.

Pienso que se debería entender que “producir” una imagen, en este caso fotográfica, no es sólo obturar la cámara fotográfica que la registra, pues “producir” significa también “procurar, originar, ocasionar” y “ocasionar” significa “ser causa o motivo para que ocurra una cosa”.

La recepción de estas fotografías, configura su tenencia a las que se suma la enorme cantidad de imágenes similares que suelen encontrarse en los discos rígidos de las computadoras utilizadas para tales fines.

Es común en estos casos que el acosador tenga una verdadera “voracidad de imágenes fotográficas” y es común que se busquen mecanismos para su difusión en Internet, y de páginas de difusión de imágenes de páginas pornográficas, que premian con dinero a los suscriptores, que envían el material con esa artera finalidad, puede exhibir la intención de distribución de esas imágenes de forma ilícita, sobre todo sí se le hacía saber a la niña, luego de que preguntara con ingenuidad las razones de los requerimientos de tanta cantidad de fotografías y se le respondiera “que las fotos tienen valor, las fotos valen en la red”, circunstancia que también puede indicar una intención de comercializar el material pornográfico.

Claramente en esta hipótesis se puede observar como el agresor utiliza los medios informáticos, y el anonimato y como estos medios le permiten, acercarse a la niña, fingiendo ser otra persona y aproximándose paso a paso, con cada palabra, con cada pedido, a obtener imágenes de esta con contenido sexual, solicitando en un comienzo que se quite alguna que otra prenda insignificante o que posara de tal o cual manera frente al lente de la cámara, para luego, tras haber adquirido la confianza de la niña.

Luego es notorio que se avanza sobre su voluntad requiriendo fotos con mayor grado de desnudez o menoscabo sexual, hasta lograr obtener imágenes que por su contenido faculte al agresor a amenazar a la niña, como ya se precisó, con la intención de obtener más imágenes, transformándose esta situación en una verdadera tortura.

Creo que finalmente y acorde los hechos descriptos y trazando un paralelismo con el análisis efectuado, desde el terreno de lo hipotético, podrían calificarse como corrupción agravada de menores, en concurso ideal con producción de material pornográfico infantil y “ciber acoso”, en concurso real con acopio de material pornográfico, conforme lo normado por los arts. 125 segundo párrafo, 128 primer y segundo párrafo y 131 del Cód. Penal.

b) ¿Qué posibilidad de concursos pueden darse en este caso?

He de soslayar desde lo hipotético los posibles concursos que pueden darse en el caso planteado al inicio.

Por un lado la corrupción agravada por amenazas que se inicia en un momento y se extiende en el tiempo consignado en la narración, en cuyo contexto se produjeron

imágenes de contenido pornográfico infantil, justifica el llamado concurso ideal que regula el art. 54 del Cód. Penal, en relación a la corrupción y la producción de imágenes de pornografía infantil; y el "ciber-acoso" que se consuma antes de consolidarse el proceso de corrupción con los mensajes de texto y la clara intención de corromper a la niña con amenazas luego destinadas a obtener un número mayor de fotografías de similares características, motivo por el cual considero este hecho como independiente de los que concurren en forma ideal (art. 55).

También podría considerarse finalmente que hubo acopio y distribución de esas y otras numerosas fotografías, motivo por el cual este acopio también es independiente de la corrupción considerada (art. 55).

Considero entonces, como adelante, que no son independientes al hecho, los delitos de "ciber-acoso" y el de producción de material pornográfico, por lo que entiendo aquí que la concurrencia es solo formal (art. 54), ya que estos delitos se cometieron con una unidad de intención y propósito de menoscabar la integridad sexual de la víctima de la cual se la corrompió con amenazas y se realizaron otras figuras penales como expliqué.

2) ¿Se puede utilizar el concurso aparente para resolver este entuerto?

Sin entrar en la discusión de la utilidad y la legitimidad del concurso aparente, y siendo este tipo de solución aceptada en la actualidad por la doctrina penal, considero que hay casos en que la conducta típica del "ciber-acoso", puede quedar subsumida en otra figura, por ejemplo si se contacta a un menor a través de medios informáticos con la intención de menoscabar su integridad sexual, al que luego se lo corrompe (art. 125) o se lo abusa sexualmente (art. 119).

No obstante ello, como lo justifiqué anteriormente, la solución legal más justa y equitativa para resolver esta situación problemática, sería hacer concurrir estos dos delitos en forma ideal (art. 54), en razón de haber una unidad de finalidad delictiva en vulnerar la integridad sexual de un niño o un adolescente.

También no me parece una buena idea que en tiempos de tanta conflictividad social, apelemos para solucionar un problema complejo como el descripto, una creación doctrinaria, que no tiene consagración legal, cuando tenemos a la mano una solución legal, porque como sociedad, tenemos que apegarnos a la ley vigente, porque la raíz de nuestros problemas pueden estar, básicamente en los constantes desapegos a la ley que hemos tenido por oír "el canto de las sirenas" de parte de la doctrina jurídica argentina.

3) ¿Existen inconsistencias de valor en las figuras de la corrupción agravada por amenazas y el abuso sexual con acceso carnal?

Como hemos visto en este hipotético caso la calificación que hemos propuesto es la de corrupción de menores agravada por el uso de amenazas en virtud de lo normado por el art. 125, tercer párrafo, del Cód. Penal, pena que legalmente prevé un mínimo de diez años de prisión, mínimo legal este que no se condice con el mínimo de escala penal establecido para el delito de abuso sexual con acceso carnal agravado, normado por el art. 119, que establece una mínima de ocho años, dos menos que el mencionado al comienzo de este párrafo. Establecida la relación que precede, podemos decir que el citado artículo, en su cuarto párrafo tipifica conductas que suponen acciones más dañosas para la víctima y una afectación moral (como lo

es el mismo acceso carnal, el riesgo de contraer una enfermedad en la relación y el riesgo de un embarazo no deseado), pero le otorga menor cuantía de pena en comparación a la corrupción de menores agravada.

Este análisis evidencia una clara inconsistencia de valor que se podría solucionar solo bajando el mínino legal previsto para delito de corrupción agravada por amenazas.

Otra alternativa, para salir de este entuerto, sería agravar la figura del "acoso informático", cuando además del contacto con la finalidad de menoscabo sexual, se produzcan amenazas o se produzca la corrupción del menor o su abuso para equiparar las inconsistencias de valor entre las penas y el desvalor social de las conductas.

4) ¿Se puede agravar en delito en las pautas de valoración de los arts. 40 y 41 del Cód. Penal, por la forma de lograr contacto con la víctima, es decir por realizarlo por un medio informático y aplicar la figura del art. 131?

En cuanto a la prohibición de la doble valoración, se ha sostenido que una circunstancia contenida ya en el tipo penal, no puede valorarse doblemente, primero, como un elemento del tipo penal y luego como agravante en la individualización judicial o viceversa.

Ello puede obedecer a que, su consideración ya fue motivo de valoración por parte del legislador a los efectos de la estructuración del respectivo tipo penal y por ende, cometido el delito, por ello, su nueva selección por el juzgador a la hora de acrecentar la sanción importa una vulneración de la prohibición de la doble valoración, comprendida actualmente como un aspecto de la garantía del "*non bis in idem*".

Puede ser posible una doble valoración, si es que se aplica la figura del art. 131 del Cód. Penal, porque según este tipo delictual los únicos medios típicos comisivos del delito son los informáticos, y es por ello que el legislador pena tener contacto con menores, porque esa conducta está comprendida dentro del tipo.

Por otro lado, podría no doble valorarse, en el caso de que el contacto mantenido por medios informáticos, con la finalidad de menoscabar la integridad sexual de los menores constituyera el delito de corrupción de menores, porque los medios informáticos no son los únicos aptos para la comisión de este delito.

f) *El lugar del contacto como un elemento importante para determinar la ley aplicable, y en especial, la jurisdicción que debe intervenir.* Como ya dijimos, bien reza el art. 131, el acto se configura cuando se logra el contacto, por lo que es fundamental la ubicación geográfica de la víctima al momento de recibir el mensaje por el cual se busca menoscabar su integridad sexual para determinar la jurisdicción que deberá intervenir y cuál será la ley aplicable para el caso en concreto.

