Dictamen para el Ministerio de Justicia de la Nación (Argentina) – Reforma sobre la criminalidad informática en la Argentina

Prof. Dr. Dr. Eric Hilgendorf

Dr. Dr. Leandro Dias, LL.M. (UTDT)

Wurzburgo, Alemania

20 de marzo de 2025

Índice

Introducción

En septiembre de 2024, el señor Alberto Nanzer y la señora Carolina Maglione, del Ministerio de Justicia de Argentina se pusieron en contacto con nosotros, en nombre del señor Ministro de Justicia, Mariano Cúneo Libarona. Nos propusieron realizar un análisis de la regulación actual de los ciberdelitos en Argentina y proponer una reforma, en caso de ser necesario. La propuesta era tentadora, pero al mismo tiempo extremadamente exigente. Después de deliberar un poco, decidimos aceptar la propuesta. Consideramos que esta era una oportunidad única para demostrar cómo la cooperación entre academia, política y praxis puede ser fructífera, por un lado. Por otro, estimamos que también era un buen momento para fortalecer la cooperación entre la ciencia del derecho penal alemana y la argentina.

Nuestra forma de realizar esta propuesta de reforma fue la siguiente. El señor Dias realizó una recopilación de la información relevante (legislación, artículos científicos y decisiones judiciales) en idioma español. El señor Hilgendorf, por su parte, realizó lo mismo en inglés y alemán. Tras la lectura y evaluación de las fuentes, fueron analizados distintos proyectos de ley argentinos actualmente en discusión. Esto permitió redactar cuatro conferencias sobre distintos aspectos de la regulación de los ciberdelitos que necesitan una reforma legal en Argentina. La investigación fue realizada en su totalidad en la Universidad de Wurzburgo, Alemania.

Las cuatro conferencias fueron presentadas a través de Zoom en idioma inglés entre octubre de 2024 y febrero de 2025. A esas conferencias asistieron el señor Nanzer y la señora Maglione, así como un equipo de trabajo que ellos organizaron en el marco del Ministerio de Justicia de Argentina. El señor Ministro de Justicia, Mariano Cúneo Libarona, participó de la discusión de las conferencias, así como diversos expertos argentinos sobre ciberdelitos. Entre ellos se encontraban Eugenio Sarrabayrouse, Eduardo Riggi, Marcos Salt y Jonathan Polansky, por solamente nombrar a algunos. Las discusiones que se produjeron durante esas conferencias permitieron mejorar las conferencias que ahora se han convertido en un dictamen completo. Además, los señores Marcelo Sancinetti, Marcelo Lerman y José Béguelin leyeron la versión final de las conferencias y nos brindaron valiosos comentarios sobre el tema. A todos ellos les estamos inmensamente agradecidos. La experiencia general ha sido muy enriquecedora y consideramos que se logró algo pocas veces visto: una colaboración entre expertos de dos países distintos, que hablan idiomas distintos, pero que comparten una tradición común

en el derecho penal. Todo esto fue realizado *ad honorem* y con el único fin de poder contribuir a mejorar la legislación argentina en un tema tan importante como el combate de la ciberdelincuencia. Esperamos que este sea solo el comienzo de una nueva forma de hacer legislación no solo en Argentina, sino también en todo el ámbito de habla hispana y alemana.

Prof. Dr. Dr. Eric Hilgendorf
Dr. Dr. Leandro Dias, LL.M. (UTDT)
20 de marzo de 2025
Wurzburgo, Alemania

Reforma sobre criminalidad informática en la Argentina (1). Parte General del derecho penal

Eric Hilgendorf y Leandro Dias[1]

I. Introducción

Hasta mediados de los años ochenta del siglo pasado, el uso de una computadora con fines privados era una rara excepción.[2] Hoy, sin embargo, la mayoría de los hogares europeos, y también, creemos, la mayoría de los argentinos, tienen al menos una computadora.[3] Al mismo tiempo, cada vez más dispositivos domésticos funcionan con tecnología digital, como los teléfonos y relojes inteligentes, o incluso lavarropas y heladeras. De hecho, el uso de Internet para fines personales y profesionales se ha convertido en algo habitual.[4] Hoy en día, Internet es una parte de la infraestructura pública casi tan indispensable como la red pública de rutas. Por tanto, no es exagerado hablar de una *digitalización integral* de nuestro entorno vital.[5]

El rápido avance de las nuevas tecnologías de la información y la comunicación también ha dado lugar a nuevos comportamientos socialmente nocivos y delictivos.[6] El legislador argentino ha respondido con diversas legislaciones, entre las que se encuentran la Ley 26.388 ("ciberdelitos" en general, a partir del llamado "Convenio de Budapest"[7]),[8] la Ley 26.904 (*grooming*)[9] y la Ley 27.436 (distribución y tenencia de pornografía ilícita).[10] Sin

---

[1] Este documento de trabajo se basa en dos textos anteriores de Eric Hilgendorf, uno de los autores: Hilgendorf, Eric/Valerius, Brian/Kusche, Carsten, *Computer- und Internetstrafrecht,* 3.ª ed., Berlin/Heidelberg, Springer, 2023 y Hilgendorf, Eric, "Kurze Stellungnahme zum Entwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität (BT-Drucksache 16/3656 vom 30.11.2006) für die öffentliche Anhörung im Rechtsausschuss des Deutschen Bundestages am Mittwoch, dem 21. März 2007", *Deutscher Bundestag*, Ausschüsse, 16. Wahlperiode, Mittwoch, Marz 21, 2007, disponible en: https://webarchiv.bundestag.de/archive/2008/0416/ausschuesse/a06/anhoerungen/15_Computerkriminalitaet/04_Stellungnahmen/index.html [último acceso: 15/03/2025].

[2] Hilgendorf, *Deutscher Bundestag*, p. 1 (1).

[3] Hilgendorf, *Deutscher Bundestag*, p. 1 (1).

[4] Hilgendorf, *Deutscher Bundestag*, p. 1 (1).

[5] Hilgendorf, *Deutscher Bundestag*, p. 1 (1).

[6] Hilgendorf, *Deutscher Bundestag*, p. 1 (1).

[7] Consejo de Europa, Convenio sobre la Ciberdelincuencia, 23 de noviembre de 2001, aprobado en Argentina por la Ley 27.411 del 22 de noviembre de 2017.

[8] En detalle Riquert, Marcelo, "Repensando cómo funciona la ley penal en el ciberespacio", en: Riquert (coord.), *Ciberdelitos*, 2.ª ed., Buenos Aires, Hammurabi, pp. 21 (48 ss.).

[9] En detalle Garibaldi, Gustavo, "Aspectos dogmátigos del *grooming* legislado en Argentina", *Revista derecho penal* 7 (2014), p. 21 (22 ss.).

[10] En detalle Riquert, Fabían Luis, "La ciberpornografía infantil en el Código Penal argentino", en: Riquert (coord.), *Ciberdelitos*, 2.ª ed., Buenos Aires, Hammurabi, pp. 255 (256 ss.).

embargo, debido a los constantes cambios que se producen en torno a esta área, el Ministerio de Justicia nos ha solicitado que analicemos la posibilidad de reformar el Código Penal argentino en materia de criminalidad informática.

A pedido del Ministerio de Justicia de la Argentina, analizaremos este tema en cuatro conferencias. En esta primera conferencia, evaluaremos la necesidad de tomar medidas en la parte general del Código Penal argentino para combatir la criminalidad informática. En la segunda, analizaremos la regulación actual de los delitos patrimoniales, especialmente el delito de "fraude informático", para determinar si la protección actual contra los ataques digitales al patrimonio es adecuada. En la tercera conferencia, profundizaremos en los posibles delitos sexuales cometidos a través de Internet. En la cuarta y última conferencia, examinaremos otros ciberdelitos que, según nuestra opinión, podrían ser legislados.

Comencemos por los posibles cambios que podrían introducirse en la parte general del Código Penal argentino para combatir la ciberdelincuencia: cambios en las normas básicas de la primera parte del Código Penal argentino, que en principio son aplicables a todos los tipos penales de la llamada parte especial, es decir, a todos los delitos en particular. Pero antes de hacer eso, es necesaria una aclaración. En estas cuatro conferencias guiaremos nuestras reflexiones a partir de dos directrices básicas.

La primera es la necesidad de evitar tanto un exceso de regulación, como una sobre-criminalización.[11] El exceso de regulación, por ejemplo, a partir de la incorporación de múltiples delitos o de delitos extremadamente detallados, con un sinnúmero de modalidades delictivas, genera problemas de interpretación (ya que a más regulación, más texto y, por tanto, más posibilidades de interpretaciones divergentes de los distintos términos utilizados),[12] como de acceso al servicio judicial en sentido amplio. Con esto último nos referimos a que un buen código penal debería contener delitos descriptos de forma sencilla, que la ciudadanía pudiese leer y comprender con cierta facilidad en líneas generales, de modo tal que el trabajo de los expertos quedase limitado únicamente a casos difíciles.[13] Un código penal con cientos artículos y repleto de delitos con múltiples

[11] Sobre esta terminología, véase Husak, Douglas, *Sobrecriminalización*, Madrid, Marcial Pons, 2013, pp. 42 ss.

[12] Sobre la absurdidad de buscar la regulación "más detallada posible", véase Greco, Luis, "Das Bestimmtheitsgebot als Verbot gesetzgeberisch in Kauf genommener teleologischer Reduktionen", *ZIS* 2018, 475 (476 s.).

[13] Véase Ortiz de Urbina Gimeno, Íñigo, "El caso Benítez Álvarez, Carlos Esteban de la Cámara Federal de Casación Penal, Sala II, del 20/11/12, causa n. 15.268", en: Ziffer (ed.), *Jurisprudencia de Casación Penal*, Buenos Aires, Hammurabi, 2018, p. 153 (180 s).

modalidades difícilmente pueda cumplir esa finalidad.[14] Además, eso puede conducir a que sean castigados comportamientos que no merecen serlo (por no ser dañinos o por no ser materialmente injustos).[15] Ante la duda sobre si determinado caso debe ser criminalizado, en derecho penal debe regir la prudencia y postergar la criminalización hasta que haya mayor certeza en la discusión.

La segunda directriz también hace hincapié en la prudencia: en estas cuatro conferencias no plantearemos reformas revolucionarias, que afecten en gran medida al sistema del Código Penal argentino. Tenemos entendido que ya existe un grupo de trabajo oficial que está elaborando un proyecto integral de reforma del Código Penal, por lo que esa tarea les corresponde a ellos, no a nosotros. Por consiguiente, aquí solamente se realizará una propuesta sobria sobre los puntos que deberían ser mejorados de la regulación actual de la delincuencia informática. En una reforma integral, por supuesto, será posible ser más ambicioso.

II. Cuestiones jurisdiccionales

1. Principio general: territorialidad

Una característica fundamental de Internet es su carácter global y su independencia de las fronteras nacionales.[16] En consecuencia, los procesos de transmisión de datos que utilizan sus diversos servicios de comunicación a menudo involucran a los territorios de muchos países.[17] Esto puede ilustrarse con un simple correo electrónico enviado por un remitente de un país a un destinatario de otro, posiblemente utilizando servidores de correo electrónico y líneas de comunicación de otros países.[18] Esto es aún más cierto en el caso de un sitio web de libre acceso, al que, por tanto, se puede acceder desde cualquier lugar del mundo.[19] Cuando un contenido socialmente nocivo se difunde de esta manera, todos los Estados podrían teóricamente intentar hacer valer su jurisdicción penal.[20]

---

[14] Extremadamente críticos de esta forma de legislar Alexander, Larry/Ferzan, Kimberly, *Crime and Culpability*, Cambridge, University Press, 2009, p. 264 ss.

[15] Sobre los problemas que generan las reglas penales sobreinclusivas (es decir, que conminan con pena comportamientos que no merecen ser criminalizados), véase recientemente Green, Stuart, "Legal Moralism, Overinclusive Ofenses, and the Problem of Wrongfulness Confation", *Criminal Law and Philosophy* 14 (2020), 417 (420 ss.).

[16] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 1.

[17] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 1.

[18] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 1.

[19] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 1.

[20] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 1.

El Derecho penal internacional [*internationales Strafrecht*] regula en qué medida los delitos con un punto de conexión internacional (ya sea en la persona del autor o de la víctima, o en el lugar donde fue cometido el delito) están sujetos al Derecho penal nacional.[21] Sin embargo, contrariamente a este término engañoso, son únicamente las reglas nacionales las que determinan la aplicabilidad del derecho penal nacional, tanto a los delitos cometidos en el país, como a ciertos delitos cometidos en el extranjero.[22] Por esta razón, el término "regulación jurídica de la jurisdicción penal" o "régimen de aplicación penal" [*Strafanwendungsrecht*] es más comúnmente utilizado en la literatura especializada.[23]

En la Argentina, la jurisdicción penal está regulada por el artículo 1 del Código Penal. El punto de partida es el principio de territorialidad.[24] Según este principio, el derecho penal argentino se aplica a los delitos cometidos en el territorio nacional, es decir, los delitos cometidos en la Argentina.[25] Por consiguiente, el criterio decisivo es el lugar de comisión del delito, que es complementado, además, mediante el llamado principio de ubicuidad: el delito se reputa cometido en la Argentina cuando su acción o su resultado se producen en el territorio nacional, de modo que la jurisdicción argentina está destinada a cubrir indistintamente estas dos situaciones.[26]

En el caso, no infrecuente en la era de Internet, de que además de la ley penal argentina, también sea aplicable la ley penal de otros países (según las reglas de esos otros países), y por tanto, intervengan potencialmente varios códigos penales simultáneamente, el Código Penal argentino no contiene una disposición general sobre el conflicto de leyes. En estas situaciones, la Argentina podrá reivindicar su jurisdicción penal, pero los conflictos puntuales son resueltos individualmente, ya sea por acuerdos previos con el otro país, o a partir de reglas *ad hoc* para resolver el conflicto particular.

La regulación argentina del principio de territorialidad, con su principio de ubicuidad, es bastante escueta:

"ARTICULO 1.- Este Código se aplicará

[21] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 2.
[22] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 2.
[23] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 2.
[24] Por todos Rusconi/Kierszenbaum, *Elementos de la parte general del derecho penal*, Buenos Aires, Hammurabi, 2024, p. 72.
[25] Rusconi/Kierszenbaum, *Elementos de la parte general del derecho penal*, p. 72.
[26] Rusconi/Kierszenbaum, *Elementos de la parte general del derecho penal*, p. 73.

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

Según la opinión usual en la Argentina, entonces, la expresión "delitos cometidos" se refiere tanto a la acción delictiva como al resultado delictivo. Esto puede tener ciertas consecuencias importantes en la extensión de la jurisdicción penal argentina a casos no necesariamente relacionados con la Argentina. Por ejemplo, en Alemania, una parte de la doctrina está a favor de ampliar el significado de la acción delictiva en el caso de las publicaciones en Internet.[27] Después de todo, Internet les permitiría a los usuarios iniciar operaciones de procesamiento de datos no solo en su propia computadora, sino también en la computadora a la que acceden por medio de Internet (por ejemplo, el servidor en el que se almacena el contenido de su sitio web).[28] En consecuencia, según esta postura, estaría justificado considerar que el lugar de la acción penal es tanto la computadora de origen como el la computadora de destino de la respectiva transferencia de datos.[29] Una discusión similar aparece en el marco de la determinación del resultado en ciertos delitos cometidos en Internet.[30] Incluso hasta se ha sostenido que la mera accesibilidad de los contenidos en un determinado lugar constituye un lugar del resultado, lo que resulta por demás exagerado.[31]

Sea o no correcta esta extensión del concepto de acción y de resultado, basta señalar aquí que se trata de cuestiones controvertidas en la literatura jurídico-penal: la adecuada caracterización de los conceptos de acción y resultado a efectos de la definición de la jurisdicción penal. Estas discusiones surgen no solo en el contexto de la criminalidad informática, sino en cualquier otra subdivisión del derecho penal. Y si el legislador argentino aún no se ha decidido a introducir cambios en esta sucinta regulación de las reglas de jurisdicción, no parece que haya motivos para hacerlo ahora. En todo caso, corresponderá a la doctrina y a la jurisprudencia dilucidar cuándo es aplicable el derecho penal argentino en estos difíciles casos.

2. Excepciones al principio de territorialidad

[27] Panorama en Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 15 ss.
[28] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 22.
[29] Cf. Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 22.
[30] Panorama en Hilgendorf, Eric/Valerius, Brian, *Derecho Penal. Parte General*, 2.ª ed., Buenos Aires, Ad-Hoc, 2017, § 2 n.º m. 8 ss.
[31] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 25.

Con independencia de esta última cuestión, todos los delitos que no sean cometidos en el ámbito interno según estos principios son considerados delitos cometidos en el extranjero. Para aplicar el derecho penal argentino a crímenes cometidos en el extranjero en casos excepcionales y sin violar el principio de no intervención del Derecho Internacional, se requiere un punto de conexión significativo o legitimante. Éste puede ser la necesidad de proteger bienes jurídicos nacionales (principio de protección) o internacionales (principio de jurisdicción universal), o la nacionalidad del autor o de la víctima (principio de personalidad activa o pasiva).[32]

En la discusión sobre criminalidad informática, el principio de jurisdicción universal adquiere especial relevancia.[33] Así, el legislador alemán ha decidido aplicar este principio no solo a los clásicos "*core crimes*" del derecho penal Internacional, sino también a otros crímenes, entre los que están incluidos los siguientes:

"6. Delitos cometidos en el extranjero contra bienes jurídicos protegidos internacionalmente:
El Derecho penal alemán rige, además, independientemente del Derecho del lugar del hecho, para los siguientes hechos cometidos en el extranjero:
6. difusión de contenidos pornográficos en los casos de los §§ 184a, 184b, párrafos 1 y 2, y 184c, párrafos 1 y 2".[34]

Se trata de casos de difusión de, por ejemplo, contenidos pornográficos violentos, que pueden ser perseguidos en Alemania independientemente del lugar del mundo en que se haya producido la difusión. Sin embargo, esta decisión del legislador ha sido criticada por extender demasiado la jurisdicción penal alemana a casos en los que la conexión con Alemania es más bien tenue.[35]

[32] Panorama de estos puntos conexión Chehtman, Alejandro, "Jurisdiction", en Hörnle/Dubber (eds.), *The Oxford Handbook of Criminal Law*, Oxford, University Press, 2014, p. 399 (399 ss.).
[33] Kindhäuser, Urs/Hilgendorf, Eric, *Código Penal alemán,* t. 1, Buenos Aires, Hammurabi, 2023, § 6 n.º m. 1.
[34] Se utiliza la traducción de Marcelo Sancinetti, Patricia Ziffer, Lucila Tuñón y Leandro Dias, publicada en: Kindhäuser/Hilgendorf, *Código Penal alemán,* t. 1, § 6.
[35] Al respecto, en detalle Ambos, Kai, en: *Münchener Kommentar zum Strafgesetzbuch*, 5.ª ed, Múnich, C.H. Beck, 2024, § 6 n.º m. 14: "La República Federal Alemana tampoco está habilitada por el derecho internacional a extender el derecho penal alemán hasta alcanzar la difusión de pornografía en el extranjero [nota al pie omitida]. Este delito no es un hecho que alcance la cualidad de ilícito de un crimen internacional, ni se ven afectados intereses alemanes dignos de protección si, por ejemplo, un mexicano le vende pornografía 'dura' a un compatriota en México. La distribución electrónica de pornografía a través de Internet no cambia la naturaleza de ilícito del hecho; a lo sumo, proporciona una mejor fundamentación del poder punitivo alemán, a saber, como ocurre generalmente con la ciberdelincuencia, a través del principio de los efectos" (traducción de Leandro Dias)"

No parece, entonces, justificado realizar una extensión de esta clase en la Argentina. La aplicación del Código Penal argentino a casos de criminalidad informática a partir del principio de territorialidad, complementado por el principio de ubicuidad (y acompañado, dado el caso, de una interpretación extensiva, en caso de que se lo considere necesario), parece suficiente para captar un alcance razonable de la jurisdicción penal argentina. Además, un enjuiciamiento amplio como el propuesto en Alemania para ciertos casos (es decir, casos de difusión de determinados contenidos en los que ni el acto ni el resultado del acto se realizaron en Alemania en sentido estricto, sino que pueden haber tenido lugar en África, Asia, Oceanía, etc.) podría resultar bastante inconveniente desde un punto de vista práctico y diplomático.[36] Recuérdese, nuevamente, que se trataría de casos en los que no sería posible establecer una conexión significativa entre la acción y el resultado con la Argentina. Esta clase de extensión de la jurisdicción debe quedar limitada a su núcleo de aplicación clásico, es decir, a casos de afectaciones de bienes jurídicos verdaderamente internacionales: genocidio, crímenes contra la humanidad, crímenes de guerra y crimen de agresión.

Algo similar puede decirse respecto de otras excepciones al principio de territorialidad, como la personalidad activa o pasiva. Si un hecho es cometido contra un ciudadano argentino, pero ni la acción ni el resultado de ese delito tienen una conexión mínima con la Argentina, la posibilidad teórica de una aplicación del Código Penal argentina no resulta evidente. En ese sentido, el argentino que es víctima o autor de un delito se encuentra en principio sometido a las reglas de la comunidad política en la que tuvo lugar ese delito y solo razones de peso fundamentarían una decisión legislativa diferente.[37] Dado que el principio de territorialidad, tal como es entendido en la Argentina, ya ofrece un alcance razonable de la jurisdicción penal argentina en casos de criminalidad informática, esas razones no parecerían estar dadas. Esta valoración puede cambiar y es, por supuesto, discutible. En todo caso, consideramos que la inclusión del criterio de personalidad activa o pasiva en el Código Penal no es tanto una cuestión relativa únicamente a la delincuencia informática, sino a cualquier clase de delitos (o al menos a *más* delitos). Por consiguiente, una decisión a favor de incorporar el criterio de

[36] Véase, al respecto Hilgendorf, Eric, "Crime, Law and the Internet", *Analyse & Kritik* 26 (2004), 302 (312).