Establecida esta línea, vale recordar que el art. 1 del Cód. Penal establece: "*Este Código se aplicará:*

1°. Por delitos cometidos o cuyos efectos deban producirse en el territorio de la Nación Argentina, o en los lugares sometidos a su jurisdicción".

Dicho esto, podríamos establecer que si la víctima de "ciber-acoso" encuentra en nuestro país al momento de recibir el mensaje con los fines de menoscabar su

integridad sexual, y así al recibirlo se configurará el contacto y por ende la normativa aplicable sería el Código Penal argentino (art. 1) y la CIDÑ (arts. 3, 16 puntos 1 y 2, 19 puntos 1 y 2) por lo tanto, entiendo que el proceso debería llevarse a cabo conforme el ordenamiento adjetivo del lugar donde la víctima se encontrara situada y donde efectivamente se producen sus efectos los hechos dañosos, contra la integridad sexual de la víctima, según nos indica el artículo citado.

g) *Los problemas de la ley a la luz de las recomendaciones de la AIDP y ciertos principios constitucionales y tratados internacionales suscriptos por Argentina.* Veamos ahora las recomendaciones de la AIDP y comparemos con lo legislado en Argentina.

Las recomendaciones de la AIDP que me interesa puntualizar se pueden sintetizar del siguiente modo:

• Los delitos, en el ámbito de las tecnologías de la información y la comunicación (TIC) y el ciberespacio, deben ser definidos por la ley.

• La ley debe emplear términos que definan la conducta prohibida de la manera más precisa posible.

• Son legítimas las leyes que deciden penalizar actos preparatorios (de ataques a intereses relativos a las TIC y al ciberespacio) siempre que creen un riesgo de causar un daño o peligro concreto a intereses protegidos de otros.

• Cuando se castiguen los actos preparatorios la pena debería ser menor.

• Si un Estado decide criminalizar la conducta de hacerse pasar por personas inexistentes debe limitarse a los actos cometidos con la intención de causar daño.

• Se pone especial énfasis en conductas vinculadas a la pornografía infantil, aunque también en ese caso se establece alguna clase de límite, puntualizando el caso en que se implican niños reales.

La ley argentina ha definido el llamado delito de “grooming”, pero indudablemente lo ha hecho empleando términos que describen la conducta prohibida del modo menos preciso posible. Tal es el adelantamiento y tal la simplificación, que se produce un corrimiento del comienzo de ejecución hacia momentos que, en cualquier otro caso, remiten a una etapa bien temprana de preparación.

Son legítimas las leyes que deciden penalizar actos preparatorios (de ataques a intereses relativos a las TIC y el ciberespacio), siempre que creen riesgo de causar un daño o peligro concreto a intereses protegidos de otros.

Sin discutir aquí si la recomendación se basa en presupuestos correctos desde la lógica que la informa, es posible afirmar: cuanto más alejados del daño o peligro concreto al interés que se pretende proteger estén los actos preparatorios contemplados, menos probabilidades habrá de crear efectivamente un peligro concreto o riesgo de daño para el interés protegido. Al menos, si se comparan los riesgos de un mismo curso delictivo, que progresa hacia la consecución de cierto peligro o daño.

Luego, es claro que la constelación de riesgos prohibidos que derivan de la ley argentina en análisis abarca situaciones que no causan daño ni suponen peligro concreto.

Cuando se castiguen los actos preparatorios la pena debería ser menor. La pena prevista es efectivamente menor que otras muy graves que acompañan delitos contra la integridad sexual legislados en el mismo Título III del Código Penal argentino. No obstante, la recomendación tampoco se cumple en el caso del abuso sexual simple (art. 119), un delito de daño que prevé la misma escala penal cuando se abusa sexualmente de un menor de trece años, sin necesidad de violencia, intimidación o aprovechamiento. De modo que contactar por medio de cualquier tecnología a un menor que cuenta, por ejemplo, con diecisiete años, con el propósito de abusar sexualmente de él (art. 131), tiene la misma respuesta punitiva que si efectivamente, se abusase simplemente de un niño de doce años (art. 119, párr. 1°, Cód. Penal).

Si un Estado decide criminalizar la conducta de hacerse pasar por personas inexistentes debe limitarse a los actos cometidos con la intención de causar daño.

La ley argentina no criminaliza la conducta de hacerse pasar por personas inexistentes, aunque su fórmula contactare indudablemente la abarca, entre muchas otras. Para ese contacto, efectivamente prevé el propósito de causar un daño.

Se pone especial énfasis en conductas vinculadas a la pornografía infantil.

La producción o publicación de imágenes pornográficas en que se exhibieran menores de dieciocho años y la organización de espectáculos en vivo con escenas pornográficas en que participaren dichos menores está sancionada en el art. 128, primer párrafo. Una vez más, la escala penal prevista es la misma que la del art. 131.

Entonces, organizar un espectáculo con escenas pornográficas en vivo con menores (art. 128, párr. 1°) tiene la misma respuesta punitiva dentro de la ley penal argentina que contactar al mismo menor por medio de cualquier tecnología con el propósito de abusar sexualmente de él (art. 131).

Estas observaciones permiten comprender, quizá, los motivos de la menor respuesta punitiva que propuso la Cámara Baja al Proyecto de ley, luego sancionado.

El principio de proporcionalidad de las penas veda el ejercicio del poder punitivo realizado de modo irracional, tal como sería una respuesta groseramente desproporcional al mal provocado.

De allí que es necesario establecer jerarquías de afectación y establecer mínima coherencia entre la magnitud de penas que se asocian a cada conflicto criminal. Algo que, evidentemente, no cumple la ley argentina.

h) *La ausencia de adecuación de todo el título de delitos contra la integridad sexual a la legislación de violencia contra la mujer.* También no parece razonable atento a la legislación en materia de violencia de genero incorporada por nuestro país por la ley 24.632, que incorpora la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer, “Convención de Belem do Pará”, determina en su art. 2 que: “Se entenderá que violencia contra la mujer incluye la violencia física, sexual y psicológica: *a*) que tenga lugar dentro de la familia o unidad doméstica o en cualquier otra relación interpersonal, ya sea que el agresor comparta o haya compartido el mismo domicilio que la mujer, y que comprende, entre otros, violación, maltrato y abuso sexual; *b*) que tenga lugar en la comunidad y sea perpetrada por cualquier persona y que comprende, entre otros, violación, abuso sexual, tortura, trata de personas, prostitución forzada, secuestro y acoso sexual en

el lugar de trabajo, así como en instituciones educativas, establecimientos de salud o cualquier otro lugar; *c*) la que sea perpetrada o tolerada por el Estado o sus agentes, dondequiera que ocurra".

En ese sentido la ley 26.485 "De protección integral para prevenir, sancionar y erradicar la violencia contra las mujeres en los ámbitos en que desarrollen sus relaciones interpersonales" sancionada el 11 de marzo de 2009, en su art. 4 determina que: "Se entiende por violencia contra las mujeres toda conducta, acción u omisión, que de manera directa o indirecta, tanto en el ámbito público como en el privado, basada en una relación desigual de poder, afecte su vida, libertad, dignidad, integridad física, psicológica, sexual, económica o patrimonial, como así también su seguridad personal. Quedan comprendidas las perpetradas desde el Estado o por sus agentes. Se considera violencia indirecta, a los efectos de la presente ley, toda conducta, acción omisión, disposición, criterio o práctica discriminatoria que ponga a la mujer en desventaja con respecto al varón".

En cuanto a los tipos de violencia posible contra la mujer establece en el ámbito sexual determina: art. 4.3. Sexual. Cualquier acción que implique la vulneración en todas sus formas, con o sin acceso genital, del derecho de la mujer de decidir voluntariamente acerca de su vida sexual o reproductiva a través de amenazas, coerción, uso de la fuerza o intimidación, incluyendo la violación dentro del matrimonio o de otras relaciones vinculares o de parentesco, exista o no convivencia, así como la prostitución forzada, explotación, esclavitud, acoso, abuso sexual y trata de mujeres.

Atento a que violencia contra la mujeres, incluye la violencia de tipo sexual, esta característica de violencia tendría que ser agravante, no solo en esta figura que incluye a las niñas víctimas de "ciber-acoso", sino que esta característica debería incluir un tipo agravante en todos los delitos sexuales, cuando éstos se produzcan como consecuencia de ser mujeres o por odio o desprecio hacia el género femenino; ausencia que debería ser remediada en una eventual reforma del Código Penal, para evitar condenas en tribunales internacionales, por no adecuar nuestra legislación interna a los compromisos internacionales contraídos.

En el mismo sentido, Buompadre coincide con esta idea en relación de que este tipo de violencia sexual, cometida por medios informáticos, debería contener algún tipo de agravante específico, cuando la agresión sea por la sola condición de ser mujer o por odio hacia su género[18].

7. Acciones delictivas no tipificadas

En la actualidad existen acciones que si bien se las conoce y se las evalúa como acciones delictivas, no se encuentran adecuadamente legisladas o tipificadas, estas acciones son capaces de provocar daños a las personas o sus bienes, centrándome especialmente en el análisis de tres modalidades delictivas, el llamado "*phishing*", las técnicas de *typosquatting* y la porno-venganza y el "*camfecting*"; las explicaré y

[18] Buompadre, Jorge E., *Violencia de género en la era digital*, Bs. As., Astrea, 2016, p. 35.

describiré, para luego proponer en forma sucinta algunas posibles soluciones legales, indicando como en otros países han legislado y penado estas conductas.

a. El "phishing"

Se conoce como *phishing* a la suplantación de identidad, al modelo de abuso informático, que persigue apropiarse de datos confidenciales de los usuarios para, en base a ellos, conseguir menoscabar patrimonios ajenos. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. Este tipo de fraude se efectúa habitualmente a través de mensajes de correo electrónico o de ventanas emergentes. El cibercriminal, conocido como *phisher*, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.

El término *phishing* proviene de la palabra inglesa *fishing* (pesca), haciendo alusión al intento de hacer que los usuarios "muerdan el anzuelo"; también se ha usado el término *phishing* como la contracción de *password harvesting fishing* (cosecha y pesca de contraseñas).

Los intentos más recientes de *phishing*, han tomado como objetivo a clientes de bancos y servicios de pago en línea. Puede verse como los denominados "*phishers*" envían de forma indiscriminada correos electrónicos falsos, impostando ser una entidad financiera, con la esperanza de encontrar a un cliente de dicho banco o servicio y así llevar a cabo esta acción. Estudios recientes muestran que los "*phishers*" en un principio son capaces de establecer con qué banco una posible víctima tiene relación, y de ese modo enviar un correo electrónico, falseado apropiadamente, a la posible víctima. En términos generales, esta variante hacia objetivos específicos en el *phishing* se ha denominado *spear phishing* (literalmente pesca con arpón). Los sitios de Internet con fines sociales también se han convertido en objetivos para los "*phishers*", dado que mucha de la información provista en estos sitios puede ser utilizada en el robo de identidad. Algunos experimentos han otorgado una tasa de éxito de un 90% en ataques *phishing* en redes sociales. A finales de 2006 un gusano informático se apropió de algunas páginas del sitio web MySpace logrando redireccionar los enlaces de modo que apuntaran a una página web diseñada para robar información de ingreso de los usuarios.

La mayoría de los métodos de *phishing* utilizan la manipulación en el diseño del correo electrónico para lograr que un enlace parezca una ruta legítima de la organización por la cual se hace pasar el impostor. Otros intentos de *phishing* utilizan comandos en JavaScript para alterar la barra de direcciones. Esto se hace poniendo una imagen de la URL de la entidad legítima sobre la barra de direcciones, o cerrando la barra de direcciones original y abriendo una nueva que contiene la URL ilegítima.

En otro método popular de *phishing*, el atacante utiliza contra la víctima el propio código de programa del banco o servicio por el cual se hace pasar. Este tipo de ataque resulta particularmente problemático, ya que dirige al usuario a iniciar sesión en la propia página del banco o servicio, donde la URL y los certificados de seguridad parecen correctos. En este método de ataque (conocido como *Cross Site Scripting*)

los usuarios reciben un mensaje diciendo que tienen que “verificar” sus cuentas, seguido por un enlace que parece la página web auténtica; en realidad, el enlace está modificado para realizar este ataque, además es muy difícil de detectar si no se tienen los conocimientos necesarios.

Actualmente empresas ficticias intentan reclutar tele-trabajadores por medio de correo electrónico, chats, irc y otros medios, ofreciéndoles no sólo trabajar desde casa sino también otros jugosos beneficios. Aquellas personas que aceptan la oferta se convierten automáticamente en víctimas que incurren en un grave delito sin saberlo: el blanqueo de dinero obtenido a través del acto fraudulento de *phishing*, participando con engaño de una empresa delictiva, siendo manipulado por verdaderos piratas informáticos, ya sea mediante el envío global de millones de correos electrónicos bajo la apariencia de entidades bancarias, solicitando las claves de la cuenta bancaria (*phishing*) o con ataques específicos. Dichos movimientos consisten en que los estafadores comiencen a retirar sumas importantes de dinero, las cuales son transmitidas a las cuentas de los intermediarios (muleros) para que luego éstos últimos realicen el traspaso a las cuentas de los estafadores, llevándose éstos las cantidades de dinero y aquéllos –los intermediarios– el porcentaje de la comisión.

En el mundo existen varias técnicas diferentes para combatir el *phishing*, incluyendo la legislación y la creación de tecnologías específicas que tienen como objetivo evitarlo.

Una estrategia para combatir el *phishing* adoptada por algunas empresas es la de entrenar a los empleados de modo que puedan reconocer posibles ataques. Por ejemplo, si a un usuario se lo contacta mediante un correo electrónico y se le hace mención sobre la necesidad de “verificar” una cuenta electrónica puede o bien contactar con la compañía que supuestamente envía el mensaje, o bien escribir la dirección web de un sitio web seguro en la barra de direcciones de su navegador para evitar usar el enlace que aparece en el mensaje sospechoso de *phishing*.

Hay varios programas informáticos anti-phishing disponibles. La mayoría de estos programas trabajan identificando contenidos *phishing* en sitios web y correos electrónicos; algunos software anti-phishing pueden por ejemplo, integrarse con los navegadores web y clientes de correo electrónico como una barra de herramientas que muestra el dominio real del sitio visitado. Los filtros de spam también ayudan a proteger a los usuarios de los *phishers*, ya que reducen el número de correos electrónicos relacionados con el *phishing* recibidos por el usuario.

Muchas organizaciones, como por ejemplo los bancos informáticos de nuestro país, han introducido la característica denominada “pregunta secreta”, en la que se pregunta información que sólo debe ser conocida por el usuario y la organización. Las páginas de Internet también han añadido herramientas de verificación que permite a los usuarios ver imágenes secretas que los usuarios seleccionan por adelantado; sí estas imágenes no aparecen, entonces el sitio no es legítimo. Estas y otras formas de autentificación mutua continúan siendo susceptibles de ataques, como el sufrido por el banco escandinavo Nordea a finales de 2005.

El 26 de enero de 2004, la FTC (Federal Trade Commission, la Comisión Federal de Comercio) de Estados Unidos llevó a juicio el primer caso contra un *phisher* sospechoso. El acusado, un adolescente de California, supuestamente creó y utilizó

una página web con un diseño que aparentaba ser la página de América Online para poder robar números de tarjetas de crédito.

Tanto Europa como Brasil siguieron la práctica de los Estados Unidos, rastreando y arrestando a presuntos *phishers*. A finales de marzo de 2005, un hombre estonio de 24 años fue arrestado utilizando una *backdoor*, a partir de que las víctimas visitaron su sitio web falso, en el que incluía un *keylogger* (virus que graba registro de todo lo que se escribe con el teclado de la PC en un archivo de texto) que le permitía monitorear lo que los usuarios tecleaban. Del mismo modo, las autoridades arrestaron al denominado *phisher kingpin*, Valdir Paulo de Almeida, líder de una de las más grandes redes de *phishing* que en dos años había robado entre $18 a $37 millones de dólares estadounidenses. En junio del 2005 las autoridades del Reino Unido arrestaron a dos hombres por la práctica del *phishing*, en un caso conectado a la denominada "Operation Firewall" del Servicio Secreto de los Estados Unidos, que buscaba sitios web notorios que practicaban el *phishing*.

Diversos países se han ocupado de los temas del fraude y las estafas a través de Internet. Producto de esto es el Convenio de Cibercriminalidad de Budapest. Además, de manera individual, otros países han dedicado esfuerzos legislativos para castigar estas acciones, incluyendo el *phishing* como delito en sus legislaciones, por ejemplo, mientras que en otros es materia pendiente o bajo estudio.