[37] Sobre los problemas que genera la idea de que sería legítimo perseguir delitos cometidos en cualquier parte del mundo, con independencia de si tuvieron lugar en la comunidad respectiva, con excepción de ciertos delitos internacionales, Duff, R.A., "Criminal Law and the Constitution of Civil Order", *The University of Toronto Law Journal* 70 (2020), 4 (6 ss.).

personalidad activa o pasiva debería ser tomada en el marco de una reforma integral del Código Penal, no en una limitada solo a la criminalidad informática.

En consecuencia, no parece aconsejable regular en la parte general del Código Penal argentino una aplicación del principio de jurisdicción universal o de otras excepciones a la territorialidad, limitada solo a los casos de criminalidad informática. El principio de territorialidad, con su regulación actual, luce lo suficientemente robusto como para abarcar esta clase de casos de un modo adecuado y una decisión diferente debería estar acompañada de una reforma integral. En consecuencia, no recomendamos modificar la parte general del Código Penal argentino sobre jurisdicción penal.

III. Sobre la introducción de la definición de "contenidos" y otras definiciones

Al igual que el § 11 del Código Penal alemán, el artículo 77 del Código Penal argentino contiene una disposición con definiciones de varios términos que son empleados repetidamente a lo largo de la parte especial del Código Penal. En este contexto, un término es particularmente importante en el Código Penal alemán: "contenidos".

Concretamente, el § 11, párr. 3, del Código Penal alemán establece lo siguiente:

"(3) Contenidos en el sentido de las disposiciones que hacen referencia a este párrafo son aquellos que están contenidos en escritos, soportes de sonido o imagen, medios de almacenamiento de datos, ilustraciones y otras corporizaciones o bien, independientemente de un almacenamiento, son trasladados por medio de técnicas de información o comunicación".[38]

Ciertamente, puede considerarse la posibilidad de incluir una disposición similar en el artículo 77 del Código Penal argentino. Sin embargo, el legislador argentino ha utilizado el término "contenidos" solo esporádicamente en algunas disposiciones relevantes de la parte especial, como el artículo 153 (transmisión o publicación de contenido secreto) o el artículo 154 (violación de correspondencia). Por consiguiente, pensamos que no es necesario simplificar la regulación con una regla general. Por lo demás, incorporar en los delitos respectivos de la parte especial una remisión interna a la definición de la parte general da lugar a una técnica legislativa engorrosa,[39] que en principio debe ser evitada.

[38] Se utiliza la traducción de Marcelo Sancinetti, Patricia Ziffer, Lucila Tuñón y Leandro Dias, publicada en: Kindhäuser/Hilgendorf, *Código Penal alemán,* t. 1, § 11.
[39] Véase Ambos, Kai, *derecho penal Europeo*, Valencia, Tirant lo Blanch, 2017, Cap. III n.º m. 31 ss.

Algo similar debe ser señalado respecto de la posibilidad de incorporar más definiciones en la parte general del Código Penal sobre cuestiones vinculadas a la criminalidad informática. En particular, se podría pensar en incorporar definiciones que pueden encontrarse en distintos convenios internacionales, como los que se encuentran en el Convenio de Budapest sobre Cibercriminalidad. Consideramos que tal incorporación debe ser evitada, por las siguientes razones.

En primer lugar, incorporar sin más definiciones provenientes de instrumentos internacionales cuya redacción es el resultado de negociaciones entre distintos Estados, en distintos idiomas, nunca es una buena idea.[40] Pero incluso si esa cuestión fuese considerada secundaria, no se debe perder de vista que el Código Penal es una ley pensada para regular el comportamiento punible en una determinada comunidad, a partir de los valores y compromisos de una determinada comunidad. Trasladar sin más definiciones pensadas para regular "a gran escala" una serie de cuestiones, sin atender a las particularidades de la comunidad respectiva,[41] tales como la cultura jurídico-penal en la que se enmarca, la sistemática del propio código o aquello que se considera como especialmente disvalioso, sería un error.

En segundo lugar, incorporar definiciones internacionales ya en la parte general del Código Penal limitaría demasiado la labor de los intérpretes y haría demasiado inflexible al derecho penal argentino. El hecho de no contar con definiciones fijas permite que quienes deben aplicar el derecho (jueces, pero también juristas, practicantes, etc.) postulen interpretaciones razonables que luego serán adoptadas, descartadas o modificadas parcialmente en la praxis.[42] Para evitar que la persecución y juzgamiento de la criminalidad informática termine debilitándose como consecuencia del uso de definiciones, aconsejamos no incorporar más definiciones en la parte general.

---

[40] En general sobre los problemas de la utilización de múltiples lenguajes para la interpretación del derecho Malarino, Ezequiel/Fronza, Emanuela, "Problemas de determinación de la norma penal y soluciones de interpretación en textos penales plurilingües en el ejemplo del Estatuto de Roma", en: Ambos/Malarino/Woischnik (eds.), *Temas actuales de Derecho Penal Internacional*, Montevideo, Konrad-Adenauer Stiftung, 2005, p. 169 (169 ss.).

[41] Sobre el problema similar que aparece con la utilización no autoritativa de derecho extranjero en la fundamentación de las sentencias judiciales con impacto en el derecho constitucional, véase Rosenkrantz, Carlos, "En contra de los 'préstamos' y de otros usos 'no autoritativos' del derecho extranjero", *Revista Jurídica de la Universidad de Palermo*, Año 5, n.º 1, 71 (83 ss.).

[42] Sobre las exigencias menores en materia de determinación que impone el principio de legalidad respecto de la parte general del derecho penal y en contraposición con la parte especial, véase Dias, Leandro, "Teoría del dominio del hecho y principio de legalidad en la Corte penal Internacional", *InDret: Penal* 4 (2018), 1 (10 ss.).

En tercer y último lugar, es un tanto redundante incorporar al Código Penal las definiciones que pueden encontrarse en instrumentos internacionales de los que el Estado Argentino es parte. En la Argentina, los tratados internacionales son fuente del derecho, sin la necesidad de un acto de transposición o incorporación en el derecho interno.[43] Por consiguiente, no es necesario incorporar las definiciones que se encuentran, por ejemplo, en el Convenio de Budapest, para que puedan ser utilizadas en la praxis. Ese convenio es derecho vigente aplicable en la Argentina y quienes aplican el derecho podrán utilizarlo, por ejemplo, para interpretar elementos de ciertos tipos penales. Para realizar esa tarea no es necesario incorporar absolutamente nada a la parte general del Código Penal.

IV. Responsabilidad penal de los proveedores de Internet

Navegar por la web, cargar y descargar archivos, enviar correos electrónicos, chatear y usar redes sociales son actividades cotidianas que requieren los servicios de los proveedores de servicios de Internet (ISP).[44] Estos proporcionan acceso a Internet, transmiten información a través de las autopistas de la información y ponen la información a disposición de los usuarios en servidores propios o de terceros.[45] En el otro vértice de la relación, aparecen los usuarios que utilizan los servicios de los ISP (normalmente empresas de telecomunicaciones).[46]

Debido a las diferentes tareas de los proveedores y a la variedad de servicios en Internet, varias personas (físicas y jurídicas) suelen intervenir en cada proceso de comunicación y, por tanto, en cada transferencia de datos en Internet.[47] Por ejemplo, un proceso "sencillo" como la distribución de contenidos a través de un sitio web requiere la participación de al menos cinco personas.[48] Para que el contenido esté disponible, el proveedor (persona 1) debe cargar primero el archivo en el servidor web. Para ello, necesita los servicios del llamado proveedor de red (persona 2), que le permite transferir el archivo al servidor web, y los servicios del llamado proveedor de alojamiento (persona 3), que le proporciona el espacio de almacenamiento necesario en el servidor web. Por último, el usuario del sitio

[43] En detalle, recientemente, Pinto, Mónica/Maisley, Nahuel, "Una historia de doble lealtad: el derecho internacional en la jurisprudencia de la Corte Suprema de Justicia de la Nación argentina", *Pensar en Derecho* 12 (2024), 23 (31 ss.).
[44] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 52.
[45] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 52.
[46] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 52.
[47] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 53.
[48] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 53.

web (persona 5) recurre al proveedor de acceso (persona 4) para recuperar los datos a través de los cuales se conecta a Internet.

Si son difundidos contenidos ilícitos (por ejemplo, archivos de imagen y vídeo de pornografía ilícita o declaraciones injuriantes) en Internet de esta o de cualquier otra forma, o si la transmisión causa daños ilícitos al hardware o software de un tercero (por ejemplo, mediante un virus), se plantea la cuestión de la responsabilidad de las partes implicadas en el proceso de comunicación en cuestión.[49] Mientras que, en estos casos, son aplicables las reglas generales de responsabilidad penal, la responsabilidad penal de los proveedores es una cuestión compleja en Alemania, debido a la existencia de normas especiales de exención de responsabilidad (§§ 7 y ss. TMG).[50] La TMG fue sustituida por la Ley de Servicios Digitales (*Digitale Dienste-Gesetz*, DDG) en mayo de 2024, bajo la influencia de la legislación europea. Sin embargo, las normas de exención de responsabilidad siguieron siendo esencialmente las mismas.

La Argentina no ha seguido este camino, por lo que son aplicables, sin más, las reglas generales habituales de la parte general del derecho penal. Esto es teóricamente ventajoso, ya que nadie queda por fuera de la ley si se aplican las reglas usuales de la responsabilidad penal. Y dado que en principio no hay ninguna necesidad de que ciertas personas sean eximidas de responsabilidad penal, a pesar de que realizaron un comportamiento antijurídico, no resulta apropiado seguir el camino europeo.[51] Por consiguiente, y a menos que el legislador desee modificar la responsabilidad de los ISPs de manera más amplia (por ejemplo, eximiéndolos de responsabilidad en determinados casos o estableciendo deberes especiales), sugerimos no crear reglas especiales de exención de responsabilidad penal para los ISPs en un proyecto de ley sobre criminalidad informática.

No obstante, en la última reunión analizaremos la posibilidad de crear un tipo penal de peligro abstracto consistente en proporcionar determinadas plataformas delictivas con el fin de facilitar la comisión de delitos: puesta a disposición plataformas que permiten la adquisición de armas, drogas e información necesaria para la comisión de delitos contra la propiedad, entre otras conductas ilícitas.

V. Responsabilidad por omisión

[49] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 53.
[50] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 54 ff.
[51] Para un panorama de las principales discusiones en torno a este problema, véase Kusche, Carsten, *Doping, redes sociales y fake news*, Buenos Aires, Editores del Sur, 2022, pp. 17 ss.

Los principios generales del derecho penal, que por regla general son aplicables a todos los casos de criminalidad informática, exigen, entre otras cosas, que se distinga entre la comisión de un delito por acción positiva y la comisión de un delito por omisión.[52] Si el autor solo ha cometido un delito por omisión, son necesarios requisitos adicionales para que pueda haber responsabilidad penal.[53] En particular, si no se encuentra tipificado un delito específico de omisión (los llamados "delitos propios de omisión"), para que pueda haber responsabilidad por el delito correspondiente (por ejemplo, por una estafa), el autor debe haber omitido una conducta debida, a pesar de tener un deber legal de evitar el resultado del delito (la denominada posición de garante).[54]

Dado que la responsabilidad penal por omisión es bastante restrictiva, la clasificación de una acción como acción u omisión reviste una importancia fundamental.[55] La mayoría de los penalistas suelen hacer esta distinción basándose en circunstancias externas, como la causalidad entre la conducta y el resultado típico (asumiendo que las omisiones no causan, en los casos de causalidad habría acciones) y el empleo de la energía (o el movimiento corporal).[56] Según estos criterios, si el autor interviene activamente en el mundo exterior, entonces actúa, mientras que si se comporta pasivamente, entonces omite. Sin embargo, según la opinión dominante, estos criterios son solo el punto de partida de una consideración normativa que, atendiendo a la trascendencia social de la acción (el llamado "punto neurálgico de la reprochabilidad"), resulta decisiva para determinar la conducta relevante en derecho penal.[57]

Estas cuestiones son muy importantes en el ámbito de la criminalidad informática.[58] Piénsese, por ejemplo, el caso de ofertas ilegales en Internet, donde existen principalmente dos puntos de conexión para la responsabilidad penal: la influencia en el contenido mediante la publicación o el enlace de las ofertas en cuestión, por un lado, y la participación puramente técnica, por otro, al permitir el acceso o no bloquear o eliminar los contenidos respectivos.[59] En estos casos habrá que diferenciar el análisis, según los criterios anteriormente señalados, con el fin de determinar si hubo responsabilidad por

[52] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 136.
[53] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 136.
[54] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 136.
[55] En detalle Lerman, Marcelo, *La omisión por comisión*, Buenos Aires, AbeledoPerrot, 2012, pp. 111 ss.
[56] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 137.
[57] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 137; para un panorama, con referencias adicionales, Hilgendorf/Valerius, Derecho Penal. Parte General, 2.ª ed., Buenos Aires, Ad-Hoc, 2017, § 11 n.º m. 11 s.
[58] Véase Kusche, *Doping, redes sociales y fake news*, pp. 23 ss.
[59] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 138.

acción, responsabilidad por omisión o ninguna clase de responsabilidad. Algo similar sucede con las posiciones de garante, por ejemplo de los proveedores de servicios. En particular, una posición de garante de evitar los delitos cometidos por quienes utilizan los servicios, por ejemplo por lo que publican ilícitamente en redes sociales, podría ser posible a partir de una obligación contractual o de una orden administrativa o judicial, como una orden de bloqueo.[60]

Estas cuestiones no están reguladas en detalle en la Argentina.[61] De hecho, a diferencia de otras jurisdicciones, ni siquiera existe una cláusula de equivalencia entre acciones y omisiones. En este contexto, uno podría preguntarse si sería posible dejar la regulación argentina como está, ya que una opinión usual en la doctrina es que la responsabilidad penal por omisiones "impropias" puede derivarse de la conducta delictiva descrita en la parte especial del Código Penal: en ciertos casos, actuar equivaldría a omitir, y, por ejemplo, dejar morir a alguien equivaldría a un caso usual de homicidio, como sería matar a alguien con un cuchillo.[62] La otra solución sería establecer una cláusula de equivalencia entre actuar y omitir.[63] Esta cuestión requiere un tratamiento mucho más profundo del que es posible ofrecer en un breve dictamen sobre la reforma en materia de delincuencia informática. No obstante, si el legislador argentino decide regular la cuestión, y sabemos que existe una comisión de expertos trabajando en una reforma general, quizás podría considerarse la actual regulación alemana sobre la materia:

"§ 13. Comisión por omisión

1) Quien omite impedir un resultado que integra el tipo de una ley penal es punible según esa ley solo si tiene que velar jurídicamente por que el resultado no se produzca y la omisión es equivalente a la realización del tipo legal por medio de un hacer.

2) La pena puede ser atenuada según el § 49, párrafo 1".[64]

---

[60] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 142.

[61] Para una perspectiva crítica, véase solamente Gullco, Hernán, *Casos de derecho penal. Parte general*, Buenos Aires, Ad-Hoc, 2022, pp. 281 ss.; Zaffaroni, Eugenio/Alagia, Alejandro/Slokar, Alejandro, *Derecho penal. Parte general*, Buenos Aires, Ediar, 2000, p. 553.

[62] Véase, por todos, Lerman, *La Omisión por Comisión*, p. 222; Sancinetti, Marcelo, *Casos de derecho penal,* Tomo I, 3.ª ed., Buenos Aires, Hammurabi, 2005, p. 293; ídem, "La relación entre el delito de 'abandono de persona' y el 'homicidio por omisión'", en Ziffer (eds.), *Jurisprudencia de Casación Penal,* Tomo I, Buenos Aires, Hammurabi, 2009, p. 245 (274).

[63] Sobre esta cuestión Trovato, Gustavo, "Incorporación legislativa de la comisión por omisión: ¿más cosas que beneficios?", Revista de Derecho Penal y Procesal Penal 2005, pp. 1699 (1699 ss.).

[64] Se utiliza la traducción de Marcelo Sancinetti, Patricia Ziffer, Lucila Tuñón y Leandro Dias, publicada en: Kindhäuser/Hilgendorf, *Código Penal alemán,* t. 1, § 13.

Además, un segundo inciso, como el que existe en Alemania, podría hacer referencia al estándar de atenuación previsto en el Código Penal argentino para las tentativas. El artículo quedaría regulado del siguiente modo:

"Artículo 36
1. Quien omite impedir un resultado que integra el tipo de una ley penal será penado según esta ley solo si tiene que velar jurídicamente por que el resultado no se produzca y la omisión equivalga a la realización del tipo legal mediante un actuar.
2. La pena podrá ser atenuada según la escala penal de la tentativa (artículo 44, párr. 1.°, Código Penal)".

No obstante, esta es solo una sugerencia para el caso de que se considere necesario incorporar una cláusula de adecuación. Por lo pronto, dado que en la Argentina se ha trabajado más de cien años adecuadamente sin una cláusula de equivalencia y que el tratamiento de los delitos impropios de omisión son moneda corriente en la praxis, tampoco parece imprescindible su incorporación en una futura reforma. Más bien, parecería tratarse de una cuestión de interpretación básica sobre qué significa realizar un delito, que bien puede quedar en manos de la doctrina y la jurisprudencia.

VI. Responsabilidad por autoría y responsabilidad accesoria

De acuerdo con el sistema dualista de autoría y participación, se aplican dos regímenes diferentes, según el delito sea doloso o imprudente. En los delitos dolosos es posible intervenir en un delito como autor según el artículo 45, oración 1, primera alternativa, y también como partícipe "accesorio" (complicidad primaria e instigación) según el artículo 45, oración 1, segunda alternativa y oración 2, y según el artículo 46 del Código Penal argentino (complicidad secundaria).[65] En cambio, en los delitos imprudentes solo es posible la autoría (sin posibilidad de responsabilidad por participación accesoria de la autoría).[66]

Asumiendo que es correcta esta distinción, existen diferentes enfoques sobre cómo puede trazarse la necesaria distinción entre autoría y responsabilidad accesoria en los delitos

[65] Por todos, Rusconi/Kierszenbaum, *Elementos de la parte general del derecho penal*, 3.ª ed., p. 187 s.
[66] Al respecto y desde una posición crítica, véase Sancinetti, Marcelo, *Teoría del delito y disvalor de acción*, Buenos Aires, Hammurabi, 1991 (4.ª reimpresión 2022), pp. 246 ss.

dolosos.[67] Según la teoría dominante del "dominio del hecho",[68] un autor es alguien que controla el curso del delito en virtud de su voluntad y, por lo tanto, actúa como figura central del hecho. Un partícipe, en cambio, es alguien que, sin ser el autor, se limita a iniciar o facilitar de otro modo la comisión del delito y, por lo tanto, es solo una figura periférica del hecho.[69]

La distinción entre la responsabilidad del autor y del partícipe en la difusión de contenidos prohibidos en Internet es especialmente problemática. Es indiscutible que un proveedor de contenidos que publica sus propios contenidos ilegales en Internet o crea enlaces a sus propios contenidos es autor.[70] En cambio, la valoración de los enlaces a contenidos de terceros es más difícil y controvertida. En algunos casos, la puesta a disposición de contenidos se considera un hecho delictivo a título de autoría, porque puede tener un impacto significativo en la difusión de contenidos delictivos.[71] A esto se opone, con razón, el argumento de que la criminalidad por parte del enlazador suele caer porque el enlace por sí solo no transmite ningún dominio sobre los datos enlazados.[72] La cuestión de clasificar la conducta como autoría o participación también se plantea en el caso de (in)actividades de naturaleza técnica.[73] Esto también se aplica al hecho de que los proveedores no bloqueen el contenido, que debe clasificarse como omisión: ¿se trata de una omisión realizada a título de autor o una complicidad por omisión?[74]

En este contexto, también son aplicables las normas generales sobre la responsabilidad del autor y del partícipe. Tales normas proporcionan suficiente flexibilidad para que los tribunales resuelvan estas difíciles cuestiones en cada caso de criminalidad informática. En todo caso, estos ejemplos difíciles servirán para poner a prueba las teorías creadas hasta ahora, que fueron pensadas más bien para otros delitos del derecho penal nuclear como el homicidio, las lesiones corporales y los robos. Por lo tanto, no es necesario introducir cambios en el Título VII sobre participación criminal, sino simplemente intensificar la discusión científica en materia de autoría y participación aplicada a casos de criminalidad informática.

---

[67] En detalle Sancinetti, Marcelo, *Teoría del delito y disvalor de acción*, pp. 541 ss.
[68] Para un panorama, desde una perspectiva crítica Falcone, Andrés, *La caída del dominio del hecho*, Buenos Aires, Ad-Hoc, 2017, pp. 40 ss.
[69] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 146.
[70] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 149.
[71] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 149.
[72] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 149.
[73] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 150.
[74] En detalle Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 150.

VII. Error de prohibición

El conocimiento de la ilicitud es un elemento independiente dentro la culpabilidad penal.[75] El autor debe ser consciente de que está violando los valores establecidos por el derecho.[76] Si el autor no es consciente de la ilicitud del hecho, está sujeto al denominado error de derecho o "error de prohibición".[77] Si el error sobre el ilícito resulta ser inevitable, el autor actúa sin responsabilidad penal por ausencia de culpabilidad, en virtud del principio constitucional de culpabilidad.[78] Por otro lado, si el error del autor podría haberse evitado, se suele afirmar que el juez tiene la posibilidad (pero no la obligación) de atenuar la pena dentro de la escala de penas aplicable, aunque no existe ninguna disposición legal específica al respecto.[79] Es decir, esto último no tiene, en principio, ningún sustento legal o constitucional, sino que se trata de una construcción teórica.[80]

Las peculiaridades de Internet impiden a veces que sus usuarios sean conscientes de la ilicitud de su conducta.[81] Por ejemplo, quienes navegan por Internet desde la computadora de su hogar no suelen sentirse reconocidos ni observados, lo que contribuye a la creencia de que ingresan a un espacio libre de regulación jurídica.[82] Lo mismo ocurre con quienes participan en foros o chats bajo un seudónimo que no permite sacar conclusiones sobre su identidad, ya que la sensación de anonimato puede crear la falsa impresión de que las acciones carecen de naturaleza delictiva, cuando en realidad pueden configurar, por ejemplo, una injuria punible. Además, los usuarios no suelen ser conscientes de que están dejando rastros significativos y creen que operan de incógnito en una esfera pública virtual diferente a la del mundo real.[83]

Esta percepción errónea apoya la opinión generalizada de que Internet es un espacio virtual autónomo, que se encuentra fuera del alcance del derecho.[84] Sin embargo, el ciberespacio no es un mundo separado en el que el usuario entra en Internet.[85] Más bien, cada flujo de datos se basa en el comportamiento real de una persona real en una

[75] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 151.
[76] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 151.
[77] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 151.
[78] Por todos, Rusconi/Kierszenbaum, *Elementos de la parte general del derecho penal*, p. 143.
[79] Para más detalles, véase Córdoba, Fernando, *La evitabilidad del error de prohibición*, Buenos Aires, Marcial Pons, 2011, pp. 23 ss.
[80] En detalle Gullco, Hernán, *Casos de derecho penal. Parte general*, Buenos Aires, Ad-Hoc, 2022, pp. 548 ss
[81] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 152.
[82] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 152.
[83] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 152.
[84] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 153.
[85] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 153.

computadora real.[86] Por supuesto, muchos usuarios no se dan cuenta de que sus acciones aparentemente virtuales a veces tienen graves consecuencias en la realidad.[87] Además, hay que tener en cuenta el carácter descentralizado y transnacional de Internet.[88] Se puede acceder a sitios web de libre acceso desde cualquier país y, por lo tanto, pueden ser relevantes para muchos ordenamientos jurídicos nacionales.[89] En muchos casos, un autor no será consciente, o no lo será plenamente, de esta dimensión de sus acciones.[90] Es poco probable, a su vez, que alguien que publica contenidos en línea, cuya distribución no es punible en su país de origen, considere la posibilidad de que sus declaraciones sean punibles en otro país.[91]

Es cierto que tales errores jurídicos son en gran medida evitables, es decir, que el autor podría haber evitado el error si se le hubiera informado adecuadamente. Sin embargo, si el autor no creía realmente que estaba cometiendo un delito, su conducta merece un tratamiento más indulgente que en los casos en que no hubo tal error. El hecho de que en la Argentina no exista una norma específica respecto de los errores de derecho evitables crea la impresión de que tales errores son irrelevantes, lo que no es el caso, y menos aún en contextos como el que nos ocupa.

En este contexto, la posibilidad de incluir una norma explícita sobre el error de derecho evitable en el Código Penal argentino podría ser una posibilidad muy interesante para explorar. Un punto de partida para la regulación sería el artículo 34 del Código Penal, que señala lo siguiente:

"Artículo 34.- No son punibles: 1º. El que no haya podido en el momento del hecho, ya sea por insuficiencia de sus facultades, por alteraciones morbosas de las mismas o por su estado de inconciencia, error o ignorancia de hecho no imputables, comprender la criminalidad del acto o dirigir sus acciones".

Una regulación sencilla del error de prohibición consistiría en añadir un segundo párrafo, con una regulación equivalente a la Alemana (§ 17, Código Penal alemán):[92]

[86] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 153.
[87] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 153.
[88] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 155.
[89] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 155.
[90] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 155.
[91] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 2 n.º m. 155.
[92] Se utiliza la traducción de Marcelo Sancinetti, Patricia Ziffer, Lucila Tuñón y Leandro Dias, publicada en: Kindhäuser/Hilgendorf, *Código Penal alemán,* t. 1, § 17.

"§17. Error de prohibición
Si, al cometer el hecho, al autor le falta la comprensión de realizar un ilícito, actúa sin culpabilidad, si no pudo evitar este error. Si el autor podía evitar el error, la pena puede ser atenuada según el § 49, párrafo 1".

Adoptamos esta formulación a partir de las reflexiones sobre el tema de Marcelo Sancinetti,[93] quien en especial ha señalado que, en caso de que se quiera regular expresamente el error de prohibición evitable, la utilización de la frase "no comprendiere su criminalidad" es lo suficientemente general como para abarcar los casos relevantes de error de prohibición (incluyendo posibles errores sobre la punibilidad del acto). Sin embargo, una reforma de esta clase excede el ámbito de regulación de un proyecto sobre criminalidad informática. Más bien, quienes estén a cargo de reformar íntegramente el Código Penal deberán tomar esta decisión.

VIII. Regulación del ejercicio de la acción penal

Antes de cerrar esta primera conferencia, debe decirse que en la parte general del Código Penal argentino aparece una anomalía en el ejercicio de las acciones. En particular, los delitos de violación de secretos se encuentran regulados en al artículo 173, inciso 2, como delitos de acción privada, a excepción de los artículos 154 y 157. Esta regulación en principio tiene sentido, debido a que los delitos de violación de secretos están estrechamente vinculados a las relaciones personales entre privados, por lo que el interés del Estado en la protección de la intimidad en estos casos suele estar subordinado al interés en las partes en que el Estado persiga la conducta. A su vez, las excepciones de los artículos 154 y 157 están justificadas, debido a que se trata de conductas que pueden poner en peligro intereses de la sociedad en su conjunto. Así, el artículo 154 merece persecución penal autónoma debido a que se criminaliza la conducta de un empleado de correos o telégrafos que abusa de sus funciones y afecta el normal funcionamiento de los servicios generales de correspondencia. El artículo 157 criminaliza a los funcionarios públicos que revelan determinados datos cuyo secreto se encuentra establecido por ley, lo que puede poner en peligro no solo la confianza en el accionar estatal, sino también aquellos intereses que se quiso proteger originariamente al establecer el secreto legal.

[93] Sancinetti, Marcelo, "Exigencias mínimas de la dogmática del hecho punible en la parte general de los códigos penales", disponible en: https://perso.unifr.ch/derechopenal/assets/files/articulos/a_20080527_01.pdf [último acceso: 15/03/2025], 1 (27).

Si se tiene en cuenta esta dinámica del ejercicio de las acciones, resulta curioso que dos delitos de violación de secretos que resultan muy importantes para el castigo justo de la criminalidad informática sean meramente de acción privada. El primero de ellos es el artículo 153bis, que criminaliza el acceso ilegítimo a un sistema o dato informático de acceso restringido, con una agravante para los casos de acceso a un "sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros". Esta clase de conductas, característica de hackeos y/o ciberataques, merece una persecución penal de oficio y no meramente una librada al arbitrio de las víctimas. En particular, estas conductas son realizadas a diario y generan grandes peligros para la intimidad de las víctimas, así como para otros intereses vinculados (ejemplo: intereses patrimoniales). El Estado debería, entonces, poder investigar y castigar estas acciones, incluso si las víctimas deciden no ejercer la acción penal.

Con mayor razón vale lo mismo respecto del artículo 157bis del Código Penal, que criminaliza con una pena relativamente alta distintos ejemplos de accesos ilegítimos a archivos y bancos de datos, así como otras acciones tendentes a afectar el secreto y la intimidad relacionada con esos bancos o archivos de datos personales. Luce evidente que hay un interés público en castigar estos casos en general y ese interés se vuelve más notable en el último párrafo de ese artículo, que establece la siguiente agravante: "Cuando las conductas reprimidas se hicieran para acceder, revelar, insertar o suprimir datos que afectaren a un banco de datos genéticos, registros, exámenes o muestras de ADN, la pena será de prisión de seis (6) meses a cuatro (4) años, con más inhabilitación especial para ejercer la profesión de dos (2) a cinco (5) años". Debido al carácter altamente personal de esos datos, el acceso, revelación, supresión, etc., es una conducta con un elevado contenido de ilícito (o antijuridicidad material), que debe ser perseguida de oficio.

Proponemos hacer lo mismo con un delito que propondremos en la última conferencia a partir de la incorporación de un artículo 153 ter al Código Penal. Se trata del delito de difusión de información personal peligrosa y que conmina con pena el hacer accesible a terceros información sensible de un modo idóneo para causar daños. Dado que estas conductas son potencialmente muy perjudiciales tanto para los individuos, como para la generalidad (ya que está en juego la intimidad de las personas, por un lado, y la consciencia general de que los datos personales están protegidos), este delito debe ser de acción pública.

Por consiguiente, proponemos que el artículo 73, inciso 2, del Código Penal quede redactado de la siguiente manera:

"Artículo 73. Son acciones privadas las que nacen de los siguientes delitos: […]
2) Violación de secretos, salvo en los casos de los artículos 153 bis, 153 ter, 154, 157 y 157 bis".

IX. Conclusión

Las conclusiones de esta primera reunión pueden ser resumidas del siguiente modo:

1) En cuanto a la jurisdicción penal, las reglas generales del derecho penal argentino son aplicables a los casos de delitos informáticos. Los principios de territorialidad y ubicuidad brindan suficiente flexibilidad para resolver estos casos y no es necesaria ninguna reforma. Tampoco es necesario extender el principio de jurisdicción universal a los casos de ciberdelitos.

2) En principio, no es necesario incluir una definición general del término "contenidos" en el artículo 77 del Código Penal argentino, aunque el § 11, párr. 3, del Código Penal alemán contiene tal definición. Tampoco es necesario incorporar a la parte general del Código Penal las definiciones que pueden encontrarse en distintos instrumentos internacionales, como el Convenio de Budapest.

3) La responsabilidad penal de los proveedores de Internet sigue los principios generales de la responsabilidad penal. El derecho penal argentino no les otorga inmunidades excepcionales de castigo, y en principio no hay razón para crear un régimen legal especial.

4) La distinción entre actos y omisiones es particularmente importante en el caso de ciberdelitos, ya que muchas actividades ilícitas son omisiones. En la Argentina, los delitos de omisión son reconocidos por la opinión predominante en la doctrina, aunque no existe una regulación legal explícita sobre el tema. Por lo tanto, no es estrictamente necesario regular esta cuestión. Sin embargo, si el legislador argentino lo desea, una disposición como la del § 13 del Código Penal alemán podría servir de modelo.

5) Las reglas generales de autoría y responsabilidad accesoria también son aplicables a los ciberdelitos. Estas normas están adecuadamente definidas en los artículos 45 y siguientes del Código Penal argentino y no requieren ninguna modificación *ad hoc*.

6) Es posible que, en muchos casos de criminalidad informática, el autor actúe con un error de prohibición evitable. Este concepto jurídico es reconocido por la doctrina argentina, pero no se encuentra explícitamente regulado en el Código Penal. Por esta

razón, puede ser aconsejable incluir un párrafo adicional en el Artículo 34 Inciso 1 del Código Penal argentino para regular esta cuestión. Esa decisión deberá ser tomada por quienes planifiquen una reforma integral del Código Penal.

7) Se propone que los delitos de los artículos 153 bis (junto con el 153 ter, todavía no existente, pero que se propondrá en la última conferencia) y 157 bis dejen de ser de acción privada y pasen a ser de acción pública, debido al evidente interés estatal en la persecución y castigo de esas conductas de criminalidad informática grave.

Reforma sobre la criminalidad informática en la Argentina (2). Delitos patrimoniales

Eric Hilgendorf y Leandro Dias[1]

I. Introducción

Las computadoras y las redes informáticas, como Internet, pueden ser utilizadas no solo para lesionar los bienes jurídicos de terceros mediante la publicación de contenidos como tales.[2] Además de las habituales violaciones al honor (injurias) y de la posible invasión de la privacidad a través de Internet, que analizaremos en la última conferencia, también pueden ser cometidos otros delitos en relación con las computadoras y las redes informáticas.[3] En todos estos casos, la computadora actúa como medio para cometer el delito o como objeto del delito.[4] Un ejemplo claro son las estafas cometidas bien contra una persona (estafa del artículo 172 del Código Penal argentino), bien directamente contra un sistema informático (fraude informático, estafa informática o defraudación informática, del artículo 173 del Código Penal argentino).

En los siguientes apartados analizaremos la protección patrimonial prevista en el Código Penal argentino y su relación con los posibles supuestos de criminalidad informática. La conclusión a la que se llega es que la protección que brinda el Código Penal argentino en esta materia es insuficiente, ya que ciertos casos (entre los que se destaca el *phishing*) no están (o no se hallan) adecuadamente contemplados en las disposiciones legales (sección II). A continuación, propondremos tres modificaciones a la normativa vigente. En primer lugar, propondremos la tipificación del *phishing* como delito de peligro abstracto; en segundo lugar, propondremos la modificación del delito de fraude informático para incluir los casos de uso no autorizado de datos; en tercer lugar, defenderemos la tipificación como delito de los actos preparatorios del fraude informático (sección III). Por último, sintetizaremos brevemente el contenido de esta conferencia (sección IV).

---

[1] Este documento de trabajo se basa en dos textos anteriores de Eric Hilgendorf, uno de los autores: Hilgendorf, Eric/Valerius, Brian/Kusche, Carsten, *Computer- und Internetstrafrecht,* 3.ª ed., Berlin/Heidelberg, Springer, 2023 y Hilgendorf, Eric, "Kurze Stellungnahme zum Entwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität (BT-Drucksache 16/3656 vom 30.11.2006) für die öffentliche Anhörung im Rechtsausschuss des Deutschen Bundestages am Mittwoch, dem 21. März 2007", *Deutscher Bundestag*, Ausschüsse, 16. Wahlperiode, Mittwoch, Marz 21, 2007, disponible en: https://webarchiv.bundestag.de/archive/2008/0416/ausschuesse/a06/anhoerungen/15_Computerkriminalitaet/04_Stellungnahmen/index.html [último acceso: 15/03/2025].

[2] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 264.

[3] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 264.

[4] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 264.

II. La situación jurídica actual: estafa y fraude informático

1. Estafa (Art. 172, Código Penal argentino)

a. Cuestiones generales

Mientras que la estafa (artículo 172 del Código Penal argentino) desempeña un papel relativamente menor en la criminalidad cometida a través de los medios de comunicación tradicionales, los nuevos medios, especialmente Internet, crean nuevas clases de riesgos para la ciudadanía, y en especial para los consumidores.[5] Entre otras cosas, el *homebanking*, el comercio electrónico, los juegos en línea y el llamado *ransomware* amplían las oportunidades de los delincuentes con los conocimientos adecuados para cometer delitos.[6] En muchos casos, las nuevas capacidades de la tecnología de las comunicaciones se utilizan para cometer, de hecho, estafas.[7]

La estafa cometida a partir de Internet puede adoptar dos formas.[8] Por una parte, la acción típica puede ser cometida *contra un sistema informático* con el fin de influir en el resultado de una operación de procesamiento de datos. Dicha manipulación es punible en Argentina en virtud de lo dispuesto en el artículo 173, apartado 16 del Código Penal argentino (fraude informático). Por otra parte, la estafa puede ser cometida *contra una persona* de manera convencional.[9] Este delito clásico de estafa, tipificado en el artículo 172 del Código Penal argentino, ha encontrado nuevas formas de comisión mediante Internet, como en el pasado ha encontrado nuevas formas de comisión a partir del descubrimiento del teléfono, por ejemplo.[10] En muchos casos, se trata de formas conocidas de estafa bajo una nueva apariencia, por lo que no existen particularidades en términos de la responsabilidad penal.[11] El autor aprovecha las ventajas de Internet: se puede acceder a Internet en cualquier momento y lugar, y el usuario permanece en el anonimato.[12] Además, el efecto es rápido y eficaz, ya que se puede llegar prácticamente sin demora a muchos destinatarios, que pueden reaccionar inmediatamente a un mensaje.[13] A diferencia de la estafa tradicional, la víctima suele ser completamente

[5] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 266.
[6] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 266.
[7] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 266.
[8] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 267.
[9] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 267.
[10] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 267.
[11] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 267.
[12] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 267.
[13] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 267.

desconocida para el autor, es decir, no solo el autor sino también la víctima son anónimos en Internet.[14]

Aunque la redacción del artículo 172 del Código Penal argentino no lo deja suficientemente claro, el tipo objetivo de estafa consta de cuatro elementos fundamentales: engaño, error, disposición patrimonial y perjuicio o daño patrimonial.[15] Entre estos elementos debe existir una relación causal: el autor engaña a su víctima, provocándole un error.[16] Este error hace que la parte equivocada realice un acto de disposición patrimonial, lo que en última instancia da lugar a un daño patrimonial.[17] Mientras que la persona engañada y la que realiza la transferencia de activos deben ser la misma, no es necesario que la persona que realiza la transferencia y la víctima del perjuicio sean idénticas.[18] Por tanto, es posible engañar a alguien para que realice una disposición patrimonial por error con el fin de enriquecer al autor con los activos de un tercero que la persona engañada tiene a su disposición.[19]

A pesar de lo que pueda parecer a primera vista, este tipo penal redactado de un modo tan elegante como sucinto permite resolver adecuadamente muchos casos relevantes de criminalidad informática, sin que sea necesaria ninguna reforma. Sin embargo, algunos casos no pueden ser adecuadamente cubiertos por esta disposición, ni por la disposición sobre defraudación informática del artículo 173, inciso 16 del Código Penal argentino. En las siguientes secciones, analizaremos algunas formas usuales de estafa por Internet con el fin de descubrir lagunas de punibilidad. Asumiremos, en todos los casos, que el autor actúa con dolo directo (es decir, sabe que está estafando y que quiere estafar) y que además tiene ánimo de enriquecerse mediante la estafa. De este modo, los eventuales problemas que suelen surgir en relación con el elemento subjetivo de la estafa quedarán neutralizados y se podrá centrar la atención en lo decisivo, es decir, en los alcances del delito de estafa ya en su faceta objetiva.

b. Estafa a través de plataformas de comercio electrónico

[14] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 267.
[15] En detalle Righi, Esteban, *El delito de estafa*, 2.ª ed. (2.ª reimpresión), Buenos Aires, Hammurabi, 2023, pp. 72 ss.; Romero, Gladys, *Delito de estafa*, 2.ª ed., Buenos Aires, Hammurabi, 2007, pp. 109 ss.
[16] Por todos Righi, Esteban, *El delito de estafa*, p. 110.
[17] Por todos Righi, Esteban, *El delito de estafa*, pp. 118 ss.
[18] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 268.
[19] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 268; así también Righi, *El delito de estafa*, p. 121.

Piénsese en un autor que pone a la venta bienes en una tienda online contra pago por adelantado o pago en efectivo en la entrega, pero no entrega los bienes solicitados (en el caso de pago por adelantado) o solo entrega un paquete vacío o un artículo de menor valor (en el caso de pago en efectivo en la entrega).[20] En este caso, el autor que celebra el contrato afirma implícitamente su capacidad y voluntad de cumplir.[21] Esta es una acción engañosa, apta para generar un error en el comprador, lo que termina sucediendo. Con el pago se produce la disposición patrimonial, que termina afectando negativamente el patrimonio del propio comprador (o de un tercero, en nombre de quien se realizó la transacción). Por consiguiente, se trata de casos de estafas consumadas según el art. 172 del Código Penal y no es necesario hacer ninguna modificación legislativa para abarcar adecuadamente estos casos.

c. Trampas de suscripción

Ahora imaginemos que el autor diseña un sitio web que da la impresión de que ofrece servicios gratuitos tras una suscripción obligatoria.[22] Sin embargo, la suscripción requiere que el usuario realice un pago, que se produce automáticamente o de un modo casi automático tras el ingreso de un medio de pago que no iba a ser utilizado para un pago. En este caso, la configuración externa del sitio web declara tácitamente que el servicio es gratuito.[23] Si esta tergiversación de servicios gratuitos da lugar a una disposición patrimonial y a un perjuicio, entonces se produce una estafa según el art. 172 del Código Penal. El hecho de que el sitio web haya sido configurado y lanzado incluso mucho tiempo antes que la disposición patrimonial mediada por error no impide, en principio, la configuración del tipo objetivo. Piénsese en casos de homicidio en los que alguien realiza una conducta, por ejemplo colocar una bomba en la casa de otra persona, que luego se detona automáticamente unos días después. Si el paso del tiempo no impide la configuración del tipo objetivo en el homicidio y parecería que tampoco en la estafa. En todo caso, la discusión se deberá dar en el marco del tipo subjetivo: si el grado de representación de los elementos del tipo objetivo es suficiente para configurar el dolo,[24] al menos en casos en los que el autor actuó sin dolo directo de primer grado. Empero, esta

[20] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 275.
[21] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 273.
[22] En detalle Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 276.
[23] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 276.
[24] Sobre esta cuestión, véase solamente Sancinetti, Marcelo, *Teoría del delito y disvalor de acción*, Buenos Aires, Hammurabi, 1991 (4.ª reimpresión 2022), pp. XVII ss., con referencias adicionales.

es una cuestión general de interpretación y aplicación del derecho, que puede (y debe) abordarse sin una reforma de la ley, al menos en principio. Por consiguiente, el tipo penal clásico de estafa soluciona los casos de trampas de suscripción y no es necesario un tipo penal adicional

d. Subastas fraudulentas en línea

Ahora pensemos en que alguien realiza una oferta en su propia subasta en línea para hacerle subir el precio al producto.[25] Es discutible si esto ya constituye una conducta delictiva, por tratarse de un engaño típico de la estafa, o si el autor aún está dentro del ámbito de la conducta comercial socialmente adecuada.[26] Las condiciones generales de las plataformas de subastas suelen prohibir este tipo de comportamiento, que también afecta al sentido de una subasta.[27] Se supone que el subastador no participará en la subasta en sí, y si lo hace, se produce un engaño que puede conducir al fraude. Por eso, difícilmente pueda decirse que esa clase de conducta todavía se enmarca en lo comercialmente permitido. Más bien, se trata de un engaño que conduce al error de la víctima, quien cree que el precio del producto es mayor que el real. Dado que el pago que termina realizándose es superior al que debería haberse realizado si no hubiera mediado un engaño, entonces se produce una estafa en estos supuestos.