En Chile, aunque no existe un tipo penal en el Código que sancione al *phishing*, los tribunales recurren a la figura de la estafa tradicional para castigar estas conductas.

En los Estados Unidos, el senador Patrick Leahy introdujo la ley anti-phishing el 1 de marzo de 2005. Esta ley federal de anti-phishing establecía que aquellos criminales que crearan páginas web falsas o enviaran spam a cuentas de correo electrónico con la intención de estafar a los usuarios podrían recibir una multa de hasta $250,000 USD y penas de cárcel por un término de hasta cinco años.

Algunos Estados tienen leyes que tratan las prácticas fraudulentas o engañosas o el robo de identidad y que también podría aplicarse a los delitos de *phishing*.

En nuestro país si bien como lo hemos mencionado más arriba el art. 173, inc. 16 del Cód. Penal, castiga la estafa informática incluyendo al catálogo de lo ilícito las conductas típicas de defraudación a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

De lo dicho puede interpretarse que la inclusión del autor del delito de *phishing* en el presente artículo claudica, ya que el que solo pesca el dato para obtener la información o utilizarla para venderla, no realiza la maniobra de defraudación por lo que no podrá ser el autor, pero si considerado como partícipe necesario, secundario o instigador.

Otra dificultad que plantea esta modalidad, como lo dijimos más arriba, es que los piratas informáticos no realizan la maniobra de manera individual, de forma solitaria, si no que utilizan a terceros que subcontratan de manera lícita, para que realice el captado de las claves, desconociendo las maniobras de las que están participando y su finalidad delictiva.

Sería necesario adecuar la legislación creando un tipo penal autónomo o vinculándolo con la estafa. Se puede crear un tipo autónomo que castigue la maniobra del *phishing* o robo de identidad en la red, captándola en toda su dimensión y no dejando impune ningún tramo del delito, que tendrá que contener como elemento típico sin lugar a dudas el conocimiento real de quien pesca los datos personales para eventualmente generar un detrimento patrimonial.

Otro tipo de fraude similar es el del *vishing*, que persigue el mismo fin que el *phishing*, la obtención de datos confidenciales de usuarios, pero a través de un medio distinto, la telefonía IP. Los ataques de *vishing* se suelen producir siguiendo dos esquemas:

- Envío de correos electrónicos, en los que se alerta a los usuarios sobre algún tema relacionado con sus cuentas bancarias, con el fin de que estos llamen al número de teléfono gratuito que se les facilita.
- Utilización de un programa que realice llamadas automáticas a números de teléfono de una zona determinada.

En ambos casos, cuando se logra contactar telefónicamente con el usuario, un mensaje automático le solicita el número de cuenta, contraseña, código de seguridad, etcétera.

b. El "typosquatting"

Esta maniobra es un tipo de amenaza cibernética que puede poner en serio riesgo a nuestro ordenador, hace referencia a la probabilidad de que un usuario abra una página diferente a la que se pensaba visitar, al teclear erróneamente una dirección web. Es por eso que este tipo de ciberataque también se les llama Url Hijacking (secuestro de url). Los cibercriminales que lo utilizan se encargan de registrar direcciones derivadas del nombre de algún sitio famoso en Internet (Yahoo, Google o Netflix por ejemplo), pero que contiene evidentes errores de ortografía o tipeo (www.tahoo.com, para continuar con el ejemplo).

Esta técnica supone al estudio, por parte de los atacantes, los errores cometidos de manera más común por los usuarios al escribir direcciones web en su navegador. Una vez descubiertas y registradas las direcciones con más probabilidades de ser accedidas a través de un error, los *cibersquatters* cargan en los sitios malintencionados material peligroso para la PC, usualmente *ransomware*.

También se conoce a esta maniobra como generación de sitos peligrosos con técnicas a través de las cuales los criminales modifican la dirección del sitio web original (al que llamaremos sitio-víctima) una vez generada la información, el contenido cargado suele ser similar en apariencia al del sitio original (sitio-víctima): tanto los logos como la organización de la plantilla y el framework del sitio son, en muchos casos, copiados al extremo (lo cual supone, en sí, un segundo crimen o ilícito).

Las técnicas más utilizadas suelen ser el aprovechamiento de los errores de dicción en un sitio. Esto se aplica especialmente a sitios cuyo nombre es de origen

extranjero o se supone una onomatopeya o alguna aliteración. Por ejemplo, www.flicker.com en lugar de www.flickr.com.

En este ejemplo de ataque, los cibercriminales decidieron incluir un vínculo de contacto y uno de sindicación a un newsletter que, en cualquiera de los casos, nos exige un correo electrónico. Esta dirección será utilizada, según he comprobado, para enviar gusanos y correos de *phishing*.

La segunda de las técnicas más comunes es la basada en los errores de tipeo que cometen los usuarios involuntariamente. Por ejemplo, si equivocamos www.calrin.com y lo escribimos en lugar de www.clarin.com puede que, de ser un error común, algún cibercriminal lo aproveche para crear el sitio e insertar contenido dañoso para nuestro ordenador. Son muchas las empresas que, alertadas de estas técnicas, registran y redireccionan estas páginas para evitar que sean utilizadas de mala manera. Este es el caso de Google, que compró www.gogle.com y redirigió todo su tráfico a los sitios regionales oficiales de la página.

También se puede dar esta situación en una variación en el armado de la frase en los sitios web cuyos nombres aceptan plurales o están conformados por frases. La peligrosa página www.argentinas.com se basa en una variante de la página www.argentina.com. En ella podemos leer que el sitio se encuentra en proceso de rediseño y encontraremos una dirección de correo que, de ser usada, confirmara a los cibercriminales que nuestro e-mail es válido. Luego recibiremos miles de correos spam a diario.

Hay otras técnicas de *typosquatting* basadas en errores universales de escritura, que son utilizadas a diario por cibercriminales y otros tipos de atacantes que, en algunos casos, son simples comerciantes que quieren lucrar nuestros errores.

Al entrar en un sitio puesto en marcha por un cibercriminal que haya utilizado la técnica de *typosquatting* seremos, en la mayoría de los casos una víctima de uno de los ataque de la *ransomware*, sin embargo, en algunas ocasiones las consecuencias son otras: podemos encontrar un ataque de *phishing* que pretende robar nuestras claves, formularios que pidan nuestro correo electrónico a cambio de información para enviarnos spam e, incluso, publicidades que intentan salvajemente instalar adware y spyware en el equipo.

Las observaciones efectuadas para el *psihing*, son las mismas que efectuare con el *typosquatting* en cuanto en la legislación penal aplicable y las reformas que se estiman necesarias para adecuar las nuevas modalidades delictivas ya que muchas veces esta técnica le abre la puerta a los ciber-delincuentes para pescar información claves o contraseñas para efectuar las estafas informáticas y de esa forma quedarían conductas dañosas para nuestra sociedad impunes.

c. La distribución no consentida de imágenes de contenido sexual o íntimas

Como primera aproximación podríamos decir que la comúnmente llamada “distribución no consentida de imágenes de contenido sexual y/o íntimas” hace referencia a la publicación ilegítima de imágenes o videos de contenido sexual o erótico explícito en Internet o en cualquier medio masivo de comunicación sin el consentimiento del individuo que aparece representado.

Lo que suele suceder con este tipo de fenómenos, luego de que alguien publique cierto material con contenido erótico, ya sea un video o una foto, y aunque la vía judicial haya ordenado el bloqueo del encale web que contiene ese material mencionado, o bien, se desindexen de los buscadores los resultados referentes a este material sexual de la búsqueda, no resulta ser una solución definitiva a la cuestión ya que siempre existe la posibilidad de que dicho material sea nuevamente alojado en algún sitio web, ya sea por el sujeto que cometió el acto en la primera oportunidad o por terceros, que al descargar la información la retienen para sí y posteriormente deciden subirla y compartirla en Internet, ya que el control y la limitación que se puede llevar a cabo afecta solo a lo que esté ya depositado en la web, quedando por fuera el contenido ya descargado por los usuarios y alojados en su ordenador personal.

Por lo tanto, la posibilidad de que eso ocurra y que la pesadilla para la víctima vuelva a ser realidad, es técnicamente incontrolable, por ello es necesario que esa conducta sea tipificada e incorporada al Código Penal argentino como delito autónomo.