En todo caso, podrá discutirse si en ejemplos de esta clase se produce un verdadero daño patrimonial en virtud del estándar que se utilice para determinarlo.[28] En particular, se podría argumentar que si el comprador terminó pagando un precio usual de mercado (o incluso uno por debajo del precio usual de mercado), entonces no habría ningún daño patrimonial, a pesar de que el vendedor realizó una acción engañosa.[29] Esta cuestión puede quedar abierta aquí.[30] Lo importante es señalar que el tipo penal de estafa está perfectamente preparado para abarcar esta clase de casos, que podrán ser impunes en algunas ocasiones y punibles en otras, según la interpretación que se realice de los distintos elementos del tipo objetivo del delito. Por consiguiente, no luce necesaria una reforma para abarcar estos casos.

[25] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 277.
[26] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 277.
[27] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 277.
[28] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 291.
[29] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 291.
[30] Para un desarrollo comprensivo en la literatura argentina, véase Righi, Esteban, *El delito de estafa*, pp. 134 ss

e. Estafas de spam

Ahora concentrémonos en el caso de un remitente de un correo electrónico que le informa a la víctima que debe sacar del sistema financiero de su país una suma muy importante de dinero procedente de un país lejano.[31] Le pide al destinatario del mensaje que facilite una cuenta bancaria para recibir ese dinero y le promete una importante comisión.[32] Sin embargo, para hacer eso primero deben pagarse tasas u otros gastos, y recién después se realizaría la transferencia del dinero.[33] Una vez pagadas las "tasas", la víctima no vuelve a tener noticias de su supuesto socio comercial.[34] En estos casos, parecería darse un engaño: el autor finge su condición de persona en un aprieto y que debe enviar dinero a otro país, por lo que estaría dispuesto a pagar una comisión. También hay error, ya que la víctima cree que todo eso es cierto y que recibirá una comisión como consecuencia del pago de las tasas y la puesta a disposición de la cuenta bancaria. El pago de las tasas es una disposición patrimonial que termina siendo perjudicial, en la medida en que el patrimonio de la víctima se ve disminuido. Por consiguiente, se trata de casos usuales de estafa, que presentarán distintas particularidades en la praxis, pero que pueden ser abordados adecuadamente a partir del art. 172 del Código Penal.

f. Esquemas de bola de nieve y esquemas piramidales

Estos casos son de particular importancia en la Argentina, ya que se han convertido recientemente en formas populares de criminalidad.[35] En ambos modelos de negocio, el iniciador recibe dinero de los clientes reclutados para participar en el esquema que promete rendimientos seguros o casi seguros.[36] Entonces, los participantes intentan ganar dinero atrayendo a más inversores al programa, también con la promesa de obtener rendimientos extraordinarios.[37] Si no se encuentran más inversores y capital, el sistema colapsa y los que no pueden recuperar sus pérdidas sufren un perjuicio patrimonial.[38] Por supuesto, en estos esquemas no son realizadas inversiones reales, al menos como regla general, sino que el único rendimiento que se genera es el que proviene de conseguir

[31] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 283.
[32] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 283.
[33] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 283.
[34] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 283.
[35] Solo a modo de ejemplo, véase esta reciente sentencia sobre el tema: Tribunal de Juicio de la 2.ª Circunscripción Judicial de Goya (Corrientes), Legado de juicio n.° 2124/22 (LIF n.° 16511/22 – Goya), 25 de febrero de 2025, con comentario de Aboso, Gustavo, "La estafa mediante esquema Ponzi y el caso Cositorto", *ElDial.com*, DC35B7, 1 (1 ss.).
[36] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 294.
[37] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 294.
[38] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 294.

nuevos participantes en el esquema, quienes aportan capital y permiten que el ciclo continúe.[39]

A veces, "sistema de bola de nieve" y "sistema piramidal" se toman como sinónimos, otras veces los conceptos se utilizan para hacer referencia a distintos tipos de interacción. La diferencia más importante entre los sistemas de bola de nieve o piramidales es que en los primeros el organizador es solo el socio contractual de los clientes iniciales, que suscriben sus propios contratos con los demás participantes.[40] En los esquemas piramidales, sin embargo, todos los contratos se celebran con el organizador, es decir, también los participantes que se incorporan más tarde suscriben un contrato con el que inicia el ciclo.[41] En ambos casos, el patrimonio de los participantes está en peligro desde el momento en que son reclutados, lo que bastaría para hablar de un perjuicio o pérdida financiera.[42] En otras palabras, se trata de casos de estafas que ya podrían estar consumados con la primera aportación de la víctima a la estafa piramidal o bola de nieve. Esto se debe a que la oferta de participar en el esquema a cambio de una determinada cuota se compensa con la alta probabilidad de que no se reclute a ningún otro participante, o al menos no lo suficiente como para recuperar la inversión.[43] Si el participante individual consigue más tarde recuperar su pago anticipado reclutando a nuevos participantes, esto no impide la consumación de la estafa, sino que a lo sumo podrá tener efecto sobre la determinación de la pena.[44]

Por supuesto, el momento exacto de la consumación del hecho puede discutirse. Uno puede considerar que el mero peligro de daño patrimonial no es suficiente y considerar que hay una estafa consumada desde el momento en el que el inversor solicita el pago de lo invertido más el extra producido o al menos la devolución del capital inicial.[45] En todo caso, esas son cuestiones de interpretación y aplicación del derecho clásicas del delito de estafa del art. 172 del Código Penal,[46] y nada nuevo sucede aquí que permita justificar la creación de un nuevo delito. Lo mismo se aplica respecto de la cuestión relativa a si en estos esquemas se produce una verdadera acción engañosa, o si se trata de esquemas tan

[39] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 294.
[40] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 294.
[41] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 294.
[42] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 294.
[43] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 294.
[44] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 294.
[45] Sobre esta cuestión, válida tanto para el delito de estafa como el de administración fraudulenta, véase Wostry, Thomas, "El daño patrimonial de la estafa (§ 263, CP alemán) en la jurisprudencia del Tribunal Constitucional y del Tribunal Supremo Alemán", *En Letra: Derecho Penal* 5 (2017), 32 (36 ss.).
[46] Similar Aboso, *ElDial.com*, DC35B7, 1 (4 ss.).

burdos que en realidad no hay ningún engaño.[47] La cuestión del estándar mediante el cual se debe evaluar la acción del autor de la estafa también es un tema discutido en la dogmática del delito de estafa y estos casos no presentan ninguna particularidad que obligue a modificar el derecho vigente.

g. Phishing

Esta palabra inventada, formada por "*password*" (contraseña) y "*fishing*" (pesca), describe la práctica delictiva de pedirles a los usuarios de Internet, por ejemplo, que faciliten datos de acceso como PINs (números de identificación personal) y TANs (números de transacción) para el *homebanking* a través de un correo electrónico supuestamente del banco de la persona o de una institución similar de confianza.[48] Nuevamente, este es un ejemplo y los detalles pueden cambiar, pero ese es el modelo general consistente en tratar de "pescar" contraseñas de forma engañosa para producir un daño patrimonial. El núcleo de esta práctica debe ser encontrado en el comportamiento de la víctima, que consiste en proporcionarle credenciales al *phisher*, quien obtiene acceso en línea a una cuenta bancaria.[49]

Sin embargo, en este momento del hecho, el autor aún necesita dar un importante paso intermedio para utilizar los datos obtenidos para acceder realmente al patrimonio del titular de la cuenta.[50] Por tanto, la divulgación (preparatoria) de los datos personales en sí *no conduce directamente a una disposición patrimonial*, ni a una pérdida patrimonial, ni siquiera en forma de amenaza de daño, equivalente a perjuicio patrimonial.[51] Una amenaza al patrimonio equivalente a un perjuicio o pérdida solo podría entrar en consideración si el autor estuviese en posesión, por ejemplo, de una tarjeta SIM de sustitución comprada al proveedor de telefonía móvil de la víctima y recibe así números de transacciones en su teléfono móvil a través del denominado procedimiento mTAN.[52] No obstante, en la mayoría de los casos, la mera divulgación de datos personales por medio de un engaño no es suficiente para la disposición patrimonial (ni para un daño patrimonial)[53] y, por tanto, la disposición será realizada *por el propio autor* y con

[47] En detalle sobre este problema general Pastor Muñoz, Nuria, *La determinación del engaño típico en el delito de estafa*, Madrid, Marcial Pons, 2004, pp. 119 ss., 238 ss.
[48] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 286.
[49] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 286.
[50] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 286.
[51] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 286.
[52] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 286.
[53] Hilgendorf, *Deutscher Bundestag*, p. 1 (10).

posterioridad a la entrega de datos. Recuérdese que para que se configure el delito de estafa debe haber identidad entre quien sufre el engaño y quien realiza la disposición patrimonial: si la disposición patrimonial la hace otra persona, entonces no habrá estafa.[54] Si esto es así, entonces los casos de *phishing*, al menos por regla general, no son supuestos de estafa, por ausencia de disposición patrimonial. Y dado que el Derecho Penal argentino no tiene una regla general de apropiación indebida, estos casos en principio podrían quedar impunes,[55] a menos que se recurra a una interpretación no ortodoxa de la ley,[56] y solo podrían dar lugar a acciones civiles contra quien se ha enriquecido antijurídicamente. Esta laguna de punibilidad es la que debe ser cubierta por medio de una reforma legal.

2. Fraude informático (artículo 173, inciso 16, Código Penal argentino) y fraude mediante uso no autorizado de tarjetas de pago (artículo 173, inciso 15 Código Penal argentino)

---

[54] Así también Béguelin, José/de Tezanos Pinto, Lola, "El delito de estafa y su estructura de autoría mediata. Análisis de la jurisprudencia del Tribunal Superior de Justicia de la CABA", en Ariza Clerici (ed.), *Compendio de jurisprudencia en conmemoración de los veinte años desde la asunción de los primeros magistrados del Fuero Penal, Contravencional y de Faltas de la CABA*, Buenos Aires, Jusbaires, 2024, p. 327 (340). El autor la engaña, la víctima sufre un error y, como consecuencia del error, realiza un acto que no es de disposición patrimonial, sino que consiste en entregar los datos de acceso a un sistema informático bancario o financiero. Luego el autor, por sí mismo, realiza las transferencias (o actos similares) que causan un perjuicio patrimonial a la víctima".

[55] Como esta consecuencia es valorativamente insostenible, tanto en la doctrina como en la praxis se ha recurrido a esta clase de interpretaciones no ortodoxas. Para una síntesis de estas posibles interpretaciones, así como de la jurisprudencia del Tribunal Superior de Justicia de la CABA sobre el tema, véase Béguelin/de Tezanos Pinto, *Compendio de jurisprudencia*, p. 327 (329 ss.). Más detalles sobre las distintas perspectivas de la jurisprudencia en Mahiques, Juan Bautista, *Formas modernas de criminalidad*, Buenos Aires, Hammurabi, 2024, pp. 105 ss.

[56] La interpretación doctrinal y jurisprudencial usual que considera a estos casos como típicos de estafa es expuesta con particular claridad por Riggi, Eduardo, "El delito de estafa informática", en Dupuy (ed.), *Ciberfraudes*, Buenos Aires, Hammurabi, 2024, p. 51 (58 s.): "ese texto […] no exige de modo alguno, a diferencia de la doctrina y jurisprudencia, que la disposición patrimonial tenga que ser ejercida de propia mano por el sujeto engañado". No obstante, eso no es ningún impedimento para que por interpretación se incluyan elementos *no escritos* en el tipo penal, siempre y cuando eso no expanda la punibilidad. Solo a modo de ejemplo, el tipo penal de homicidio (art. 79, CP) no incluye expresamente un requisito de causalidad, pero resulta evidente que este elemento debe ser incorporado a partir de una interpretación basada en el ilícito material que subyace a ese tipo penal: la acción de homicidio merece ser castigada porque le causa la muerte a otra persona. Sobre la causalidad como elemento no escrito Hilgendorf, Eric/Valerius, Brian, *Derecho Penal. Parte General*, 2.ª ed., Buenos Aires, Ad-Hoc, 2017, § 4 n.º m. 24. Por lo demás, que la víctima del engaño tenga que ser la misma que realiza la disposición patrimonial responde a la estructura de la estafa como delito de autoría mediata tipificada legalmente (véase Kindhäuser, Urs, *La estafa como autoría mediata tipificada*, Bogotá, Universidad del Externado, 2022, passim) y tiene implicancias en la delimitación de la estafa con otros delitos, como el hurto y la extorsión, en el marco del sistema de delitos patrimoniales (véase Hruschka, Joachim, "La conducta de la víctima como clave para un sistema de los delitos patrimoniales que llevan consigo sustracción", *Anuario de Derecho Penal y Ciencias Penales* LII [1999], 451 [452 ss.]). Por tanto, si bien aceptar que estos casos son verdaderas estafas no genera problemas de legalidad (la interpretación sigue siendo compatible con el texto de la ley), sí genera costos de legitimación, ya que la solución pasa a ser difícilmente compatible con los fundamentos teóricos del delito de estafa. Para evitar estos últimos costos, se propondrá una reforma legislativa más adelante en este texto. Le agradecemos a Eduardo Riggi por el constructivo intercambio que tuvimos respecto de esta cuestión.

El delito de fraude informático criminaliza el daño a la propiedad individual por influir en el resultado de una operación de procesamiento de datos, abarcando así nuevos delitos en el ámbito de la criminalidad informática. Este tipo penal del artículo 173, inciso 16, Código Penal argentino pretende cubrir los vacíos legislativos de responsabilidad penal basadas en el hecho de que el artículo 172 del Código Penal argentino presupone error humano,[57] que a menudo está ausente cuando se influye en un sistema de procesamiento de datos. De ahí que la influencia en el resultado de una operación de procesamiento de datos sustituye al error humano en el delito de fraude informático.[58] Ambas disposiciones exigen en el tipo objetivo una disposición patrimonial, ya sea por parte de una persona o como resultado de una operación de procesamiento de datos, que cause una pérdida o un perjuicio patrimonial.[59] A diferencia de Alemania, el legislador argentino decidió, de un modo por demás elogiable en términos de técnica legislativa, considerar cualquier manipulación técnica de una computadora como un acto delictivo, en lugar de regular variantes específicas.

Antes de crear el delito de fraude informático, el legislador argentino introdujo el denominado fraude mediante uso no autorizado de tarjetas en el artículo 173, inciso 15, Código Penal argentino.[60] Concretamente, este delito establece: "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".

Este delito es muy importante para la dogmática del delito de estafa en la Argentina, ya que permite castigar como estafa casos importantes en la actualidad, como el uso no autorizado de tarjetas de crédito o débito en sistemas de pago sin contacto, que no podrían ser considerados estafas sin más por falta de error humano, sin causar mayores problemas de interpretación.[61] A modo de ejemplo, este artículo permite castigar el fraude en

[57] Así, con claridad y por todos Riggi, Eduardo, *Ciberfraudes*, p. 51 (53).
[58] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 300.
[59] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 302.
[60] Panorama detallado en Righi, *El delito de estafa*, pp. 271 ss.
[61] Véase Righi, *El delito de estafa*, pp. 274 ss. Al parecer comparte esta apreciación Sueiro, Carlos Christian, *Ciberdelitos*, Buenos Aires, Hammurabi, 2023, p. 41. En contra de esto, Molina, Gonzalo, *Manual de Derecho Penal. Parte Especial*, Resistencia, ConTexto, 2021, p. 582 ss., quien considera que por tratarse de una defraudación siempre es necesario un error humano y, de otro modo, se violaría el principio de legalidad. Sin embargo, eso no se desprende del texto de la ley, sino que en todo caso es una interpretación. Las interpretaciones no forman parte del texto de la ley, por lo que no hay ningún problema de legalidad. En todo caso, la pregunta es si la interpretación aquí propuesta es adecuada. Y parecería que sí: si solo

operaciones de pago electrónico con el denominado procedimiento del punto de venta (POS) sin que medie un error humano de forma directa.[62] En este caso, el medio de pago es también una tarjeta de débito, y el titular se legitima ante el comerciante introduciendo su PIN.[63] Se comprueba el saldo de la cuenta y, si hay fondos suficientes, se establece una garantía de pago del banco emisor de la tarjeta.[64] La introducción del PIN de un *tercero* es un uso no autorizado de los datos y, por tanto, constituye un fraude mediante el uso de tarjetas de crédito.

Sin embargo, el delito de fraude informático previsto en el artículo 173, inciso 16, Código Penal argentino no abarca los casos de uso *no autorizado* de datos en sistemas automatizados.[65] Como se señaló anteriormente, el delito requiere la manipulación del funcionamiento normal del sistema ("mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos"), por lo que el uso no autorizado de datos no está cubierto. Esto genera problemas, por ejemplo, en los casos de uso indebido de las operaciones de pago en *homebanking* que no implican el uso de tarjetas de pago, como consecuencia incluso de operaciones de *phishing*.

Como ya se señaló, estas lagunas de punibilidad solo pueden ser resueltas en la praxis mediante interpretaciones poco ortodoxas de los tipos penales en cuestión. Dado que la probabilidad de que un tribunal esté dispuesto a realizar esta clase de interpretaciones puede variar, con el fin de lograr seguridad jurídica es necesario modificar la ley. En el próximo apartado se hará una propuesta en este sentido.

3. Conclusión

La protección penal de los bienes contra ataques informáticos en la Argentina definitivamente no es *fundamentalmente* inadecuada. Todo lo contrario: el delito de

importase el error humano de quien entrega un producto, entonces el tipo penal de estafa clásica ya es aplicable y no sería necesaria esta regulación.

[62] Sobre el tratamiento de estos casos en Alemania Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 320.

[63] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 320.

[64] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 320.

[65] Para una perspectiva diferente Béguelin/de Tezanos Pinto, *Compendio de jurisprudencia*, p. 327 (350 ss.), quienes sin embargo son plenamente conscientes del problema: "En contra de esta interpretación, en primer lugar, se podría argumentar que la expresión 'técnica de manipulación informática' refiere exclusivamente a una técnica en sí misma informática y que una manipulación no informática sobre un sistema informático queda fuera del concepto. En segundo lugar, se podría afirmar que en estos casos no se altera el normal funcionamiento de un sistema informático, dado que el sistema sigue funcionando tal como ha sido diseñado, solo que no logra sus fines. Pero no lograr sus fines, podría decirse, no es lo mismo que funcionar anormalmente".

estafa, complementado con los delitos de fraude informático y fraude mediante el uso no autorizado de tarjetas de pago, parece suficiente para cubrir un número importante de hechos delictivos relevantes.

Sin embargo, el análisis efectuado ha revelado al menos dos clases importantes de casos que hoy no serían punibles a menos que se recurra a una interpretación poco ortodoxa de la ley. El primero es el *phishing*, ya que *brindar* datos personales mediante error no constituye en sí mismo una disposición patrimonial, ni una pérdida patrimonial para la víctima.[66] El segundo es la transferencia ilegal de dinero mediante el uso no autorizado de datos (normalmente también como resultado del *phishing*) en el *homebanking* o en otros casos en los que quien sufre el error no es una persona física, sino una "máquina".

III. Propuesta legislativa

Sobre la base de lo expuesto, realizamos tres propuestas para mejorar la actual regulación de los delitos contra la propiedad en la Argentina:

1. Tipificar el "Phishing" como delito autónomo

Debido a la gran cantidad de casos y al daño causado por el *phishing*, es necesario no solo castigar adecuadamente estos actos, sino también tipificarlos de un modo justo.[67] Por ello, proponemos la creación de un tipo penal específico, de modo que estos actos tengan un significado propio en la práctica judicial argentina y se refuerce adecuadamente la protección de las víctimas de estos delitos. La idea sería crear un llamado "delito de emprendimiento",[68] en el sentido de que ya el hecho de tratar de inducir a otro a revelar datos personales, con el fin de perjudicarlo patrimonialmente, sea punible. De este modo, no habría que esperar a que la víctima por error divulgue sus datos para que esté ya configurado el delito, lo que permitiría castigar ya la fase preparatoria según la escala penal de los delitos consumados. Específicamente, proponemos que se incluya el siguiente delito en un segundo párrafo del artículo 173, inciso 16 del Código Penal argentino, como complemento del delito de fraude informático:[69]

---

[66] Al parecer llega a una conclusión similar Moyano, Lucas, *Ciberdelitos*, Buenos Aires, Hammurabi, 2024, pp. 117 s., quien considera al phishing como una acción no tipificada.

[67] Hilgendorf, *Deutscher Bundestag*, p. 1 (10).

[68] Sobre esta clase de delitos Kindhäuser, Urs/Hilgendorf, Eric, *Código Penal alemán,* t. 1, Buenos Aires, Hammurabi, 2023, Comentario previo al § 13 n.º m. 261 ss.

[69] Esta propuesta fue presentada oportunamente por Eric Hilgendorf al Parlamento alemán (Hilgendorf, *Deutscher Bundestag*, p. 1 [11]). El texto de la propuesta original es el siguiente: "Wer es in der Absicht, einem anderen Nachteil zuzufügen, unternimmt, in den Kommunikationsdiensten des Internets den Empfänger durch unzutreffende Angaben zur Preisgabe von Passwörtern oder anderer Zugangsdaten zu

"El que, con intención de perjudicar a otro, emprendiere la inducción al destinatario a revelar contraseñas u otros datos de acceso en comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, proporcionándole información falsa o mediante cualquier otro engaño, será reprimido con prisión de un mes a tres años".

Se trata de un delito de peligro abstracto, en el sentido de que basta con llevar a cabo la acción de *phishing* y no es necesario que la víctima tenga que facilitar sus datos ni sufrir ningún tipo de perjuicio patrimonial. De esta forma, este tipo de conductas se convierten en delictivas y perseguibles desde un primer momento. Téngase en cuenta que la conducta de brindarle información falsa a una persona, o tratar de engañarla, para obtener acceso a sus datos personales todavía no configurará una tentativa de estafa en la mayor parte de los casos, en la medida de que todavía hacen falta varios actos para cumplir con el primer elemento de la estafa: el engaño. Por lo demás, la consideración de estos casos como estafa es dudosa, en la medida de que el engañado no es quien realiza la disposición patrimonial, al menos por regla general. La idea de este delito autónomo de "phishing" es, entonces, la de abarcar estos actos preparatorios de estafas posteriores o, en caso de que no se trate de posibles casos de estafa en sentido estricto, de enriquecimientos sin causa. Por esta razón, la pena es menor que para otras clases de estafa. En el caso de que el autor termine perjudicando patrimonialmente a la víctima, existirá la posibilidad de castigar el fraude informático, especialmente si se cumple la segunda propuesta legislativa, que se abordará de inmediato.

2. Reforma del delito de fraude informático

Para cubrir adecuadamente los casos de uso no autorizado de los sistemas de *homebanking* (por ejemplo, transferencia no consentida de activos), no es necesario introducir grandes cambios en la normativa. En este sentido, la creación de nuevos tipos penales extremadamente detallados (como se hizo en España con el artículo 249 del Código Penal Español[70]) no parece aconsejable, ya que un exceso de regulación crea el

bewegen, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist".

[70] El texto español es el siguiente:

"1. También se consideran reos de estafa y serán castigados con la pena de prisión de seis meses a tres años: a) Los que, con ánimo de lucro, obstaculizando o interfiriendo indebidamente en el funcionamiento de un sistema de información o introduciendo, alterando, borrando, transmitiendo o suprimiendo indebidamente datos informáticos o valiéndose de cualquier otra manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

riesgo de que la legislación quede rápidamente obsoleta. Además, la regulación por medio de ejemplos es incompatible con un derecho penal que tienda a la simplicidad, de modo tal que los ciudadanos puedan comprender cuáles son las conductas permitidas o prohibidas si lo deseasen, incluso con un mínimo de asesoramiento jurídico. Por consiguiente, la inclusión de una variante penal del uso no autorizado de datos en el delito de fraude informático sería suficiente para cubrir estos casos.
En definitiva, recomendamos la modificación del artículo 173, inciso 16, Código Penal argentino, que quedaría redactado de la siguiente manera:

"Artículo 173.- No obstante lo dispuesto con carácter general en el artículo anterior, se tendrán en cuenta los casos especiales de estafa, a los que se impondrá la misma pena que en el artículo 172.
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, **o mediante el uso no autorizado de sus datos**".

De esta forma, la utilización de datos obtenidos a través de *phishing* u otros medios en un sistema automatizado para causar un perjuicio económico queda adecuadamente cubierta por el tipo penal de fraude informático y recibe una pena adecuada: superior a la del delito de *phishing* y equivalente a la de cualquier estafa simple del artículo 172. Esta adición al artículo 173 inciso 16 del Código Penal argentino ya ha sido propuesta en la Argentina por José Béguelin y Lola de Tezanos Pinto en un reciente estudio,[71] por lo que tiene una sólida base teórica.

3. Criminalización de la preparación del fraude informático

b) Los que, utilizando de forma fraudulenta tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.
2. Con la misma pena prevista en el apartado anterior serán castigados:
a) Los que fabricaren, importaren, obtuvieren, poseyeren, transportaren, comerciaren o de otro modo facilitaren a terceros dispositivos, instrumentos o datos o programas informáticos, o cualquier otro medio diseñado o adaptado específicamente para la comisión de las estafas previstas en este artículo.
b) Los que, para su utilización fraudulenta, sustraigan, se apropiaren o adquieran de forma ilícita tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo.
3. Se impondrá la pena en su mitad inferior a los que, para su utilización fraudulenta y sabiendo que fueron obtenidos ilícitamente, posean, adquieran, transfieran, distribuyan o pongan a disposición de terceros tarjetas de crédito o débito, cheques de viaje o cualesquiera otros instrumentos de pago materiales o inmateriales distintos del efectivo".
[71] Béguelin/de Tezanos Pinto, *Compendio de jurisprudencia*, p. 327 (353).

Es bien sabido que muchos casos de fraude informático se quedan en la fase preparatoria. Pensemos, por ejemplo, en la creación o distribución fallida de *malware*, o incluso los ya mencionados casos de *phishing*. Aunque estos últimos merecen ser penalizados de forma autónoma, por su significado social especialmente importante, también puede ser necesario criminalizar otros actos preparatorios potencialmente perjudiciales con el fin de proteger al público en general de la criminalidad informática. Esto es lo que ocurrió en Alemania ya en 2003,[72] cuando los actos preparatorios del fraude informático se tipificaron en el § 263a, párr. 3, StGB:[73]

"Quien prepare un hecho punible según el párrafo 1 al elaborar, procurarse o procurarle a un tercero, poner en venta, conservar o entregarle a un tercero un programa de computación cuyo fin sea la comisión de un hecho de esa clase será castigado con una pena privativa de la libertad de hasta tres años o con pena de multa".

Según este delito de peligro abstracto, puede ser castigado quien prepare un fraude informático creando programas informáticos con el fin de cometer dicho delito, adquiriéndolos para sí mismo o para otra persona, guardándolos para la venta, almacenándolos o dejándoselos a otra persona. Este delito se basa en las disposiciones de la Decisión Marco del Consejo de la Unión Europea, del 28 de mayo de 2001, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo. El objetivo[74] de la Decisión Marco es garantizar la persecución del fraude y la falsificación de todas las formas de medios de pago distintos del efectivo en todos los Estados miembros de la Unión Europea.[75] Además, la normativa alemana ha sido intensamente estudiada y sometida a diversos procesos de evaluación legislativa. Por lo tanto, esta disposición alemana puede considerarse un buen ejemplo para una reforma legislativa, que además tenga como base las disposiciones internacionales sobre criminalidad informática.

Sobre esta base, se propone añadir el siguiente párrafo al delito de fraude informático:

---

[72] En detalle Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 334.
[73] Se utiliza la traducción de Marcelo Sancinetti, Fernando Córdoba, Marcelo Lerman y Leandro Dias disponible en: Hilgendorf, Eric/Valerius, Brian, *Derecho Penal. Parte Especial*, t. 2, 2.ª ed., Buenos Aires, Ad-Hoc, 2024, § 8.
[74] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 334
[75] Decisión marco del Consejo, de 28 de mayo de 2001, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo, 2001/413/JAI, 28 de mayo de 2001, Diario Oficial n° L 149 de 02/06/2001 pp. 0001-0004.

"El que prepare un delito según el primer párrafo de este inciso al elaborar, procurarse o procurarle a un tercero, poner en venta, conservar o entregarle a un tercero un programa de computación cuyo fin sea la comisión de un delito de esa clase será reprimido con pena de prisión de un mes a tres años".

4. Excursus: ¿Es necesario un tipo penal de "hurto informático"?

En los últimos años se discutió en la Argentina la posibilidad de incorporar un delito de "hurto informático", entendido como la copia o sustracción de información con valor comercial contenida en dispositivos o sistemas informáticos ajenos.[76] En particular, el último Proyecto de Código Penal[77] establecía lo siguiente:

"ARTÍCULO 499.- Se impondrá prisión de UN (1) mes a DOS (2) años, al que, violando medidas de seguridad, ilegítimamente se apoderare o copiare información contenida en dispositivos o sistemas informáticos ajenos que no esté disponible públicamente y que tengan valor comercial para su titular o para terceros".

Consideramos que no es conveniente la creación de esta clase de delito. El tipo penal de hurto se encuentra estrechamente vinculado a la protección de la tenencia o custodia de una cosa mueble y es una de las bases de la protección penal del patrimonio.[78] El contenido de ilícito de un hurto se encuentra vinculado a la sustracción,[79] con ánimo de apropiación, de una cosa total o parcialmente ajena, a la que la víctima en principio no volverá a tener acceso, salvo que pueda recuperarla de alguna forma. En el "hurto informático", salvo que se borre la información, la víctima sigue contando con los datos "hurtados", por lo que el contenido de ilicitud es diferente. No se trata, en ese sentido, de un delito patrimonial o un delito contra la custodia o tenencia de una cosa, sino que se trata más bien de una infracción a la intimidad de la víctima, a cuyos datos ha accedido alguien que no tenía autorización para hacerlo. Por lo tanto, esta clase de comportamientos más bien han de ser regulados como delitos contra la intimidad o, dado el caso, como delitos contra derechos de propiedad intelectual, y no como delitos

[76] Solo a modo de ejemplo, véase Moyano, *Ciberdelitos*, pp. 119 s.
[77] Senado de Argentina, Número de Expediente 52/19, MEN-2019-60-APN-PTE, 25 de marzo de 2019, disponible en: https://www.senado.gob.ar/parlamentario/comisiones/verExp/52.19/PE/PL [último acceso: 15/03/2025].
[78] Hilgendorf/Valerius, *Derecho Penal. Parte Especial*, t. 2, § 2 n.º m. 1 ss.
[79] En detalle sobre esta cuestión Dias, Leandro, "El ánimo de apropiación como elemento del delito de hurto", *Lecciones y Ensayos* 98 (2017), 135 (153 ss.).

patrimoniales. Por lo demás, la creación de un "hurto informático", en la que el concepto de custodia aparece diluido, solo puede generar confusiones en este contexto.

IV. Propuesta final

En síntesis, nuestra propuesta de modificación legislativa de la protección penal del patrimonio en casos de ciberdelitos consiste en una triple modificación del artículo 173, inciso 16 del Código Penal argentino. En primer lugar, proponemos el agregado de un delito de peligro abstracto para criminalizar el *phishing* como tal. En segundo lugar, sugerimos que se incluya la variante de "uso no autorizado de datos" en el delito de defraudación informática. En tercer lugar, proponemos la creación de un delito de peligro abstracto para tipificar la preparación del fraude informático. La redacción final es la siguiente:

"ARTICULO 173.- No obstante lo dispuesto con carácter general en el artículo anterior, se tendrán en cuenta los casos especiales de estafa, a los que se impondrá la misma pena que en el artículo 172.

[…]

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, **o mediante el uso no autorizado de sus datos.**

El que, con intención de perjudicar a otro, emprendiere la inducción al destinatario a revelar contraseñas u otros datos de acceso en comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, proporcionándole información falsa o mediante cualquier otro engaño, será reprimido con prisión de un mes a tres años.

El que prepare un delito según el primer párrafo de este inciso al elaborar, procurarse o procurarle a un tercero, poner en venta, conservar o entregarle a un tercero un programa de computación cuyo fin sea la comisión de un delito de esa clase será reprimido con prisión de un mes a tres años".

Reforma sobre la criminalidad informática en la Argentina (3). Delitos contra la libertad sexual

Eric Hilgendorf y Leandro Dias

I. Introducción

En esta tercera sesión, debatiremos algunos de los temas más problemáticos y controvertidos de una posible reforma de los delitos informáticos: los delitos contra la libertad sexual. Esta cuestión es problemática porque la criminalización general del sexo es un tema muy debatido en la actualidad.[1] No es ninguna novedad que en los últimos años han surgido nuevos modelos de regulación de los delitos sexuales.[2] Al mismo tiempo, la moral sexual es muy sensible a las particularidades de cada sociedad.[3] Mientras que ciertos comportamientos incorrectos pueden considerarse universalmente intolerables, como la violación, otros dependen en gran medida de lo que la sociedad esté dispuesta a tolerar, como en el caso de la tenencia de ciertos materiales pornográficos.[4] Así, la criminalización de las conductas sexuales incorrectas cometidas en el ciberespacio depende fundamentalmente de decisiones legislativas generales sobre la criminalización de lo sexual. En esta breve conferencia, por consiguiente, limitaremos nuestras consideraciones a varios hechos graves que son impunes en la Argentina y merecen una regulación penal. Por supuesto, sería posible criminalizar más conductas, dependiendo de las necesidades de prevención de una sociedad y de las consideraciones de política criminal que el legislador estime oportunas. Hoy, sin embargo, haremos una propuesta que podría implementarse aun si el legislador decide mantener la actual regulación argentina de los delitos sexuales y otros delitos vinculados. Debido a estas limitaciones, algunos tipos penales que propondremos no serán, en sentido estricto, delitos contra la libertad sexual, sino contra el honor o contra la intimidad. No obstante, el hilo conductor de esta conferencia serán los delitos sexuales cometidos en el ciberespacio.

[1] Al respecto, recientemente Green, Stuart, *La criminalización del sexo*. *Una teoría liberal unificada*, Madrid, Marcial Pons, 2024, passim.
[2] Para un panorama, véase Hörnle, Tatjana, "Violación como relaciones sexuales no consentidas", *En Letra: Derecho Penal* 10 (2020), 197 (201 ss.).
[3] Sobre la cuestión de la contingencia incluso en el delito de violación (por ejemplo, si la violación en sentido estricto requiere penetración de un varón o no parecería depender de consideraciones sociales que pueden variar), véase Gardner, John, *Ofensas y defensas*, Madrid, Marcial Pons, 2012, pp. 43 ss.
[4] Al respecto Green, Stuart, "Sexual Offences", en Caeiro/Gless/Mitsilegas (eds.), *Elgar Encyclopedia of Crime and Criminal Justice*, vol. 4, Cheltenham, Elgar Publishing, 2024, p. 447 (456).

También hay que señalar que el derecho penal debe seguir siendo la *ultima ratio* de la intervención estatal.[5] Si hay otras formas más indulgentes de realizar los objetivos legítimos que el Estado quiere lograr mediante la criminalización, entonces esas alternativas deben ser preferidas, y la criminalización debe ser descartada.[6] Por este motivo, intentaremos ofrecer una criminalización sobria del comportamiento sexual incorrecto, aunque, por supuesto, existan formas más expansivas de criminalización todavía defendibles. Este enfoque prudente o parsimonioso se verá, por ejemplo, en la propuesta de criminalizar los *deepfakes* sexuales: aunque puede haber razones para castigar la mera posesión o creación de al menos ciertos tipos de *deepfakes* sexuales, nos centraremos únicamente en la publicación y difusión de este tipo de contenidos. No estamos seguros de si la criminalización de la mera posesión (o creación) conllevará una mejora en la prevención o si los derechos de las víctimas mejorarán sustancialmente con una criminalización exhaustiva de esa clase de conductas. Y si existen estas dudas, entonces hay buenas razones para que prevalezca la prudencia.[7] Si en el futuro el legislador, y la sociedad en su conjunto, consideran oportuno ampliar nuestra propuesta de criminalización, con otros argumentos, entonces las cosas pueden cambiar. Esto es, de hecho, lo que ha sucedido en la Argentina con la criminalización de conductas vinculadas a la pornografía ilícita que tiene por objeto a menores de edad, que fueron criminalizadas, en líneas generales, primero en su faceta de difusión, y luego se amplió la criminalización para abarcar también la tenencia simple.[8]

Comoquiera que fuese, analizaremos tres grupos principales de casos de ciberdelincuencia que son especialmente relevantes para la práctica judicial y la vida cotidiana. El primero es el llamado "abuso sexual a distancia", es decir, los casos en los que una persona obliga a otra a realizar actos sexuales desde un lugar distante, por ejemplo, a través de la emisión en directo de una *webcam* y de un programa de *streaming* de video en directo (sección II). El segundo es la llamada "pornovenganza": la difusión

[5] Véase Hilgendorf, Eric, "Strafrecht im Kontext der Normenordnungen", en Hilgendof/Kudlich/Valerius (eds.), *Handbuch des Strafrechts*, t. 1, Heidelberg, C.F. Müller, 2019, § 1 n.º m. 2.

[6] Sobre los fundamentos constitucionales de esta manifestación del principio de *ultima ratio*, a partir del llamado test de proporcionalidad Schmahl, Eric, "Verfassungsrechtliche Vorgaben für das Strafrecht", en Hilgendof/Kudlich/Valerius (eds.), *Handbuch des Strafrechts*, t. 1, Heidelberg, C.F. Müller, 2019, § 2 n.º m. 15.

[7] Para un panorama detallado de cómo la incertidumbre moral puede repercutir en la criminalización de conductas potencialmente incorrectas Barry, Christian/Tomlin, Patrick, "Moral Uncertainty and the Criminal Law", en Alexander/Ferzan (eds.), *The Palgrave Handbook of Applied Ethics and the Criminal Law*, Cham, Palgrave Macmillan, 2019, p. 445 (455 ss.).

[8] En detalle Aboso, Gustavo, *Delito de distribución de pornografía infantil en la era digital*, Buenos Aires, Hammurabi, 2021, pp. 21 ss.

no autorizada de contenidos audiovisuales de carácter sexual (sección III). El tercero es la creación de imágenes sexuales falsas ("*deepfakes*") utilizando inteligencia artificial (sección IV). Por último, ofreceremos un resumen de la propuesta (sección V).

Pero antes es necesario decir algo sobre el tratamiento argentino de dos "delitos informáticos" usuales. El primero es el llamado "*cyber-grooming*": contactar por medios telemáticos a una persona menor de edad para ganarse su confianza y eventualmente cometer delitos sexuales contra ella. El delito de *cyber-grooming* del artículo 131 del Código Penal argentino cubre ampliamente este tipo de casos al tipificar los actos preparatorios pertinentes. Una criminalización más amplia es una cuestión que debe decidir el legislador.[9] Sin embargo, dado que hay un grupo de expertos trabajando en una reforma general de la parte especial del Código Penal, no exploraremos esta alternativa.

Lo mismo debe decirse de los delitos de pornografía ilícita. En el artículo 128, el legislador argentino ha decidido penalizar la diseminación y posesión de pornografía que tenga por objeto a menores de edad, y la cuestión de si esto incluye también los casos de pornografía "simulada" (realizada por mayores de edad que se hacen pasar por menores) en principio está excluida del alcance del tipo penal, a menos que se recurra a alguna clase de interpretación extensiva.[10] Por supuesto, es posible limitar o ampliar la tipificación de los delitos de pornografía. Pero, una vez más, esas decisiones le corresponden al legislador argentino, y eventualmente a los jueces que consideren adecuado un desarrollo progresivo del derecho, y no es realmente una cuestión específica de la criminalidad informática, sino de los límites de los comportamientos vinculados a la sexualidad que la sociedad está dispuesta a permitir o tolerar. Dejamos estas cuestiones abiertas para que el grupo de trabajo pertinente pueda dar su opinión al respecto.

II. Violación sin contacto físico con la víctima ("a distancia")

La llamada "violación por internet" o, más claramente, "violación a distancia" es objeto de debate desde una sentencia del Tribunal Correccional de Bruselas de 25 de septiembre de 2018.[11] En este caso concreto, un hombre obligó a una adolescente mediante una

[9] Véase Aboso, Gustavo, *Delito de distribución de pornografía infantil en la era digital*, pp. 131 ss.
[10] Sobre la propuesta del último proyecto de reforma, que amplía la punibilidad del delito de *grooming*, véase (de forma parcialmente aprobatoria) Neme, Catalina, "'Grooming': ciberacoso sexual infantil", en Dupuy (dir.), *Acosos en la red a niños, niñas y adolescentes*, Buenos Aires, Hammurabi, 2022, p. 103 (136 ss.). Véase también Aboso, Gustavo, *Delitos sexuales*, Buenos Aires, Hammurabi, 2025, pp. 244 ss.
[11] Al respecto Hope, Alan, "Five years in jail for 'rape at a distance' for online abuser", en *The Brussels Times*, 26/09/2018, disponible en https://www.brusselstimes.com/all-news/belgium-all-news/justice-belgium/50940/five-years-in-jail-for-rape-at-a-distance-for-online-abuser [último acceso: 15/03/2025].

coacción a realizar una práctica de automasturbación, incluida una autopenetración. El Tribunal Correccional condenó al autor por violación, aunque no hubo contacto físico entre él y la víctima.[12]

En la Argentina también es discutible si estos casos pueden considerarse violación o, al menos, abuso sexual.[13] La respuesta no es fácil debido a la forma en que están tipificados los delitos de abuso sexual (delito básico) y violación (agravante) en el artículo 119 del Código Penal argentino. La conducta ilícita básica, el "abuso sexual" (artículo 119, párrafo 1), puede interpretarse, por supuesto, en el sentido de que no sería necesario contacto físico del autor con la víctima.[14] Sin embargo, este tipo de interpretación tiene el problema de hacer que el delito de exhibiciones obscenas resulte en cierto modo redundante: si *no* se requiere contacto físico con la víctima para cometer abuso sexual, no está claro por qué sería necesario el delito específico de exhibiciones obscenas, que de hecho existe en el artículo 129.[15] Este artículo establece lo siguiente "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".[16] Dado que forzar a otra persona a observar actos sexuales puede considerarse también una forma de "abuso sexual", deja de ser necesario que exista un delito específico de exhibiciones obscenas, al menos si se considera este delito como autónomo. El delito de exhibiciones obscenas sería entonces una forma atenuada de abuso sexual, interpretación que nada tiene que ver con la sistemática de la regulación actual de los delitos sexuales en la Argentina.[17]

---

[12] En detalle sobre este caso Aboso, Gustavo, "Violación mediante Internet", en Aboso (ed.), *Ciberdelitos*, Buenos Aires, El Dial, 2022, p. 245 (245 ss.).

[13] Cf. Aboso, *Ciberdelitos*, p. 245 (247 s.).

[14] Así, por ejemplo, Aboso, *Ciberdelitos*, p. 245 (247 s.); De la Fuente, Javier, *Abusos sexuales*, Buenos Aires, Hammurabi, 2021, pp. 55 s.; Wacker Schroder, Federico, en: Simaz (dir.), *Manual de Derecho Penal. Parte Especial*, 2.ª ed., 2024, p. 71 (73); ambiguos De Luca, Javier/López Casariego, Julio, *Delitos contra la integridad sexual*, Buenos Aires, Hammurabi, 2009, pp. 50 s.; en contra, por ejemplo, Figari, Rubén, *Delitos sexuales*, 2.ª ed., Buenos Aires, Hammurabi, 2020, p. 50; Molina, Gonzalo, *Manual de Derecho Penal. Parte Especial*, Resistencia, ConTexto, 2021, p. 277, quien sin embargo considera que siempre es necesario que haya contacto entre dos personas, por lo que quedaría fuera del tipo el caso de auto-masturbación aparentemente.

[15] Reconoce esta cuestión, pero concluye que obligar a la víctima a realizarse actos sexuales a sí misma es un abuso De la Fuente, *Abusos sexuales*, pp. 54 ss.

[16] La agravante del segundo párrafo ("[s]i 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") puede ser dejada de lado aquí, ya que no incide en el argumento que estamos discutiendo.