La distribución no consentida de imágenes de contenido sexual y/o íntimas, es típicamente distribuida en los medios masivos como Internet, tanto por exparejas como por hackers con acceso no autorizado a imágenes y grabaciones íntimas de la víctima. Muchas de las fotografías son tomadas por las propias personas que aparecen en ella, más conocidas como “selfies”.

Las imágenes suelen ir acompañados de información personal, incluyendo el nombre completo del individuo en la foto o video, enlaces a Facebook, los perfiles y las direcciones de las redes sociales.

Este tipo de acción, al someter a la víctima en una situación de exposición no consentida de su sexualidad, se considera como violencia sexual, aunque no sea física, sino psicológica. Los casos reportados muestran consecuencias que pueden llegar a ser muy graves para la víctima, con perjuicios en su derecho al honor y trastornos serios en su vida familiar y laboral. La víctima se entera sorpresivamente del hecho, cuando el material ya está cargado en Internet, momento en que se puede ubicar el inicio del trauma y un escarnio social que en muchos casos de personajes conocidos tienen un doble escarnio el mediático.

La distribución no consentida de imágenes de contenido sexual y/o íntimas en el derecho comparado.

En Estados Unidos de América, en 2012 había nueve Estados que cuentan con leyes aplicables en situaciones de difusión de imágenes íntimas no consensuadas, estos Estados son: Alaska, Arizona, California, Colorado, Georgia, Maryland, Nueva Jersey, Idaho, Utah, Virginia y Wisconsin. Para 2016 el número de Estados con leyes especiales de “*revenge porn*” había subido a 26 Estados.

Entre estos, destacamos la ley en Nueva Jersey que prohíbe a cualquier persona la distribución y venta de fotografías y videos con contenido sexual explícito sabiendo que no posee con la licencia o el derecho de hacerlo sin la previa autorización de los individuos. Esta ley fue utilizada para enjuiciar al estudiante de la Universidad de Rutgers, Dharun Ravi quien distribuyó las imágenes captadas con una cámara web cuando su compañero Tyler Clementi mantenía actividad sexual y por lo cual el joven Clementi posteriormente decidió suicidarse. Por otro lado, cabe mencionar que esta

ley también fue utilizada para llevar a juicio a otros hombres quienes presuntamente distribuían material pornográfico de sus ex novias.

La ley de California la cual fue aprobada en octubre del año 2013, prohíbe la comercialización de fotografías o videos íntimos que tengan como finalidad el causar determinado tipo de angustia emocional de tipo grave en algún individuo. Esta ley protege a aquellas imágenes que han sido tomadas consensualmente solamente en el caso de que la persona que distribuye dichas imágenes es también fotografiado, lo que ha sido muy criticado por los defensores de las víctimas.

Esta práctica será delito siempre que las imágenes se hayan publicado en Internet para "causar daño emocional y angustia", sin el consentimiento del afectado, y tras ser tomadas "en circunstancias en las que la otra persona tendría razones para esperar que no saldrían del ámbito privado", estipula la norma. La intención legisladora se suma a la pretensión de resolver problemas culturales con el Código Penal.

Los derechos a la intimidad, el honor o la propia imagen están reconocidos en la inmensa mayoría de países del mundo como derechos fundamentales de la persona y, por tanto, su vulneración es recogida en las legislaciones nacionales y perseguidas por los tribunales de justicia.

Aun así, la proliferación de nuevas tecnologías de la comunicación y la información ha hecho necesario el desarrollo de leyes específicas que hagan frente a determinados actos muy concretos: es el caso del llamado "porno de venganza".

También Japón ha puesto manos a la obra a partir de una legislación específica para este tipo de delito que ya ha permitido identificar 110 webs que albergaban y explotaban este tipo de contenidos donde el 99% de víctimas eran mujeres. La nueva ley nipona castiga estos actos delictivos con penas de prisión y multas obligando además a los proveedores de Internet a eliminar todos estos contenidos.

Dinamarca presentó en el mes de febrero medidas para limitar la "porno venganza", castigando esa práctica con dos años de cárcel. "Las fotos de examantes son puestas en línea", subrayó el Primer ministro danés Lars Løkke Rasmussen en Facebook. "Las víctimas quedan afectadas (por estas prácticas) durante todas sus vidas", agregó. En Dinamarca, 17% de los hombres y 13% de las mujeres de 15 a 25 años tienen fotos de ellos desnudos publicados en Internet, según cifras dadas por el gobierno. Ningún dato indica si esas fotos fueron publicadas en la red con o sin su acuerdo. El proyecto gubernamental, presentado por los ministros de Justicia, de la Paridad y de la Educación, busca informar a las víctimas del procedimiento a seguir cuando presentan demandas.

La distribución no consentida de imágenes de contenido sexual y/o íntimas, en nuestro país.

El Senado de la Nación aprobó el proyecto de ley de la senadora Marina Riofrio que modifica el Código Penal incorporando "penas de seis meses a cuatro años de prisión a quien hallándose en posesión de imágenes de desnudez total o parcial y/o videos de contenido sexual o erótico de una o más personas, las hiciere pública o difundiere por medio de comunicaciones electrónicas, telecomunicaciones, o cualquier otro medio o tecnología de transmisión de datos".

Ello, sin el expreso consentimiento de las personas implicadas, contemplada la posibilidad de que incluso el registro de las mismas se produjere habiendo existido acuerdo entre las partes involucradas para la obtención de esas imágenes o videos. El proyecto prevé también que la persona condenada será obligada a arbitrar los mecanismos necesarios para retirar de circulación, bloquear, eliminar o suprimir, el material de que se tratare, a su costa y en un plazo a determinar por el juez.

Esta norma complementa la aplicación de otra norma que en el ámbito del derecho privado ya contamos. En este sentido, el Código Civil protege, en su art. 53, el derecho a la imagen, el que establece que para captar o reproducir imágenes de una persona, de cualquier modo que se haga, es necesario su consentimiento. Para estos casos las excepciones son: *a*) que la persona participe en actos públicos; *b*) que exista un interés científico, cultural o educacional y se tomen las precauciones suficientes para evitar un daño; *c*) que se trate del ejercicio regular del derecho de informar sobre acontecimientos de interés general.

También el art. 1770 es contundente respecto a la protección de la vida privada; dice que el que arbitrariamente se entromete en la vida ajena y publica retratos, difunde correspondencia, mortifica a otros en sus costumbres o sentimientos, o perturba de cualquier modo su intimidad, debe ser obligado a cesar en tales actividades y a pagar una indemnización que fijará el juez. Además, a pedido del agraviado puede ordenarse la publicación de la sentencia en un diario. Con esta nueva tipificación estaríamos aplicando una protección del orden punitivo penal al ámbito privado y personal.

Así, se complementa una tendencia nacional y mundial en materia de acciones cometidas por medios electrónicos o redes sociales. De ser aprobado por Diputados se daría respuesta legislativa a una de las cuestiones más acuciantes que hoy afectan la privacidad, voluntad o buena fe. Los casos de hostigamientos y exposición pública e involuntaria de actos privados en Internet son otras de las crueles variables de la violencia de género que en forma silenciosa ocurren en el ámbito virtual con consecuencias en el cuerpo de sus víctimas.

Respecto de las soluciones judiciales a este tipo de cuestiones, por sentencia del Juzgado Nacional de Primera Instancia en lo Civil y Comercial Federal n° 2, con fecha 14 de julio de 2016, hizo lugar a la medida cautelar solicitada por una animadora de programas de televisión y ordenó a dos buscadores de Internet que procedan a la inmediata eliminación y bloqueo de los sitios web de contenido sexual, pornográfico y otras actividades vinculadas al tráfico de sexo, a los que se accede a través de los mencionados motores de búsqueda y en los cuales se encuentran fotografías de la actora trucadas en forma burda y grave.

Se afirmó que la inclusión del nombre y fotografías en los sitios web que refieren sin autorización, constituye un uso indebido del nombre e imagen que su titular tiene derecho a preservar pues hace a su intimidad y tal turbación queda comprendida en la previsión del art. 1071 bis del Cód. Civil que da lugar a la consiguiente reparación. Asimismo considera que el rechazo de la medida solicitada es susceptible de acarrear consecuencias más gravosas para la actora que los eventuales perjuicios que su admisión podría producir a su contraria, pues con relación a esta última tales derivaciones, en la mejor de las hipótesis, aparecen circunscriptas a la esfera

patrimonial, mientras que en el caso de su adversaria pueden comprometer derechos de mayor jerarquía.

Una eventual reforma debería estar estructurada dentro de los siguientes parámetros de política criminal:

- Es necesario crear una figura penal que esté despojada, de todo elemento subjetivo o finalidad de venganza, en hacer públicas o difundir imágenes de desnudez total o parcial y/o videos de contenido sexual o erótico de una o más personas.
- En este estado de las cosas, no debería importar si se hace pública la foto o el video íntimo, si no que sería constitutivo del delito; el efectivo quebrantamiento de la "buena fe o reserva", en la intimidad de los actos de las personas.
- Entendiendo que en estas cuestiones el bien jurídico vulnerado sería una especie "de intimidad compartida", sobre todo si estas imágenes o videos, se hubieran obtenido con acuerdo expreso o tácito entre las partes involucradas para la obtención y producción de las imágenes o videos, que se desean reservar para la esfera de la intimidad personal o de la pareja.

Atento a ello entiendo que este tipo penal debería estar legislado en principio dentro del capítulo de los delitos que afectan la intimidad y la dignidad de la persona humana.

Entiendo, que podría tratarse además de la inclusión de esta figura, como un positivo gesto de política criminal, que se contemple, la posibilidad de además de imponer como una condición accesoria a la pena, que la persona que cometió el delito tenga que arbitrar a su exclusiva costa, los mecanismos necesarios para retirar de circulación, bloquear, eliminar o suprimir, el material de que se tratare y ello es así porque instaura un viento de justicia restaurativa en nuestro sistema penal en el orden de que quien cause un perjuicio, debe procurar "reparar el daño causado en forma integral", principio que desgraciadamente, se ha licuado o debilitado en nuestro ordenamiento jurídico.

d. El "camfecting"

Otro de los delitos que generan gran preocupación en las masas sociales es el denominado "*camfecting*", en el que el criminal infecta el ordenador personal o notebook de la víctima y de forma oculta abusa de la cámara web incorporada, grabándola en todo momento, logrando obtener imágenes de la intimidad de la persona víctima, quien se comporta de forma natural, en un espacio de confianza desconociendo que la cámara web del ordenador se encuentra siendo manipulada por otro sujeto desde otro ordenador en cualquier parte del mundo.

Está claro que esta conducta delictiva puede ser el canal o facilitador para la comisión de otro tipo de delitos comunes o de delitos "típicamente" informáticos, por lo que sería importante dentro de "la política legislativa argentina", incluir este tipo

como una forma de violación al bien jurídico intimidad, que la ley debe proteger y respetar.

También entiendo que esta figura debería estar legislada, también en principio como dijimos con la porno-venganza, dentro del capítulo de los delitos que afectan la intimidad y la dignidad de la persona humana.

8. ¿Qué ocurre en el extranjero?

Durante los últimos años se ha ido perfilando en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los problemas derivados del mal uso que se hace de las computadoras, lo cual ha dado lugar a que, en algunos casos, se modifique el derecho penal de los países.

En un primer término, debe considerarse que en 1983, la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales.

Las posibles implicaciones económicas de la delincuencia informática, su carácter internacional y, a veces, incluso transnacional y el peligro de que la diferente protección jurídico-penal nacional pudiera perjudicar el flujo internacional de información, condujeron en consecuencia a un intercambio de opiniones y de propuestas de solución. Sobre la base de las posturas y de las deliberaciones surgió un análisis y valoración ius-comparativista de los derechos nacionales aplicables así como de las propuestas de reforma. Las conclusiones político-jurídicas desembocaron en una lista de acciones que pudieran ser consideradas por los Estados, por regla general, como merecedoras de pena.

De esta forma, la OCDE en 1986 publicó un informe titulado Delitos de Informática: análisis de la normativa jurídica, en donde se reseñaban las normas legislativas vigentes y las propuestas de reforma en diversos Estados miembros y se recomendaba una lista mínima de ejemplos de uso indebido que, los países podrían prohibir y sancionar en leyes penales (lista mínima), como por ejemplo el fraude y la falsificación informáticos, la alteración de datos y programas de computadora, sabotaje informático, acceso no autorizado, interceptación no autorizada y la reproducción no autorizada de un programa de computadora protegido.

Con objeto de que se finalizara la preparación del informe de la OCDE, el Consejo de Europa inició su propio estudio sobre el tema a fin de elaborar directrices que ayudasen a los sectores legislativos a determinar qué tipo de conducta debía prohibirse en la legislación penal y la forma en que debía conseguirse ese objetivo, teniendo debidamente en cuenta el conflicto de intereses entre las libertades civiles y la necesidad de protección.

La lista mínima preparada por la OCDE se amplió considerablemente, añadiéndose a ella otros tipos de abuso que se estimaba merecían la aplicación de la legislación penal. El Comité, Especial de Expertos sobre Delitos relacionados con el empleo de las computadoras, del Comité Europeo para los problemas de la Delincuencia, examinó esas cuestiones y se ocupó también de otras, como la protección de la esfera personal, las víctimas, las posibilidades de prevención, asuntos

de procedimiento como la investigación y confiscación internacional de bancos de datos y la cooperación internacional en la investigación y represión del delito informático.

Una vez desarrollado todo este proceso de elaboración de las normas en el ámbito continental, el Consejo de Europa aprobó la recomendación R(89)9 sobre delitos informáticos, en la que se "recomienda a los gobiernos de los Estados miembros que tengan en cuenta cuando revisen su legislación o creen una nueva, el informe sobre la delincuencia relacionada con las computadoras... y en particular las directrices para los legisladores nacionales". Esta recomendación fue adoptada por el Comité de Ministros del Consejo de Europa el 13 de septiembre de 1989.

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

Por otra parte, en el ámbito de organizaciones intergubernamentales de carácter universal, debe destacarse que en el seno de la Organización de las Naciones Unidas (ONU), en el marco del Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en 1990 en la Habana, Cuba, se dijo que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos.

Además, la injerencia transnacional en los sistemas de proceso de datos de otros países, había traído la atención de todo el mundo. Por tal motivo, si bien el problema principal –hasta ese entonces– era la reproducción y la difusión no autorizada de programas informáticos y el uso indebido de los cajeros automáticos, no se habían difundido otras formas de delitos informáticos, por lo que era necesario adoptar medidas preventivas para evitar su aumento.

En general, se supuso que habría un gran número de casos de delitos informáticos no registrados.

Partiendo del estudio comparativo de las medidas que se han adoptado a escala internacional para atender esta problemática, deben señalarse los problemas que enfrenta la cooperación internacional en la esfera de los delitos informáticos y el derecho penal, a saber: la falta de consenso sobre lo que son los delitos informáticos, falta de definición jurídica de la conducta delictiva, falta de conocimientos técnicos por parte de quienes hacen cumplir la ley, dificultades de carácter procesal, falta de armonización para investigaciones nacionales de delitos informáticos. Adicionalmente, la ausencia de la equiparación de estos delitos en los tratados internacionales de extradición.

Al respecto se debe considerar lo que dice el Manual de la Naciones Unidas para la Prevención y Control de Delitos Informáticos el cual señala que, cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada. Asimismo, la ONU resume de la siguiente manera a los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

- Falta de acuerdos globales acerca de qué tipo de conductas deben constituir delitos informáticos.
- Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.
- Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.
- No armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.
- Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.
- Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

Internet y las redes y tecnologías relacionadas se han convertido en instrumentos indispensables para los Estados miembros de la OEA. Internet ha impulsado un gran crecimiento en la economía mundial y ha aumentado la eficacia, productividad y creatividad en todo el hemisferio. Individuos, empresas y gobiernos cada vez utilizan más las redes de información que integran la Internet para hacer negocios; organizar y planificar actividades personales, empresariales y gubernamentales; transmitir comunicaciones; y realizar investigaciones. Asimismo, en la Tercera Cumbre de las Américas, en la ciudad de Quebec, Canadá, en 2001, nuestros líderes se comprometieron a seguir aumento la conectividad en las Américas.