[17] Lo que no significa que la regulación actual del delito de exhibiciones obscenas sea adecuada. De hecho, la discusión reciente sobre el tema a nivel internacional ha sido poco tenida en cuenta hasta ahora en Argentina. Al respecto solamente Green, *La criminalización del sexo*, pp. 291 ss.

Las cosas se ponen más difíciles cuando se trata de considerar estos casos de violación a distancia como casos de violación, según el artículo 119, párrafo 3, del Código Penal, incluso asumiendo que puede haber abusos sexuales sin contacto directo entre autor y víctima. *De lege lata* no es fácil ofrecer una solución para estos casos, ya que algunos comentaristas dicen que no hay penetración ("acceso carnal") sin algún tipo de contacto sexual *directo* entre la víctima y un tercero.[18] Si se sigue esta interpretación, lo más probable es que este comportamiento no se considere violación en la Argentina, contrariamente a lo que decidió el Tribunal Correccional de Bruselas. Por supuesto, estos casos podrían ser castigados como coacción, o incluso como privación de la libertad. Pero criminalizarlos sistemáticamente como verdaderos casos de violación requeriría una reforma de la ley, al menos según esta interpretación que brindan algunos comentaristas. Así, sería necesaria la creación de un delito autónomo, como el delito de abuso sexual contra menores sin contacto físico, del Código Penal alemán (§ 176a, StGB)[19] o, al menos, que en el art. 119, párrafo 2, del Código Penal argentino se agregara, donde la ley dice "introduciendo objetos", la siguiente frase: "o haciendo introducir por la víctima o un tercero…".[20]

No estamos de acuerdo con la interpretación de la disposición sobre abuso sexual y de violación que han hecho algunos comentaristas en relación con los casos de violación a distancia. Si algunos casos son tan horribles que parecen merecer el mismo castigo que una violación (como el caso de Bruselas), es porque pueden ser *violaciones reales* y no algún tipo de "violación a distancia". Es posible asumir, solo a los fines de la argumentación, que el tipo base de abuso sexual requiere alguna clase de contacto corporal entre el autor (o autores) y la víctima. Y es cierto que el delito de violación en la

[18] Así, al parecer, Aboso, *Delitos sexuales*, pp. 145 ss.; Wacker Schroder, *Manual de Derecho Penal. Parte Especial*, p. 71 (79 s.). En contra De la Fuente, *Abusos sexuales*, p. 150.

[19] "§ 176a. Abuso sexual de niños sin contacto físico con el niño
1) Será penado con pena privativa de libertad de seis meses a diez años quien:
1. realice actos sexuales delante de un niño o deje que tales actos sean realizados delante de un niño por una tercera persona,
2. determine a un niño a que realice actos sexuales, en tanto el hecho no esté conminado con pena según el § 176, párrafo 1, número 1 o número 2, o bien
3. incida en un niño mediante un contenido pornográfico (§ 11, párrafo 3) o mediante dichos equivalentes.
2) De igual modo será penado quien ofrezca un niño o prometa conseguir datos de contacto de un niño para cometer un hecho del párrafo 1, número 1, o quien se ponga de acuerdo con otro para cometer tal hecho.
3) La tentativa es punible en los casos del párrafo 1, números 1 y 2. En caso de hechos del párrafo 1, número 3, la tentativa es punible en aquellos casos en los cuales la consumación del hecho fracasa tan sólo porque el autor cree erróneamente que su incidencia recae en un niño" (traducción de Marcelo Sancinetti y Lucila Tuñón).

[20] Le agradecemos a Marcelo Sancinetti por esta propuesta de reforma legislativa minimalista que, por lo demás, consideramos adecuada.

Argentina requiere algún tipo de penetración. No obstante, hoy en día esa penetración no se limita a la penetración de órgano viril, es decir, del pene, sino que basta con la introducción de cualquier objeto. Incluso la introducción de objetos o partes del cuerpo en la vagina o el ano de la víctima es suficiente. Esto es una prueba de que el delito de violación *no es un delito de propia mano*.[21] Si esto es así, entonces al menos algunos casos de violación a distancia (y lo mismo sucede en casos de abuso sexual simple o gravemente ultrajante) podrían considerarse violación cometida por autoría mediata: la víctima coaccionada actúa como instrumento del autor, que utiliza el propio cuerpo de la víctima para lograr el acceso carnal.[22] No creemos que una interpretación así viole la prohibición de recurrir a razonamientos analógicos, ya que el término "acceso carnal" también puede implicar un auto-acceso carnal, si esa clase de comportamiento de la víctima fue controlado por el autor. Además, recuérdese otra vez que el delito de violación en Argentina ya no requiere acceso carnal en sentido estricto (es decir, con el pene), sino "actos análogos" de introducción de objetos o partes del cuerpo por vía anal o vaginal. Una auto-masturbación controlada por coacción sin dudas encuadra en este supuesto, a través de autoría mediata. Si esto ya regiría para casos de violación (artículo 119, tercer párrafo, Código Penal), con mayor razón debería regir para abusos sexuales simples (artículo 119, primer párrafo, Código penal).[23] Así, si el autor obligase a la víctima a realizarse "tocamientos a distancia", por ejemplo, a través de coacción, estaría realizando también un abuso sexual en autoría mediata.[24]

La crítica a la que ya se hizo mención respecto de la sistemática de los delitos sexuales en la Argentina y su relación con el delito de exhibiciones obscenas puede ser atendida del siguiente modo: esta interpretación sigue requiriendo que el abuso sexual tenga lugar mediante contacto corporal entre autor y víctima. No obstante, debido a que los delitos

[21] Esta parece ser la dominante usual en Argentina actualmente. Al respecto, véase Aboso, *Delitos sexuales*, p. 151; De Luca/López Casariego, *Delitos contra la integridad sexual*, p. 76 ss.; Molina, *Manual de Derecho Penal. Parte Especial*, p. 28 s. Para un tratamiento cuasi-monográfico, recientemente Guerrero, Ignacio, "La autoría en el delito de violación", Tesis inédita de maestría de la Universidad Torcuato Di Tella, 2024. La situación en Alemania es exactamente la misma. Al respecto Hörnle, Tatjana, en: *Leipziger Kommentar zum Strafgesetzbuch*, 13.ª ed, Berlín, Walter de Gruyter, 2023, § 177 n.º m. 117; Renzikowski, Joachim, en: *Münchener Kommentar zum Strafgesetzbuch*, 4.ª ed, Múnich, C.H. Beck, 2021, § 177 n.º m. 182

[22] Sobre la posibilidad general de autoría mediata en el delito de violación Hörnle, en: *Leipziger Kommentar zum Strafgesetzbuch*, § 177 n.º m. 247.

[23] Similar, respecto de la discusión alemana Hörnle, en: *Leipziger Kommentar zum Strafgesetzbuch*, § 177 n.º m. 117.

[24] Respecto de la categoría de autoría mediata de utilización, por medio de dominio de coacción, de la propia víctima como instrumento, véase Roxin, Claus, "Mittelbare Täterschaft", en Hilgendorf/Kudlich/Valerius (eds.), *Handbuch des Strafrechts*, t. 3, Heidelberg, C.F. Müller, 2021, § 52 n.º m. 46 ss.

de abuso sexual pueden ser cometidos por autoría mediata, en ciertos casos la acción realizada por la propia víctima le será atribuida al autor como propia.[25] Por tanto, en casos de abuso sexual "a distancia" es el propio autor el que realiza el abuso, ya que controla el cuerpo de la víctima como si fuese propio.[26] No se trata, ni más ni menos, que de la aplicación de las reglas generales de la autoría mediata.

Por lo tanto, no creemos que sea estrictamente necesario cambiar la ley argentina de violación para castigar los casos de violación a distancia, ni creemos que sea prudente reformar toda la regulación de los delitos sexuales a través de una reforma sobre delitos informáticos. Crear nuevos delitos para castigar conductas que pueden castigarse fácilmente interpretando las leyes correspondientes no es una buena idea, a menos que haya una necesidad imperiosa en la praxis de clarificar la cuestión (lo que no se observa aquí). También es necesario evitar la sobrerregulación que se produciría si se creasen reglas penales redundantes de forma apresurada cada vez que un nuevo caso de amplia repercusión aparece en los titulares de los diarios o en las redes sociales.[27] En cualquier caso, una reforma integral de los delitos sexuales debería tener en cuenta la problemática de los abusos sexuales a distancia y, al mismo tiempo, crear delitos generales, sin necesidad de regular cada caso de conducta ilícita como un delito autónomo.

III. La llamada "pornovenganza"

Otro grupo de casos que ha causado mucha preocupación en la Argentina es el de la "pornovenganza".[28] En estos casos, una pareja graba fotos, audios o vídeos de actos sexuales entre ellos de forma consentida o uno de los *partners* le envía al otro imágenes íntimas de forma consentida, pero sin autorización para su difusión ulterior.[29] Luego, generalmente una vez terminada la relación, uno de los miembros de la pareja difunde las imágenes, audios o videos para dañar la reputación del otro o por alguna otra razón. Otra

[25] Hörnle, en: *Leipziger Kommentar zum Strafgesetzbuch*, § 177 n.º m. 118.
[26] Así también Renzikowski, en: *Münchener Kommentar zum Strafgesetzbuch*, § 177 n.º m. 34. La jurisprudencia alemana ha avalado esta interpretación respecto del delito de violación, pero sin recurrir a las reglas de la autoría mediata: BGH, NStZ-RR, 2020, 276 (277),
[27] Para una crítica a esta forma de proceder respecto de los delitos sexuales Hörnle, Tatjana, "The New German Law on Sexual Assault and Sexual Harrassment", *German Law Journal* 18 (2017), 1310 (1315 s.).
[28] Para un panorama de la problemática global, véase Franks, Mary Anne, "The Crime of 'Revenge Porn'", en Alexander/Ferzan (eds.), *The Palgrave Handbook of Applied Ethics and the Criminal Law*, Cham, Palgrave Macmillan, 2019, p. 661 (663 ss.). Objeciones a esta terminología en Moyano, Lucas, *Ciberdelitos*, Buenos Aires, Hammurabi, 2024, pp. 111 ss.
[29] Dupuy, Daniela, "Difusión no consentida de imágenes y grabaciones íntimas", en Dupuy (dir.), *Acosos en la red a mujeres*, Buenos Aires, Hammurabi, 2023, p. 98 (134); sobre la cuestión básica de la ausencia de consentimiento como núcleo de este delito Franks, *The Palgrave Handbook of Applied Ethics and the Criminal Law*, p. 661 (663 s.).

forma de pornovenganza tiene lugar incluso sin el consentimiento real de uno de los *partners*, mientras el otro graba el contenido audiovisual. Estas conductas son prácticamente impunes en la Argentina, ya que tanto la grabación de imágenes sin consentimiento como la difusión no consentida de imágenes grabadas con consentimiento no están criminalizadas.[30] Solo el artículo 155 del Código Penal, que castiga la publicación de "comunicaciones electrónicas" no destinadas a la publicidad cuando eso pudiere perjudicar a terceros con una pena simbólica de 100.000 pesos (menos de 100 dólares al momento de escribir estas líneas), podría ser aplicable en ciertos casos en los que las imágenes hubiesen sido enviadas de un *partner* al otro de modo tal que pudiese hablarse de una comunicación electrónica.[31] Solo algunas jurisdicciones locales argentinas sancionan parcialmente este tipo de conductas como contravención, como la Ciudad Autónoma de Buenos Aires (artículo 75 del Código Contravencional).[32]

Sobre esta cuestión, lo primero que debe decirse es que la pornovenganza es solo un ejemplo particularmente extremo de conducta ilícita que actualmente queda impune en la Argentina: la grabación no autorizada de contenido audiovisual de terceros o su eventual difusión, también no autorizada.[33] En este sentido, la protección penal de la intimidad en la Argentina es inadecuada, especialmente en una era en la que las imágenes pueden difundirse en cuestión de segundos a través de Internet y las redes sociales, a pesar de que las víctimas no deseen verse sometidas a esa exposición.[34] Por lo tanto, una solución adecuada al problema de la pornovenganza requiere dos pasos. El primer paso sería el de

---

[30] Al respecto Aboso, Gustavo, "El resguardo de la intimidad en la sociedad de la información y el delito de 'pornovenganza' ('sexting' o 'non-consensual pornography')", en Riquert (dir.), *Sistema penal e informática*, t. 3, Buenos Aires, Hammurabi, 2020, p. 255 (270 ss.). Véase también Dupuy, *Acosos en la red a mujeres*, p. 98 (134 ss.).

[31] Sobre la diferenciación entre estas dos formas de conducta, ambas merecedoras de castigo, Aboso, *Sistema penal e informática*, t. 3, p. 255 (257 s.)

[32] "Artículo 75 - *Difusión no autorizada de imágenes o grabaciones íntimas*.- Quien difunda, publique, distribuya, facilite, ceda y/o entregue a terceros imágenes, grabaciones y/o filmaciones de carácter íntimo sin el consentimiento de la persona y a través de cualquier tipo de comunicación electrónica, de transmisión de datos, páginas web y/o a través de cualquier otro medio de comunicación, siempre que el hecho no constituya delito, es sancionado con una multa de cuatrocientas (400) a mil novecientas cincuenta (1950) unidades fijas o cinco (5) a quince (15) días de trabajo de utilidad pública o con tres (3) a diez (10) días de arresto. El consentimiento de la víctima para la difusión, siendo menor de 18 años, no será considerado válido.
Tampoco podrá alegarse el consentimiento de la víctima en la generación del contenido como defensa a la realización de la presente conducta.
Acción dependiente de instancia privada con excepción de los casos donde la víctima sea menor de 18 años de edad.
No configura contravención el ejercicio del derecho a la libertad de expresión".

[33] Véase, en detalle, Hilgendorf, Eric/Valerius, Brian/Kusche, Carsten, *Computer- und Internetstrafrecht,* 3.ª ed., Berlin/Heidelberg, Springer, 2023, § 3 n.º m. 227 ss.

[34] Cf. Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 228.

criminalizar de forma general (es decir, con independencia de que se trate de contenido "íntimo" o sexual) la producción y difusión de imágenes no consentidas, así como la difusión de imágenes consentidas sin autorización de la víctima. Para ello, el legislador argentino debería considerar si es necesario crear un delito similar al § 201a del Código Penal alemán: violación de la intimidad y los derechos personales mediante la toma de fotografías u otras imágenes.[35] Recién el segundo paso debería ser el de agravar la pena en los casos en que la imagen en cuestión sea de naturaleza sexual. De este modo, la toma y difusión no autorizada de imágenes en general quedaría penalizada en la Argentina, con excepciones relacionadas con el ejercicio de determinados derechos y profesiones, como el ejercicio conforme a derecho del periodismo.[36]

En esta breve presentación, no podemos desarrollar los detalles de esta regulación penal de la intimidad, aunque la creación de tales delitos es necesaria para castigar adecuadamente no solo los casos de pornovenganza, sino también todos los ejemplos de violación de la privacidad mediante la producción o difusión no autorizada de imágenes

---

[35] Se utiliza la traducción de Marcelo Sancinetti, Fernando Córdoba, Marcelo Lerman y Leandro Dias disponible en: Hilgendorf, Eric/Valerius, Brian, *Derecho Penal. Parte Especial*, t. 1, Buenos Aires, Ad-Hoc, 2022, § 6 n.º m. 36):
"§ 201a. Violación del ámbito vital altamente personal y de los derechos de la personalidad, mediante tomas de imágenes
1) Será penado con pena privativa de libertad de hasta dos años o con pena de multa quien
1. sin autorización, produzca o transmita la toma de una imagen de otra persona que se halla en una vivienda o en un espacio especialmente protegido de la visual y, por medio de eso, viole el ámbito vital altamente personal de la persona representada,
2. sin autorización, produzca o transmita la toma de una imagen que muestre el desamparo de otra persona y, por medio de ello, viole el ámbito vital altamente personal de la persona representada,
3. sin autorización, produzca o transmita la toma de una imagen que exponga a una persona fallecida, de manera gravemente ofensiva,
4. utilice o haga accesible a una tercera persona la toma de una imagen captada como resultado de un hecho de los números 1 a 3, o
5. haga accesible a una tercera persona, a sabiendas de carecer de autorización, la toma de una imagen de la clase descrita en los números 1 a 3, captada con autorización, y por medio de ello viole el ámbito vital altamente personal de la persona representada.
2) De igual modo será penado quien, sin autorización, haga accesible a una tercera persona la toma de una imagen de otra persona que sea apta para dañar considerablemente la reputación de la persona representada. Esto rige, bajo los mismos presupuestos, también para la toma de una imagen de una persona fallecida.
3) Será penado con pena privativa de libertad de hasta dos años o con pena de multa quien a la toma de una imagen que tenga por objeto la desnudez de otra persona menor de dieciocho años:
1. la produzca u ofrezca obtenerla para una tercera persona, a cambio de remuneración o
2. la obtenga para sí o para una tercera persona, a cambio de remuneración.
4) El párrafo 1, números 2 y 3, también en conexión con el párrafo 1, números 4 o 5, y los párrafos 2 y 3 no rigen respecto de acciones que se lleven a cabo en salvaguarda de intereses legítimos preponderantes, a saber, el arte o la ciencia, la investigación o la enseñanza, la información sobre acontecimientos de actualidad, de historia o fines similares.
5) Los soportes de imágenes, así como los dispositivos de tomas de imágenes u otros medios técnicos utilizados por el autor o el partícipe pueden ser decomisados. Es aplicable el § 74a".

[36] Probablemente en un mismo sentido Aboso, "*Sistema penal e informática*, t. 3, p. 255 (284), al menos en el caso de ciertas fotografías tomadas en un ámbito de intimidad.

a través de Internet. Además, incorporar un tipo penal como el del § 201 del Código Penal implicaría una modificación sustancial de prácticas usuales, que ahora pasarían a ser punibles, así como una reestructuración general del sistema de delitos contra la intimidad. Consideremos que, si bien esa alternativa sería la óptima, una reforma orientada únicamente a la criminalidad informática no puede ir tan lejos. Por el contrario, esa clase de reforma tiene que darse o bien en el marco de un proyecto autónomo sobre el refuerzo de la protección de la intimidad o, mejor, en un proyecto de reforma integral del Código Penal argentino. Con independencia de eso, el fenómeno de la "pornovenganza" es tan grave que debería ser abordado incluso si el legislador argentino no considera necesario reforzar la protección general de la intimidad.

La difusión de imágenes íntimas sin autorización es claramente un acto ilícito porque viola el derecho negativo a la intimidad de la víctima, quien puede decidir libremente quién puede observar las imágenes tomadas con su consentimiento o si quiere someterse a una grabación de imágenes.[37] Eso resulta casi una obviedad. No obstante, también habría buenas razones para penalizar la posesión de estas imágenes. En los últimos años, los filósofos morales Helen Frowe y Jonathan Parry han presentado tres argumentos a favor de la penalización autónoma de la tenencia de imágenes de "pornovenganza", del mismo modo que sucede en el caso de la pornografía infantil.[38] En primer lugar, sostienen que el consumo real de pornografía vengativa *agrava* el daño sufrido por la víctima porque uno de los objetivos de los autores es humillar a sus víctimas y la humillación aumenta a medida que más y más personas ven las imágenes.[39] En segundo lugar, argumentan que la pornovenganza no solo *daña* a las víctimas, sino que también *viola sus derechos* de una manera particular, por encima de la violación al derecho general a la privacidad: las degrada, enviando el mensaje de que son meros objetos sexuales para una audiencia.[40] En tercer lugar, afirman que los consumidores de pornovenganza *facilitan* el daño/violación de derechos sufrida por las víctimas de un modo similar a lo que ocurre en los casos ordinarios de complicidad: contribuyen al ciclo de difusión, ya que sin una

[37] Sobre el perjuicio a la privacidad que genera esta clase de prácticas, pero también sobre el daño social que genera, véase solamente Franks, *The Palgrave Handbook of Applied Ethics and the Criminal Law*, p. 661 (675 ss.).

[38] Para una síntesis de los principales argumentos, véase Frowe, Helen/Parry, Jonathan, "The case for criminalising revenge porn consumption", *LSE British Politics and Policy*, 15/03/2022, disponible en https://blogs.lse.ac.uk/politicsandpolicy/criminalising-revenge-porn-consumption/ [último acceso: 15/03/2025].

[39] Cf. Frowe, Helen/Parry, Jonathan, "Wrongful Observation", *Philosophy & Public Affairs* 47 (2019), 104 (118 ss.).

[40] Cf. Frowe/Parry, *Philosophy & Public Affairs* 47 (2019), 104 (121 ss.).

audiencia no habría una difusión exitosa.[41] Suponiendo que Frowe y Parry estén en lo cierto en su apreciación, el Código Penal argentino podría incluir un nuevo delito de pornografía ilícita, tendente a criminalizar la tenencia de imágenes íntimas no consentidas de un modo autónomo. En particular, se podría pensar en la creación de un artículo con estructura similar a la del art. 128 del Código Penal.

No obstante, pensamos, una vez más, que debemos ser cautos a la hora de criminalizar conductas de esta clase en un proyecto de reforma de la ciberdelincuencia, sin embarcarnos en una reforma general de los delitos sexuales. Equiparar (o casi equiparar) la pornovenganza a la pornografía infantil implicaría no solo una reforma generalizada de los delitos sexuales, sino también un cambio importante en las valoraciones que subyacen a estos delitos respecto de qué comportamientos incorrectos la sociedad está dispuesta a tolerar (y cuáles no), sobre todo si implica la criminalización de la tenencia y no solo de la difusión. En otras palabras, esta criminalización de la tenencia de determinados contenidos no debe tomarse a la ligera, ya que ampliaría considerablemente el ámbito de conductas punibles, y tal decisión le corresponde a la sociedad tras una deliberación profunda. En cualquier caso, aunque existan argumentos convincentes a favor de criminalizar incluso la tenencia de "pornovenganza", puede ser preferible comenzar con la criminalización de la difusión en esta reforma de la ciberdelincuencia y dejar abierta la cuestión de la mera posesión para una futura reforma legislativa más ambiciosa. De hecho, esto es lo que ha sucedido en el pasado con otros casos de pornografía ilícita en la Argentina, que comenzó con una criminalización de ciertos casos especialmente graves y recién en un momento posterior se amplió la punibilidad hasta abarcar la tenencia.

La criminalización de la difusión de esta clase de contenido audiovisual también parece estar en línea con los estándares internacionales más recientes. En particular, la reciente Convención de Naciones Unidas para prevenir y combatir el delito cibernético establece un deber de criminalización de esta clase de conductas.[42] Con independencia de la entrada en vigencia de esta convención, puede decirse que hay al menos una tendencia internacional a castigar esas conductas. Véase, en particular, el artículo 16 de esta Convención:

---

[41] Cf. Frowe/Parry, *Philosophy & Public Affairs* 47 (2019), 104 (125 ss.).

[42] Naciones Unidas, Asamblea General, A/79/460, Distr. general 27 de noviembre de 2024, Septuagésimo noveno período de sesiones Tema 108 del programa, Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, p. 1 (13).

"Artículo 16

Difusión no consentida de imágenes de carácter íntimo

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito en su derecho interno la venta, distribución, transmisión, publicación o facilitación de otra manera, de forma deliberada y sin derecho, de una imagen de carácter íntimo de una persona por medio de un sistema de tecnología de la información y las comunicaciones, sin el consentimiento de la persona mostrada en la imagen.

2. A los efectos del párrafo 1 del presente artículo, por "imagen de carácter íntimo" se entenderá un registro visual de una persona mayor de 18 años de edad captado por cualquier medio, con inclusión de un registro fotográfico o videográfico, que sea de carácter sexual, en el cual estén expuestas las partes íntimas de la persona o esta realice actividades sexuales, que fuera privado en el momento de captarse y respecto del cual la persona o personas mostradas tuvieran una expectativa razonable de privacidad en el momento de cometerse el delito.

3. Un Estado parte podrá ampliar la definición del término "imagen de carácter íntimo", según proceda, a las representaciones de personas menores de 18 años de edad si han alcanzado la edad mínima legal para realizar actividades sexuales establecida en el derecho interno y la imagen no muestra abusos o explotación de niños.

4. A los efectos del presente artículo, una persona menor de 18 años de edad mostrada en una imagen de carácter íntimo no puede consentir la difusión de una imagen de carácter íntimo que constituya material que muestre abusos sexuales de niños o explotación sexual de niños en virtud del artículo 14 de esta Convención.

5. Los Estados partes podrán exigir como requisito que exista el propósito de causar daños para que se considere que existe responsabilidad penal.

6. Los Estados partes podrán adoptar otras medidas en relación con los asuntos vinculados al presente artículo, de conformidad con su derecho interno y en consonancia con las obligaciones internacionales aplicables".

Por esas razones, proponemos incorporar el delito de difusión no consentida de contenidos sexuales como un delito contra la intimidad, y no necesariamente como un delito contra la libertad sexual equivalente a los de pornografía ilícita. Esto está en línea con la tendencia que se observa en los recientes proyectos de reforma en la Argentina. En particular, en el último Proyecto de Reforma se propuso el siguiente delito:

"ARTÍCULO 493.- Se impondrá prisión de SEIS (6) meses a DOS (2) años o SEIS (6) a VEINTICUATRO (24) días-multa, al que sin autorización de la persona afectada difundiere,

revelare, enviare, distribuyere o de cualquier otro modo pusiere a disposición de terceros imágenes o grabaciones de audio o audiovisuales de naturaleza sexual, producidas en un ámbito de intimidad, que el autor hubiera recibido u obtenido con el consentimiento de la persona afectada, si la divulgación menoscabare gravemente su privacidad.

La pena será de prisión de UNO (1) a TRES (3) años:

1°) Si el hecho se cometiere por persona que esté o haya estado unida a la víctima por matrimonio, unión convivencial o similar relación de afectividad, aun sin convivencia.

2°) Si la persona afectada fuere una persona menor de edad.

3°) Si el hecho se cometiere con fin de lucro".

Esta propuesta fue retomada recientemente por algunos legisladores argentinos. Así, a modo de ejemplo, el proyecto de Mónica Macha,[43] tendente a un refuerzo de la criminalización de conductas sexuales indebidas en base a la llamada "Ley Belén", incluye reformas importantes al delito de exhibiciones obscenas,[44] así como un tipo penal equivalente al propuesto en el proyecto de reforma del Código Penal, pero más detallado y que incluye también la toma de imágenes no consentidas.[45] También el reciente proyecto

[43] Cámara de Diputados de Argentina, Expediente 1123-D-2024, 03/04/2024, disponible en: https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2024/PDF2024/TP2024/1123-D-2024.pdf [último acceso: 15/03/2025]).

[44] La redacción propuesta es la siguiente:

"Artículo 129°: Será reprimido con multa de pesos seiscientos mil ($600.000) a pesos cuatro millones ($ 4.000.000) el que ejecutare, o hiciere ejecutar por otros, actos de exhibiciones obscenas expuestas a ser vistas involuntariamente por terceros; o exhibiciones de partes genitales con fines predominantemente sexuales, enviadas por intermedio de las tecnologías de la información y la comunicación sin consentimiento de quien las recepta.

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".

[45] La redacción propuesta es la siguiente:

"Artículo 155° bis: Se aplicará prisión de ocho meses a un año y el doble de la multa establecida en el artículo 155° a quien, por cualquier medio, sin autorización de la víctima o mediando engaño, videograbe, audiograbe, fotografíe, filme o elabore, documentos con contenidos de desnudez, naturaleza sexual o representaciones sexuales.

Se aplicará prisión de tres meses a tres años y el doble de la multa establecida en el art. 155 a quien, por cualquier medio, y sin autorización de la víctima difunda, publique, envíe o de cualquier manera ponga al alcance de terceros documentos con contenidos de desnudez o naturaleza sexual o representaciones sexuales que el autor haya recibido de la persona afectada, o que el autor haya producido u obtenido de la persona afectada con o sin mediar su consentimiento.

Se aplicará prisión de ocho meses a un año y el doble de la multa establecida en el art. 155 a quien, habiendo recibido del autor del párrafo anterior o de terceras personas o teniendo en su poder por cualquier circunstancia distinta a la descrita en el primer párrafo, los documentos allí referidos, por cualquier medio, y sin consentimiento de la víctima los difunda, publique, envíe o de cualquier manera ponga al alcance de terceros.

Se aplicará prisión de ocho meses a un año y el doble de la multa establecida en el art. 155° a quien, por cualquier medio, y sin autorización de la víctima, difunda, publique, envíe o de cualquier manera ponga al alcance de terceros, documentos con contenidos de desnudez, naturaleza sexual o representaciones sexuales que se hayan elaborado con el uso de las tecnologías de la información y la comunicación, o de la inteligencia artificial, y no correspondan con la persona que es retratada, señalada y/o identificada en los mismos".

de Rodrigo de Loredo y Pablo Cervi aborda el tema,[46] a partir tanto de un artículo 155 bis[47] similar al del Proyecto de Reforma del Código, como de un artículo 155 ter[48] que tendería a abarcar la "redistribución" de contenidos ya distribuidos previamente (aunque la terminología no es la mejor, al prescindir del verbo, más preciso, "difusión", utilizado en la Convención de Naciones Unidas). Sobre el primer proyecto, así como de cualquier otra propuesta que vaya en esas líneas, debe decirse que la regulación que se propone implica una reforma integral de los delitos contra la integridad sexual y contra la intimidad, incluyendo la punición de la toma de imágenes no consentidas. Si bien consideramos necesaria esa clase de criminalización, estimamos que una reforma de ciberdelitos tiene que ser más modesta. Por lo demás, ese proyecto incorpora tipos penales extremadamente detallados, que probablemente podrían ser redactados de un modo más sencillo. Algo similar sucede con la regulación del segundo proyecto. Quien "redistribuye" (mejor dicho: "redifunde") ya cumple el tipo penal de distribución (o "difusión", según la redacción que consideramos apropiada) de contenidos, por lo que no es necesario un nuevo tipo penal para captar esas conductas. Consideramos que esa clase de regulación puede ser contraproducente (ya que al ser tan específica, aumentan los riesgos de que nuevos casos dignos de ser castigados no puedan ser considerados punibles) y que resulta preferible una redacción más general, aunque no por eso menos determinada.

---

[46] Cámara de Diputados de Argentina, Expediente 0447-D-2024, 08/03/2024, disponible en: https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2024/PDF2024/TP2024/0447-D-2024.pdf [último acceso: 15/03/2025]).

[47] La redacción propuesta es la siguiente:
"ARTÍCULO 155 bis. – Se impondrá una pena de prisión o reclusión de seis (6) meses a cuatro (4) años y multa de pesos cien mil ($ 100.000) a pesos quinientos mil ($ 500.000), el que en el marco de una relación íntima o de confianza, o de la prestación de un servicio, difundiere, publicase, distribuyere, revelare, o cediese a terceros, imágenes, grabaciones de audio o filmaciones de contenido sexual o erótico de una persona, por cualquier medio, sin su expreso consentimiento.
La pena será de diez (10) meses a seis (6) años y multa de pesos doscientos mil ($ 200.000) a pesos setecientos setenta y cinco mil ($ 750.000) cuando la obtención de los contenidos difundidos, publicados, distribuidos, revelados o cedidos a terceros, se produjese mediante las formas previstas en los artículos 153 y 153 bis del Código Penal de la Nación Argentina.
Si alguno de los hechos previstos en este artículo se cometiere contra una persona menor de edad, la pena será de tres (3) a seis (6) años y multa de pesos doscientos cincuenta mil ($ 250.000) a pesos un millón ($ 1.000.000)."

[48] La redacción propuesta es la siguiente:
"ARTÍCULO 155 ter. – Se impondrá una multa de pesos veinte mil ($ 20.000) a pesos ciento cincuenta mil ($ 150.000), el que, por medio de las tecnologías de la información y comunicación, redifundiere, publicase, distribuyere o compartiere a terceros, imágenes, grabaciones de audio o filmaciones de contenido sexual o erótico de una persona con la que no posee un vínculo directo previo y siempre que dicho contenido no estuviere destinado a ser accesible por el público, sin el expreso consentimiento de la persona involucrada y cuando ello no resultare en otro delito más severamente penado".

En esta línea, el proyecto de María Soledad Carrizo, entendemos, va por el camino correcto en cuando a técnica legislativa:

"Artículo 117 ter: Será reprimido con pena de 6 meses a dos años de prisión quien, sin consentimiento expreso de la víctima, revelare, publicare, facilitare, o difundiere por cualquier medio o pusiera a disposición de terceros documentos, imágenes, material fílmico, o de voz, originados y obtenidos en un ámbito de intimidad o privacidad personal con contenido sexual.
La escala penal se elevará en la mitad del mínimo y del máximo, cuando la acción fuera cometida por el cónyuge, pareja o conviviente de la víctima, o la persona con quien la victima mantiene o ha mantenido una relación de pareja".

Si bien seguiremos esta propuesta, consideramos que es necesario realizar algunos cambios. En primer lugar, estimamos que lo que está en juego en estos delitos es la intimidad de la persona, no el honor.[49] En ese sentido, la difusión de imágenes íntimas ya es incorrecta, incluso si eso no afecta la reputación de la víctima. La ubicación sistemática correcta del tipo penal es, entonces, en los delitos contra la intimidad.[50] En segundo lugar, la redacción debe ser simplificada, en especial la reiteración de acciones delictivas ("típicas") que se superponen. En tercer lugar, deben ser incluidos aquellos casos. En particular, proponemos el siguiente tipo penal, que combina la propuesta de Carrizo con la del Proyecto de Reforma del Código Penal[51]:

"Artículo 155bis:
Será reprimido con pena de seis meses a dos años el que de manera no autorizada pusiere a disposición de terceros fotografías o grabaciones de audio o video sexuales o de partes íntimas de la víctima, después de haberlas producido con conocimiento de la otra parte o sin él o después de haberlas recibido de ella u obtenido de otro modo.
La pena prevista en el párrafo anterior se aumentará en un tercio en su mínimo y en su máximo:

[49] Coincidente Aboso, *Sistema penal e informática*, t. 3, p. 255 (281). Probablemente también Dupuy, *Acosos en la red a mujeres*, p. 98 (135).
[50] Véase también Frowe/Parry, *Philosophy & Public Affairs* 47 (2019), 104 (127 ss.).
[51] Para una propuesta similar, véase el proyecto de Silvia Lospenatto (Cámara de Diputados de Argentina, Expediente 0614-D-2024, 12/03/2024, disponible en: https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2024/PDF2024/TP2024/0614-D-2024.pdf [último acceso: 15/03/2025]):
"Artículo 155 bis: "Será castigado con pena de prisión de seis (6) meses a dos (2) años quien, sin autorización de la persona afectada, difunda, revele o ceda a terceros, imágenes o grabaciones de audio y/o video de carácter íntimo, las cuales hubiera obtenido con consentimiento de la persona afectada en un lugar privado, cuando su divulgación menoscabe gravemente la privacidad de esa persona".

1°) Si el hecho fuese cometido por persona que esté o haya estado unida a la víctima por relación especial de confianza

2°) Si el hecho fuese cometido con ánimo de lucro".

De este modo, hacemos más clara la conducta ilícita, penalizando básicamente la difusión no autorizada (no consentida) de contenido sexual (que por supuesto, incluye la "redifusión") y también de representaciones de las partes íntimas de la víctima, que no tienen por qué ser de naturaleza sexual. Aclaramos que dicho contenido puede no haber sido producido con el conocimiento de la víctima, como cuando se le toman imágenes a personas dormidas.[52] No incluimos un resultado adicional de afectación grave a la intimidad, debido a que ya difusión de esta clase de contenidos en sí misma es lo suficientemente grave y afecta el derecho negativo de la víctima a terceras personas no accedan a esos contenidos.[53] En cuanto a la imposición de multas, las eliminamos porque la conducta luce lo suficientemente grave, como violación a la intimidad, como para merecer una pena de prisión. Por lo demás, las penas son "relativamente" bajas, ya que es necesario respetar la proporcionalidad de las penas en relación con otros delitos contra la intimidad. Un castigo más severo requiere, necesariamente, una reforma integral de estos delitos. Piénsese solamente que el art. 157 bis, que criminaliza conductas graves contra la intimidad a causa del acceso ilegítimo a información sensible, tiene un máximo de pena de dos años. Además, estas penas tienen también que estar en proporción, por un lado, con los abusos sexuales simples (actualmente con pena de seis meses a cuatro años), que debido al contacto corporal son, al menos en principio, más graves que la difusión de imágenes. Por otro lado, tienen que guardar proporción con las formas especialmente graves de difusión de pornografía ilícita del artículo 128 del Código Penal, que tiene una pena mínima de tres años. En cuanto a la agravante por el vínculo, utilizamos el término más general "relación especial de confianza" para evitar el recurso a ejemplos innecesarios.[54] Esto también aclararía que el delito básico puede no implicar una relación de confianza entre el autor o la víctima. Finalmente, consideramos que no es necesario incorporar una agravante por minoridad, en virtud de que en esos casos rigen las ya mencionadas reglas específicas de pornografía ilícita del artículo 128 del Código Penal.

[52] Similar Aboso, "*Sistema penal e informática*, t. 3, p. 255 (272).
[53] Probablemente también, en relación con ese requisito del Proyecto de Reforma, Aboso, "*Sistema penal e informática*, t. 3, p. 255 (270). En contra Dupuy, *Acosos en la red a mujeres*, p. 98 (155 ss.).
[54] Similar, aunque recurriendo a ejemplos (algo que debe evitarse en la medida de lo posible) Dupuy, *Acosos en la red a mujeres*, p. 98 (165 ss.).

Una última cuestión. También se ha propuesto, en algunos proyectos de ley, la creación de un tipo penal de "sextorsión",[55] que pretendería abarcar casos en los que se amenaza a la víctima con la publicación de imágenes íntimas a cambio de realizar "favores sexuales" o incluso a cambio de un precio.[56] Somos escépticos respecto de la necesidad de crear un tipo penal así en la Argentina. Si el mal amenazado (publicación de las imágenes sexuales) es utilizado para coaccionar a la víctima y obligarla a tener relaciones sexuales, entonces esos casos ya pueden ser abarcados por las reglas del delito de coacciones (artículo 149bis, segundo párrafo del Código Penal). Si la víctima coaccionada aceptase tener relaciones sexuales en razón de la coacción, serían aplicables las reglas de abuso sexual, incluso de violación, del artículo 119 del Código Penal. En el caso de que se quiera obtener dinero a cambio de no publicar las imágenes, las reglas clásicas de extorsión (artículo 168 del Código Penal) y o de chantaje (artículo 169 del Código Penal) resultan aplicables. Es cierto que se podría pensar en la creación de agravantes específicas de esos delitos, pero eso implicaría una reforma importante de esa clase de delitos, cuya necesidad no es evidente. Por consiguiente, la creación de esta clase de agravantes para hechos que ya están criminalizados según el derecho vigente puede ser dejada de lado en un proyecto de ley sobre criminalidad informática.

IV. Deepfakes, especialmente sexuales

Una última cuestión que requiere un tratamiento especial es la creación o modificación de imágenes, o videos en especial imágenes o videos sexuales, mediante inteligencia artificial u otros medios técnicos.[57] Esta cuestión ha adquirido relevancia en los últimos tiempos por distintos casos en los que mediante estas tecnologías fueron creadas imágenes fotorrealistas de celebridades (y también de personas comunes) teniendo relaciones sexuales o participando de actividades especialmente humillantes.[58] Esto ha dado lugar a distintas reacciones legislativas. En la Argentina, en particular, el proyecto de Eugenia

[55] Véase, por ejemplo, la redacción del artículo 169 del Código Penal que se plantea en el ya mencionado proyecto de Rodrigo de Loredo y Pablo Cervi:
"ARTÍCULO 169. - Será reprimido con prisión o reclusión de tres (3) a ocho (8) años, el que, por amenaza de imputaciones contra el honor, de difusión de documentos con contenido sexual o erótico, o de violación de secretos, cometiere alguno de los hechos expresados en el artículo precedente".
[56] Véase también Moyano, *Ciberdelitos*, pp. 114 s.
[57] Véase Thiel, Markus, „Deepfakes" – Sehen heißt glauben?", *ZRP* 2021, 202 (203).
[58] Para un panorama al respecto, véase Kira, Beatriz, "Deepfakes, the Weaponisation of AI Against Women and Possible Solutions", *Verfassungsblog*, 03/06/2024, disponible en: https://verfassungsblog.de/deepfakes-ncid-ai-regulation/ [último acceso: 15/03/2025].

Alianello[59] resulta interesante, ya que propone la criminalización de la producción y difusión de *deepfakes* sexuales que tengan por objeto a menores de edad:

"Artículo 131 bis.
Será reprimido con prisión de uno (1) a tres (4) años quien hostigue, acose, persiga o intimide a menores de dieciocho (18) años utilizando cualquier medio digital o electrónico, incluyendo la creación o difusión de contenido *deepfake*, con el objetivo de generar temor, angustia o daño emocional.
La pena prevista en este artículo se elevará en un tercio en su mínimo y en su máximo cuando la víctima fuere menor de trece (13) años".

Consideramos que esta propuesta va por el buen camino, pero que tiene algunos inconvenientes importantes. El primero es que no aborda de modo general el problema de los *deepfakes* degradantes,[60] de los cuales los *deepfakes* sexuales son solamente un subtipo. El segundo es que la protección frente a *deepfakes* degradantes no debe alcanzar solamente a menores de edad, sino también a mayores, cuya imagen pública también pueda verse dañada por su difusión. El tercero es que no se está en presencia de delitos contra la integridad sexual en sentido estricto, sino más bien de delitos de injuria en un sentido específico: violaciones al respeto que se le debe a cualquier ser humano.[61] Por tanto, la correcta regulación debe figurar en el marco de los delitos contra el honor, no en el marco de los delitos sexuales.[62] Y el cuarto es que utilizar el concepto "contenido deepfake" en un tipo penal luce muy extraño y genera problemas de determinación (*lex certa*): ¿qué significa exactamente eso y por qué se ha recurrido al idioma inglés en el Código Penal argentino?
La reciente experiencia alemana puede ayudar a encontrar una alternativa superadora. En Alemania el Estado de Baviera propuso recientemente un proyecto de ley sobre la criminalización de *deepfakes*,[63] pero el gobierno federal no consideró necesario proceder

[59] Cámara de Diputados de Argentina, Expediente 7225-D-2024, 02/12/2024, disponible en: https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2024/PDF2024/TP2024/7225-D-2024.pdf [último acceso: 15/03/2025]
[60] Al respecto, véase Thiel, *ZRP* 2021, 202 (204).
[61] En detalle sobre esta concepción de las injurias Hilgendorf, Eric, "Beleidigung als Respektverletzung. Interdisziplinäre Perspektiven", en Hilgendorf/Oğlakcıoğlu (eds.), *Verrohung der Kommunikation? Verrohung des Strafrechts*, Berlín, Duncker & Humblot, 2025, p. 35 (35 ss.).
[62] Agradecemos a Jonathan Polansky por esta adecuada sugerencia.
[63] Bundesrat, Drucksache 222/24, Gesetzesantrag des Freistaates Bayern, Entwurf eines Gesetzes zum strafrechtlichen Schutz von Persönlichkeitsrechten vor Deepfakes, 14/05/2024, disponible en https://www.bundesrat.de/SharedDocs/drucksachen/2024/0201-0300/222-24.pdf?__blob=publicationFile&v=1 [último acceso: 15/03/2025]. Véase también la propuesta del

a una reforma.[64] Esto se debió a que, según el gobierno federal, las imágenes sexuales falsas ya son punibles en Alemania. Entre otros argumentos, el gobierno federal señaló lo siguiente. En el caso de los adultos, la difusión de *deepfakes* ya sería punible como difamación en virtud del § 187 del Código Penal alemán:[65] "Quien, de mala fe, afirme o difunda un hecho no verídico con referencia a otro, que sea apropiado para desacreditarlo o denigrarlo ante la opinión pública o poner en peligro su reputación crediticia será penado con pena privativa de libertad de hasta dos años o con pena de multa y, si el hecho es cometido públicamente, en una reunión o por medio de la difusión de un contenido (§ 11, párrafo 3), lo será con pena privativa de libertad de hasta cinco años o con pena de multa".[66] Lo mismo se aplicaría a los menores. En Alemania, las *deepfakes* sexuales de menores estarían cubiertas por las disposiciones que prohíben la posesión y difusión de pornografía infantil en virtud de los §§ 184b y 184c.[67]

Sin embargo, estas consideraciones no se aplican a la Argentina. El Código Penal argentino no contempla el delito de difamación con ese alcance, sino que solo se podría recurrir al delito general de injurias del art. 110 del Código Penal, que tiene una pena bajísima y un régimen especialmente benigno en los artículos siguientes. Por tanto, la difusión de *deepfakes*, incluso sexuales de adultos, o bien recibiría una pena mínima por injurias, o bien quedaría impune por las reglas especiales del delito de injurias. Además, la Argentina en principio solo penaliza la posesión y difusión de representaciones de un menor (real) vinculadas a su genitalidad (real) o una actividad sexual (real), no la difusión de imágenes falsas de pornografía infantil creadas por inteligencia artificial,[68] aunque la redacción de la norma no es suficientemente clara y pueda recurrir a alguna clase de interpretación extensiva poco ortodoxa. Sigue vigente, entonces la pregunta de si sería conveniente penalizar al menos algunos casos de *deepfakes* degradantes.