Lamentablemente, la Internet también ha generado nuevas amenazas que ponen en peligro a toda la comunidad mundial de usuarios de Internet. La información que transita por Internet puede ser malversada y manipulada para invadir la privacidad de los usuarios y defraudar a los negocios. La destrucción de los datos que residen en las computadoras conectadas por Internet puede obstaculizar las funciones del gobierno e interrumpir el servicio público de telecomunicaciones y otras infraestructuras críticas.

Estas amenazas a nuestros ciudadanos, economías y servicios esenciales, tales como las redes de electricidad, aeropuertos o suministro de agua, no pueden ser abordadas por un solo gobierno ni tampoco pueden combatirse utilizando una sola disciplina o práctica. Como reconoce la Asamblea General en la resolución AG/RES. 1939 (XXXIII-O/03) (Desarrollo de una Estrategia Interamericana para Combatir las Amenazas a la Seguridad Cibernética), es necesario desarrollar una estrategia integral para la protección de las infraestructuras de información que adopte un enfoque integral, internacional y multidisciplinario.

La OEA está comprometida con el desarrollo e implementación de esta estrategia de seguridad cibernética y en respaldo a esto, celebró una Conferencia sobre Seguridad Cibernética (Buenos Aires, Argentina, del 28 al 29 de julio de 2003) que demostró la gravedad de las amenazas a la seguridad cibernética para la seguridad de los sistemas de información esenciales, las infraestructuras esenciales y las economías en todo el mundo, y que una acción eficaz para abordar este

problema debe contar con la cooperación intersectorial y la coordinación entre una amplia gama de entidades gubernamentales y no gubernamentales.

La Estrategia Interamericana Integral de Seguridad Cibernética se basa en los esfuerzos y conocimientos especializados del Comité Interamericano contra el Terrorismo (CICTE), la Comisión Interamericana de Telecomunicaciones (CITEL), y la Reunión de Ministros de Justicia o Ministros o Procuradores Generales de las Américas (REMJA). La Estrategia reconoce la necesidad de que todos los participantes en las redes y sistemas de información sean conscientes de sus funciones y responsabilidades con respecto a la seguridad a fin de crear una cultura de seguridad cibernética.

Se debe tomar en cuenta de igual forma lo manifestado en la AG/RES. 2137 (XXXV-O/05), aprobada en la cuarta sesión plenaria, celebrada el 7 de junio de 2005, en donde se reafirma que el terrorismo, cualquiera sea su origen o motivación, no tiene justificación alguna y que, de conformidad con la Declaración de Puerto España, adoptada por los Estados miembros en el quinto período ordinario de sesiones del CICTE, el terrorismo constituye una grave amenaza a la paz y la seguridad internacionales, socava los esfuerzos continuos que fomentan la estabilidad, prosperidad y equidad en los países de la región, y viola los valores y principios democráticos consagrados en la Carta de la OEA, la Carta Democrática Interamericana y otros instrumentos regionales e internacionales.

9. Glosario de palabras útiles

- *Cookies*. Pequeños archivos que algunos sitios web guardan en la computadora del usuario. Almacenan información como nombre de usuario o datos de registro, entre otros. Si se habilita una cookie de un sitio web al que se accede a menudo, esta recuerda información que hará la próxima visita a esa página, un poco más fácil e incluso más rápida.

- *Criptografía*. Procedimiento que permite a un emisor ocultar el contenido de un mensaje, de modo que solo personas en posesión de determinada clave puedan leerlo.

- *Cloud* (nube). Término que hace referencia al almacenamiento, procesamiento, transmisión y análisis de información que se ubican en nodos de Internet (datacenters), de la red mundial, y que podrán ser accesibles desde cualquier computadora o dispositivo con conexión a Internet.

- *DNS* (sistema de nombre de dominio). Servidor cuya tarea es traducir nombres de dominio a direcciones IP, por ejemplo: www.google.com a un código que entienden las computadoras.

- *Domain name* (nombre de dominio). Nombre legible o alias de Internet que las computadoras traducen a una dirección de IP (Internet Protocol) para poder determinar en una red.

- *Encriptación*. Cifrado. Tratamiento de un conjunto de datos, contenidos o no en un paquete, a fin de impedir que nadie, excepto su destinatario pueda leerlos.

- *Exploits o programas intrusos*. Técnicas que aprovechan las vulnerabilidades del software y que pueden utilizarse para evadir seguridad o atacar un equipo en la red.

- *Firewall*. Dispositivo o conjunto de dispositivos configurados para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

- *Firma digital*. Información cifrada que identifica al autor de un documento electrónico y autentica su identidad.

- *Host*. Computadora conectada a una red, que provee y utiliza servicios de ella. Los usuarios deben utilizar hosts para tener acceso a la red.

- *HTTP* (protocolo de transferencia de hipertexto). Protocolo de comunicación que permite la transferencia de archivos (textos, imágenes gráficas, sonido, video y otros archivos multimedia) en la World Wide Web. El acceso a las páginas web es mayoritariamente a través de este protocolo.

10. Conclusión

Dados los tiempos que corren es necesario hablar de una nueva forma de relacionarnos y comunicarnos, la que podemos llamar como “la sociedad de la comunicación”; en esta nueva sociedad, nos encontramos con actores que consumen y producen nuevas formas de relacionarse y al mismo tiempo, en este contexto, estas tendencias sociales impactan sin dudas en tres aspectos de nuestra vida:

- En la criminalidad como un fenómeno social inevitable.

- En la visibilización e investigación de la criminalidad de los delitos informáticos o cometidos con objetos y medios informáticos.

- Y finalmente esta sociedad impacta de lleno en el seno de nuestra familia y en las relaciones sociales y en la vida y tranquilidad de nuestros niños.

Digo que impacta en la criminalidad porque, sin dudas las redes sociales pueden ser utilizadas para un uso personal y privado, pero se debe tener en cuenta que todo lo que se publique quedará registrado hasta la posteridad y ello, sin dudas, supone un riesgo a los bienes jurídicamente protegidos, como lo son la vida, la propiedad, la intimidad, la libertad, la indemnidad sexual, etc.; en este ámbito es donde el “cibercrimen”, se monta y se camufla sobre la idea misma de la sociedad cibernética y le genera consecuencias directas en su tejido social. De allí nace nuestro deber como una sociedad adulta y responsable que consiste en remediar ese daño, por la vía del derecho con la finalidad de lograr la deseada paz social.

Este fenómeno también genera una mayor visualización en la sociedad de la información, porque como hemos dicho; la investigación de los delitos informáticos se asemeja a una moneda de dos caras, donde uno de sus lados, parece indicar en la mayoría de los actores sociales; que se tiene la sensación que las actividades criminales realizadas por medios informáticos garantizan una especie de "impunidad", de los acechadores o de los delincuentes que utilizan los medios informáticos, donde se cobijan, esconden, parapetan y digitan sus crímenes en un lugar común donde todos transitamos, desde "la web".

Otro aspecto, lado de la moneda, es que posibilita y genera, que si se realiza una buena y seria investigación, que se garantiza con el acopio de prueba objetivable, para lograr el descubrimiento de los crímenes colectando las marcas y las evidencias palpables, que evidenciaran y posibilitaran la persecución judicial de este tipo de delitos.

Desde lo social este fenómeno criminal nos confunde y aterra; porque que como dice Kukso "Más que un ardid de ilusionistas e imitadores de David Copperfield, la idea de la invisibilidad tiene raíces profundas en la cultura occidental. De *La Ilíada* de Homero y *La República* de Platón al cristianismo primitivo, la hechicería y el folklore medieval, pasando por las hermandades invisibles, las sesiones de linterna mágica, la fotografía de hadas, el ilusionismo victoriano, *El hombre invisible* de H. G. Wells, *El Hobbit* de Tolkien y la serie de Harry Potter, el erotismo de lo invisible permea la historia como secreto, como poder maravilloso o desafío moral. Es un sueño tan antiguo como el de volar –escribe el inglés Philip Ball en su fascinante *El peligroso encanto de lo invisible* (Turner)–. La invisibilidad brinda acceso a sitios liminales, matizados de deseo, fascinación y posibilidad. Nos transforma y nos traslada a otro reino"[19].

En esa creencia las redes sociales extienden silenciosamente una cadena que se infiltra bajo nuestra piel: imponen la obligación de estar permanentemente ahí, conectados, disponibles, con lo bueno y lo malo de nuestro ser. Tenemos la idea de una sociedad que se comunica en forma ilimitada y estar on-line, se volvió un certificado de control.

Según el ya citado Kukso, "hay que tuitear, opinar de todo aunque no tengamos argumentos, 'whatsappear', 'instagramear' y mostrar cuán maravillosa es nuestra vida" (editada). Es lo que varios filósofos y sociólogos llaman la "coacción de la comunicación".

El notable autor coreano Byung-Chul Han nos dice al respecto "El smartphone no sólo es un eficiente aparato de vigilancia, sino también un confesionario móvil. Facebook es nuestra iglesia global. La hipercomunicación digital destruye el silencio que necesita el alma para reflexionar y para ser ella misma"[20].

Nuestros niños de hoy, son sin dudas, el futuro del mañana, y es un dato alarmante que según el premiado documental de Delaney Ruston, que muestra la trastienda de la vida familiar, en la que un niño promedio pasa seis horas y media por

[19] Kukso, Federico, *Apología de la desconexión*, "Diario La Nación", 15/1/17.

[20] Han, Byung-Chul, *La sociedad de la transparencia*, Herder, 2013, p. 29.

día mirando pantallas y ciertamente es preocupante que nuestros niños estén expuestos a las redes del delito en forma permanente un cuarto del día[21].

Otro gran impacto que se puede observar en la sociedad de la información, se da en la institución social de la familia, que es donde verificamos a diario la asimetría entre grandes y niños, en el manejo y en el conocimiento de cuestiones relacionadas con la informática, donde los niños están familiarizados con las redes sociales y son consultados por las generaciones sociales más adultas sobre su uso y funciones; que además, estos últimos, son los que deben controlar y resguardar a los integrantes más pequeños de la sociedad del acecho de la delincuencia.

Es entonces necesario, repensar, este fenómeno, para que estas nuevas tecnologías no los dañen y nos dañen a nosotros, ya que esta singular paradoja (*entre víctimas que manejan tecnologías de forma hábil y padres y tutores que deben cuidarlos, que nos las manejan con presteza*); y es allí, donde considero que reside la complejidad y dificultad de erradicar este fenómeno delictivo, que golpea de lleno en el seno de nuestras familias, que es el núcleo de nuestra estructura social, que se puede estar resintiendo, con esta "contradicción social", que los delincuentes, sin dudas aprovechan.

Intenté, primero, entonces, buscar una definición de delitos informáticos por parte de la doctrina, que satisfaga los requerimientos de nuestra legislación penal, apelando a los fines prácticos de una definición y ya he fundamentado porque he elegido relegar las definiciones para emplear, luego, tres categorías de clasificación para analizar a cada una por separado.

He propuesto diferenciar, entonces, tres grandes grupos de clasificación, como "los delitos propiamente informáticos", es decir, que estos son solo los tipos penales, que tienen que ser cometidos con objetos o medios informáticos y no por otros medios u objetos para configurar el delito.

En la otra categoría, nos encontramos con los delitos, que por la asimilación realizada por el art. 77 del Cód. Penal, en relación la ampliación de las definiciones legales de documento, firma y suscripción, instrumento privado y certificado y la información privilegiada, en cuanto a que son términos, que comprenden ahora a los elementos informáticos que resultan ser *las bases de datos de documentos digitales y la firma o certificados firmados en forma digital*, que fueron asimilados e incluidos por definición a los delitos que contenían esos términos o aspectos informáticos.

La tercera categoría analizada comprende un amplio catálogo de delitos, que pueden ser cometidos por medios informáticos y de un modo ejemplificativo realizamos un veloz recorrido de todo nuestro Código Penal para demostrar que la generalidad de los delitos puede ser cometidos por estos medios; ya sea por una interpretación legal de los tipos legales de modo informático o por medios o través de objetos informáticos que son los elementos analizados a documentos.

- Los propósitos de este trabajo primariamente, se centraron en buscar primero, una definición de delitos informáticos o bien realizar una

[21] Ruston, Delaney, *Screenagers: growing up in the digital age*, www.youtube.com/watch?v=LQx2X0BXgZg.

clasificación, que tenga fines prácticos para facilitar su estudio y análisis; para explorar luego los delitos que pueden ser cometidos por medios informáticos en nuestro Código Penal, detenernos en el “ciber-acoso”, esbozar las dificultades que tiene esta figura para compararlo finalmente compararlo con otros delitos contra la integridad sexual y como como corolario de ello, analizar cuatro conductas disvaliosas que se dan en la sociedad cibernética, que sin dudas se erigen como problemas políticos criminales, que son el “phishing”, el “typosquatting”, la “distribución no consentida de imágenes de contenido sexual o íntimas” y el “camefting”.

Estas conductas delictivas no legisladas, las trajimos al tapete y las presentamos como cuatro maniobras delictivas informáticas, que en otras latitudes han sido debidamente legisladas y tipificadas, para señalarnos el camino, de cómo y dónde se podrían legislar.

Ha sido materia de mayor análisis, en este trabajo, sistematizar e interpretar de forma detallada el reciente delito incorporado a nuestro Código Penal, el llamado por la doctrina como “*grooming*”, tipo penal al que denominamos deliberadamente, en este trabajo “ciber-acoso” o “acoso informático”.

Este nuevo tipo penal como dijimos, constituye un delito típicamente informático, del que se ha explicado en primer término, la maniobra delictiva de este delito, luego su regulación legal en el Código, sus dificultades de interpretación, sus proyectos de reformas y sus posibles soluciones; fundamentalmente para propender que en nuestra sociedad no se generen, dos efectos socialmente disvaliosos, como lo son la injusticia y la impunidad.

Es por ello que se decidió más allá de analizar en particular el delito de “acoso informático”, para ilustrar los aspectos positivos y problemáticos de esta figura, poniendo en práctica la teoría, con un caso real, que nos lleva a realizar preguntas, como disparadores, para diseñar posibles respuestas.

Entiendo que estas nuevas situaciones requieren de todo nuestro esfuerzo tanto social, como académico para legislar de manera adecuada, estas situaciones, en pos de tener una sociedad real y cibernética más justa, donde se protejan, se respeten los derechos de quienes eligen a la web, como un nuevo modo de vida y son vulnerables ante ellas.

Y finalmente pienso que debemos “tener las antenas bien puestas”, para estudiar, analizar y proyectar las consecuencias, sopesando entonces los pros y las contras, de las posibles soluciones que ensayemos como sociedad, situación está, que ni más ni menos, nos enfrenta a diferentes paradigmas de vida y nos presenta un desafío para el futuro, que es erradicar o atenuar el impacto de los crímenes informáticos.

Es aquí donde tenemos que alertar a nuestras instituciones sociales y convocarlas a un debate público ciudadano, porque si bien como hemos dicho nuestra legislación tiene problemas de interpretación, con deficiencias de técnica legislativa, que a veces desnudan la falta de adecuación a los tratados internacionales y otras veces, exhiben inconsistencia valorativas en los tipos penales; considero que esta última, es la peor cara que puede mostrar nuestro Código Penal, porque como dijimos, un texto puede exhibir problemas de redacción e interpretación, pero los valores

sociales y culturales y su contenido axiológico, son el “último bastión” de nuestra comunidad que nos permitirá, encontrar nuestro justo norte, para apuntalar nuestra legalidad como una útil y democrática herramienta de control social.

Entiendo finalmente, que todavía falta mucho camino por recorrer en materia de política criminal, en el caso de los delitos informáticos, ya que día a día aparecen nuevas conductas que son socialmente disvaliosas, en la que es vital el uso de la tecnología.

Y es allí donde debemos detenernos en esta encrucijada y analizar si castigamos esas “conductas desajustadas socialmente” imponiendo una pena o si buscamos la manera de corregir la nocividad de ciertas prácticas de otro modo, pero lo que no podemos hacer como comunidad, es quedarnos inmóviles ante los delitos informáticos.

Finalmente lo que hemos pretendido soslayar, en este trabajo, es solo un análisis jurídico y social del problema; que no está dirigido a erigirse como un catálogo de certezas absolutas, sino que simplemente, busca deliberadamente que el lector se formulara ciertas preguntas e interrogantes para comprender este flagelo; para poder finalmente “destejer”, desde lo que falta comprender, que siempre es mucho, lo que llamaremos de aquí en adelante la “telaraña” de las redes del delito.