Al igual que con el resto de los delitos analizados en esta conferencia, se debe actuar con cautela. No se debe aprovechar esta oportunidad para proponer una reforma integral de la

---

Bundesrat: Bundesrat, Drucksache 222/24 (Beschluss), Gesetzentwurf des Bundesrates Entwurf eines Gesetzes zum strafrechtlichen Schutz von Persönlichkeitsrechten vor Deepfakes, 05/07/24, disponible en https://kripoz.de/wp-content/uploads/2024/07/br-drs-222-24B.pdf [último acceso: 15/03/2025].

[64] Deutscher Bundestag, Drucksache 20/12605, 20. Wahlperiode Gesetzentwurf des Bundesrates, Entwurf eines Gesetzes zum strafrechtlichen Schutz von Persönlichkeitsrechten vor Deepfakes, 21/08/2024, disponible en https://dserver.bundestag.de/btd/20/126/2012605.pdf [último acceso: 15/03/2025].

[65] Deutscher Bundestag, Drucksache 20/12605, 1 (21).

[66] Se utiliza la traducción de Marcelo Sancinetti, Fernando Córdoba, Marcelo Lerman y Leandro Dias disponible en: Hilgendorf/Valerius, *Derecho Penal. Parte Especial*, t. 1, § 5 n.º m. 44.

[67] Deutscher Bundestag, Drucksache 20/12605, 1 (21).

[68] Véase Aboso, *Delitos sexuales*, pp. 201 ss.; Teodoro Álvarez, Javier, *Delitos sexuales*, Buenos Aires, Ediciones DyD, 2018, pp. 85 ss.

criminalización de la publicación de los delitos de pornografía ilícita, sobre todo cuando la última reforma en la materia es relativamente reciente: en 2018 fue sancionada la Ley 27.436. Si debe o no criminalizarse en el futuro es una decisión del legislador argentino en un tema particularmente sensible. Asimismo, no deberíamos aprovechar esta oportunidad para hacer una reforma integral de los delitos contra el honor, incluyendo un delito de difamación. No obstante, sí podría modificarse la regulación de los delitos contra el honor de un modo cauteloso para captar de forma general el ilícito material de la difusión de *deepfakes* especialmente denigrantes. De hecho, estudios recientes han sugerido que la mera posesión de *deepfakes* sexuales puede ser ilícita y perjudicial para la víctima, cuya intimidad, reputación y eventual salud mental se verían en peligro por la creación y posesión de imágenes sexuales.[69]

Nuestra propuesta es, por tanto, criminalizar únicamente la difusión de *deepfakes denigrantes*, en la línea de la propuesta debatida recientemente en Alemania,[70] pero sin crear un delito de difamación ni modificar el delito de posesión de pornografía infantil. En los casos en que los *deepfakes* sean sexualmente explícitos, esa circunstancia puede hacer las veces de agravante. En resumen, proponemos la inclusión del siguiente texto en el artículo 117 bis, inciso 1 del Código Penal, actualmente en blanco:

"Artículo 117 bis:

El que deshonrare o desacreditare gravemente a otra persona poniendo a disposición de un tercero imágenes o videos producidos o modificados por medios informáticos y que den la impresión de ser fieles a la realidad del aspecto, comportamiento o manifestaciones orales de esa persona, será castigado con prisión de un mes a un año.

---

[69] En detalle Kira, Beatriz, "When non-consensual intimate deepfakes go viral: The insufficiency of the UK Online Safety Act", *Computar Law & Security Review* 54 (2024), 106024, 1 (2 ss.).

[70] La propuesta de tipo penal en discusión era la siguiente:
"§ 201b: Violación de los derechos de la personalidad mediante falsificación digital
(1) Quien viole el derecho de la personalidad de otra persona poniendo a disposición de un tercero un contenido multimedia creado o modificado por medios informáticos que dé la apariencia de una grabación de imagen o sonido realista de la apariencia externa, el comportamiento o las expresiones orales de esa persona a una tercera persona, será reprimido con prisión de hasta dos años o con multa. Lo mismo se aplicará si el hecho mencionado en la primera frase se refiere a una persona fallecida y se infringe gravemente su derecho a la personalidad.
(2) Quien, en los casos del párrafo 1, frase 1, haga público el contenido de un medio de comunicación o haga público un contenido de un medio de comunicación que tenga por objeto un acontecimiento de la esfera más personal de la vida, será reprimido con prisión de hasta cinco años o con multa.
(3) El párrafo 1, oración 1, también en relación con el párrafo 2, no se aplica a las acciones realizadas en defensa de intereses legítimos preponderantes, en particular el arte o la ciencia, la investigación o la enseñanza, la información sobre acontecimientos de actualidad o históricos o fines similares.
(4) Los soportes de imagen o sonido u otros medios técnicos utilizados por el autor o partícipe podrán ser decomisados. Es de aplicación el § 74a" (traducción de Leandro Dias).

En los casos del primer párrafo, la pena máxima de prisión se elevará a dos años si las imágenes o videos se hacen accesibles a la generalidad o si se trata de un asunto relacionado con una esfera altamente personal de la vida, como la sexualidad de la víctima.
No son punibles los actos realizados en ejercicio de derechos constitucionales u otros intereses legítimos".

Hemos utilizado la reciente propuesta alemana como fuente principal de esta disposición, pero hemos introducido algunos cambios. La principal modificación es convertir este delito en un delito contra el honor y no en un delito contra la intimidad. Al fin y al cabo, los *deepfakes* son una subcategoría de contenidos falsos que, por tanto, no invaden la intimidad de otra persona. Lo que se lesiona al difundir *deepfakes* es, entonces, el honor de la víctima: con la difusión de *deepfakes*, el autor intenta desacreditar (honor externo) o dañar la percepción subjetiva de valía (honor interno) de la víctima.[71] Esto es básicamente lo mismo que ocurre con toda injuria punible y, por lo tanto, mantuvimos principalmente la redacción utilizada por el legislador argentino al regular el delito de injurias (artículo 110), pero aumentamos la pena para captar el ilícito adicional de utilizar contenidos falsos, pero que son muy difíciles (y en algunos casos pueden ser imposibles) de desacreditar como falsos. Para evitar persecuciones triviales, también hemos incorporado una cláusula de "bagatela", en el sentido de que solo puede ser punible la difusión de *deepfakes* que afecten *gravemente* el honor de otra persona. Según la regulación propuesta, la difusión de *deepfakes* sexuales es un subtipo de la agravante general de difusión *deepfakes* que afecten a la esfera más privada de la víctima. Dejamos fuera del tipo las grabaciones solamente de audio, debido a que presentan un contenido denigrante claramente menor que las que involucran contenido visual. También eliminamos la posible criminalización de *deepfakes* de personas fallecidas, debido a que es ajena a la sistemática del Código Penal argentino. Finalmente, el último párrafo deja claro que algunos casos de difusión de *deepfakes* pueden ser lícitos, si se realiza como ejercicio de un interés legítimo, como en los casos de representación artística, periodismo o educación.

V. Conclusión

[71] Sobre estas diversas facetas del concepto de honor, véase solamente Hilgendorf/Valerius, *Derecho Penal. Parte Especial*, t. 1, § 5 n.º m. 2 s.

La conclusión más importante a la que se puede arribar aquí es que solo será posible regular adecuadamente las conductas sexuales ilícitas en Internet si son modificados integralmente los delitos sexuales y contra la intimidad. Desde el punto de vista del derecho de la ciberdelincuencia, solo podemos hacer algunas propuestas mínimas para que al menos las conductas ilícitas más importantes puedan ser penalizadas en la Argentina. En particular, sugerimos los siguientes pasos:

1. En cuanto a los delitos sexuales, no debería hacerse ninguna reforma para tipificar el "abuso sexual a distancia", al menos no en una reforma sobre criminalidad informática.
2. En cuanto a los delitos contra la intimidad, debería crearse el delito de difusión no autorizada de imágenes íntimas para castigar los casos de la llamada "pornovenganza". No se estima necesaria la creación de un tipo penal de extorsión sexual.
3. La difusión de imágenes falsas creadas con inteligencia artificial debe ser un delito contra el honor independiente en la Argentina (a diferencia de lo que ha sucedido en Alemania).

Reforma sobre la criminalidad informática en la Argentina (4). Otros delitos

Eric Hilgendorf y Leandro Dias

I. Introducción

En esta última conferencia sobre la reforma de la ciberdelincuencia en la Argentina nos centraremos en otros delitos que deberían crearse o modificarse imperiosamente. En particular, se abordarán cuatro temas. El primero es el de las lagunas de punibilidad que existen en la Argentina con respecto al acoso digital (*cybermobbing*). El segundo es el de la suplantación de identidad en redes sociales, algo que hasta ahora no ha sido regulado en la Argentina. La tercera cuestión se refiere a la creación de un delito de peligro, relacionado con la administración de plataformas delictivas en Internet. Por último, haremos dos sugerencias relacionadas con la protección de la intimidad y con la cuestión de los ciberataques.

Cabe señalar una vez más que el objetivo de estos dictámenes es el de ofrecer una reforma mínima de la ciberdelincuencia, sin pretender agotar la materia. En la actualidad, aparecen nuevos problemas de ciberdelincuencia, por lo que la labor legislativa requerirá necesariamente una actualización y revisión constantes. Solo como ejemplo, en Alemania se está produciendo ahora un gran debate: ¿sería aconsejable tipificar las conductas lesivas que solo tienen lugar dentro de la plataforma Metaverso u otros mundos artificiales de realidad virtual, pero que no tienen un impacto físico en el mundo real (como el "abuso sexual" cometido a través de un avatar, controlado por un usuario, contra otro avatar, controlado por otro usuario)?[1]

Además, algunos aspectos de la regulación penal de la ciberdelincuencia están estrechamente relacionados con otras decisiones que debe adoptar el legislador en el marco de una reforma global del derecho penal. De hecho, fuimos informados de la labor que está realizando actualmente otro grupo que trabaja en una reforma integral del Código Penal argentino. Como este grupo también está trabajando en cuestiones de criminalidad informática, intentaremos ofrecer una propuesta básica para el Código Penal actual, en lugar de abogar por una reforma total del cibercrimen en la Argentina, y de ese modo dejar espacio para decisiones "macro" diferentes a las que aquí proponemos. La principal consecuencia de este enfoque es que no intentaremos cambiar lo que no está roto, aun cuando a nosotros, como académicos, nos gustaría regular las conductas de una manera

[1] Al respecto, en detalle Hilgendorf, Eric, "Virtuelle Realitäten, Metaverse, Generative KI und (Straf-) Recht", *JuristenZeitung* 2024, 677 (684 ss.).

diferente. Por eso, solo propondremos modificaciones menores y dejaremos las demás partes de una posible reforma al otro grupo de trabajo.

Otro ejemplo de reformas posibles, y quizá deseables, pero que no pueden ser tomadas en un proyecto de reforma solamente sobre la criminalidad informática, se relaciona con la inteligencia artificial. Recuérdese lo que se dijo a la hora de valorar un posible delito específico que podría incorporarse al Código Penal argentino, como una nueva forma de injuria para incluir los *deepfakes* denigrantes, especialmente los de contenido sexual. Por supuesto, se podría pensar en una reforma mucho más importante en términos de protección del honor, para incluir también la mera creación y tenencia de *deepfakes* injuriantes. Sin embargo, la relación entre la libertad de expresión y la protección penal del honor es difícil, especialmente en la Argentina, que ha adoptado una posición particularmente amplia sobre el alcance de la libertad de expresión, siguiendo el modelo estadounidense.[2] Por ello, una criminalización más amplia que la aquí propuesta tendría que ir acompañada de una modificación sustancial de todo el Código Penal argentino, algo que, de nuevo, excede los objetivos de estos dictámenes. Estas consideraciones adquirirían más relevancias si se desease regular en detalle la creación, el uso y la comercialización de sistemas de inteligencia artificial, como ha sucedido recientemente en la Unión Europea. [3] Algunos proyectos de ley de legisladores argentinos van en esa dirección, pero sin proponer una regulación penal abarcativa.[4] Consideramos que esta cuestión, es decir, la regulación general de la inteligencia artificial, merece un proyecto de ley aparte, que incluya modificaciones no solo en la ley penal. Ese proyecto deberá estar acompañado de una investigación seria sobre el tema, que incluya un estudio

[2] Véase, en detalle, Bianchi, Enrique Tomás/Gullco, Hernán, *El derecho a la libre expresión*, 2.ª ed., La Plata, Librería Editora Platense, 2009, pp. 443 ss.

[3] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo de 13 de junio de 2024 por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.o 300/2008, (UE) n.o 167/2013, (UE) n.o 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial).

[4] Véase, por ejemplo, el proyecto de "Ley Turing" de readecuación del sistema jurídico por el impacto de la inteligencia artificial, presentado por el legislador Oscar Agost Carreño (Cámara de Diputados de Argentina, Expediente 1013-D-2024, 26/03/2024, disponible en: https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2024/PDF2024/TP2024/1013-D-2024.pdf [último acceso: 15/03/2025]). Véase la regulación no penal propuesta en el proyecto de "Presupuestos Mínimos para la Promoción del desarrollo de la Inteligencia Artificial (IA) en la República Argentina", presentado por la legisladora Silvana Giudici (Cámara de Diputados de Argentina, Expediente 4079-D-2024, 02/08/2024, disponible en: https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2024/PDF2024/TP2024/4079-D-2024.pdf [último acceso: 15/03/2025]).

detallado de la regulación europea, algo que sin dudas excede los límites de la reforma mínima que estamos proponiendo en este informe.

II. Ciberacoso

El *cybermobbing* o "ciberacoso", es decir, hostigar a alguien utilizando medios electrónicos, es una conducta que en la Argentina solo está regulada como contravención en algunas jurisdicciones locales, pero no como delito.[5] Se plantea entonces la cuestión del merecimiento y necesidad de pena en los casos en que el autor de alguna manera le causa un daño psicológico a la víctima (por ejemplo, una sensación general de ansiedad), que sin embargo no supera el umbral de una lesión en la salud según el artículo 89 del Código Penal argentino, o bien que de algún modo le cercena la libertad, pero sin cumplir con los requisitos de las amenazas simples del artículo 149 bis del Código Penal.[6] Es generalmente aceptado que para que exista una lesión punible, en su variante de daño a la salud, es necesario que se genere un estado patológico en la víctima, equivalente al que generaría un daño en algún sentido "físico".[7] Como es evidente, esto no suele ocurrir en los casos habituales de ciberacoso. Lo mismo sucede con las amenazas simples, que suelen requerir la superación de cierto umbral mínimo de gravedad, que las convierta en idóneas para amedrentar desde una óptica objetiva.[8] Acciones tales como enviarle mensajes reiterados a alguien por redes sociales u observarla constantemente pueden no tener esa idoneidad o, mejor dicho, eso dependerá de las circunstancias del caso concreto.

---

[5] Solo a modo de ejemplo, véanse las siguientes disposiciones del Código Contravencional de la CABA:
"Artículo 54 - Hostigar. Intimidar. Quien intimida u hostiga de modo amenazante a otro, siempre que el hecho no constituya delito, es sancionado con uno (1) a cinco (5) días de trabajo de utilidad pública, multa ochenta (80) a cuatrocientas (400) unidades fijas y/o uno (1) a cinco (5) días de arresto. La acción será dependiente de instancia privada con excepción de los casos donde la víctima fuese menor de 18 años de edad".
"Artículo 76 - Hostigamiento digital - Quien intimide u hostigue a otro mediante el uso de cualquier medio digital, siempre que el hecho no constituya delito, es sancionado con multa de ciento sesenta (160) a ochocientas (800) unidades fijas, tres (3) a diez (10) días de trabajo de utilidad pública, o uno (1) a cinco (5) días de arresto.
La acción será dependiente de instancia privada con excepción de los casos donde la víctima fuese menor de 18 años de edad.
No configura hostigamiento digital el ejercicio del derecho a la libertad de expresión".

[6] En detalle sobre esta cuestión González Guerra, Carlos, "Hostigar, intimidar y maltratar", Revista Argentina de Derecho Penal y Procesal Penal 8 (2013), IJ-LXVIII-60.

[7] Véase, por todos, Sancinetti, Marcelo/Dias, Leandro/Nascimbene, Juan, "Introducción al delito de lesiones", en Pagani (ed.), Transferencia de la Justicia Penal Ordinaria en el Proceso de Autonomía de la CABA, Buenos Aires, Jusbaires, 2016, p. 31 (41). Sobre la regulación legal equivalente en Alemania Hilgendorf, Eric/Valerius, Brian, *Derecho Penal. Parte Especial*, t. 1, Buenos Aires, Ad-Hoc, 2022, § 3 n.º m. 23, con referencias adicionales.

[8] Por todos Molina, Gonzalo, *Manual de Derecho Penal. Parte Especial*, Resistencia, ConTexto, 2021, p. 457 s.

Para evitar lagunas de punibilidad en este aspecto, recientemente en la Argentina la diputada Mónica Macha[9] ha presentado un proyecto de ley que, entre otras cosas, propone crear un tipo penal de hostigamiento digital como delito contra la libertad, con la siguiente redacción:

"ARTÍCULO 149 quarter: Será reprimido con prisión de seis (6) meses a dos (2) años o con multa equivalente al importe de seis (6) a veinticinco (25) salarios mínimos vitales y móviles, siempre que el hecho no constituya un delito más severamente penado, el que mediante la utilización de tecnologías de la información y la comunicación o a través Internet, o medio de comunicación y sin estar legítimamente autorizado:
a) hostigue, acose, persiga, intimide, vigile y/o aceche a una persona;
b) haga accesible al público los datos personales de una persona, sin su consentimiento, causándole un daño y/o atentando contra su seguridad;
c) Establezca o intente establecer contacto con una persona, sin su consentimiento o por medio de terceras personas, alterando el normal desarrollo de su vida cotidiana".

"ARTÍCULO 149 quinto: Se aplicará prisión de uno (1) a tres (3) años y el doble de la pena de multa establecida en el artículo anterior en los siguientes casos:
a) Cuando la acción sea realizada por dos o más personas y en forma organizada;
b) Si se realizare de forma sostenida en el tiempo o de modo tal que obligare a la víctima alterar su proyecto de vida;
c) Si la victima fuera menor de 18 años:
d) Si el hecho se cometiere por persona que esté o haya estado unida a la víctima por matrimonio, unión convivencial, o relación de pareja, mediara o no convivencia;
e) Si el hecho se cometiere por odio racial, religioso, de género y/o a la orientación sexual, identidad de género o su expresión;
f) Si el hecho se cometiere contra una mujer mediando violencia de género;
g) Si el hecho fuere cometido por una persona que haya abusado de su posición de confianza o autoridad".

Esta regulación es interesante y permitiría llenar, al menos parcialmente, las lagunas de punibilidad existentes en la materia. No obstante, creemos que el abordaje tiene que ser

[9] Cámara de Diputados de Argentina, Expediente 6318-D-2024, 23/10/2024, disponible en: https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2024/PDF2024/TP2024/6318-D-2024.pdf [último acceso: 15/03/2025]).

un poco distinto. En primer lugar, estimamos que la regulación es demasiado detallada, lo que genera el problema de que se aumenta el riesgo de que nuevas conductas no encajen en las descripciones de los hechos. Lo bueno de tipos penales clásicos, como el de homicidio, lesiones, hurto o estafa, es que la redacción es sencilla, gracias al uso de conceptos generales capaces de abarcar un sinnúmero de casos merecedores de castigo. Frente a esto no se puede criticar que el principio de legalidad requiere algo así como "la máxima taxatividad legal"[10] en la criminalización. Un estándar así no solo es imposible de realizar,[11] ya que la redacción más determinada es siempre la que podría lograrse con más regulación. Además, el exceso de regulación complica el entendimiento de las conductas prohibidas. Por supuesto, el ciudadano normal probablemente no lea el código penal. No obstante, se le debe brindar la posibilidad de que, si quisiera leerlo, podría entenderlo solo o al menos con una ayuda legal mínima. El exceso de regulación va en contra de esta finalidad y por eso la redacción de la parte especial siempre es un compromiso entre determinación y simplicidad. De hecho, en esta regulación puede observarse cómo varias modalidades comisivas se solapan parcialmente: acechar es sin dudas una forma de hostigar y acosar, mientras que un acoso u hostigamiento puede producirse mediante intimidación, vigilancia, etcétera.

En segundo lugar, estimamos que el ciberacoso es una forma general de acoso, por lo que es necesario un tipo que abarque no solo los casos realizados "mediante la utilización de tecnologías de la información y de la comunicación". Los casos usuales de hostigamiento, como aquellos que consisten en seguir por la calle a la víctima, no involucran esa clase de tecnología y también son merecedores de pena, debido a que pueden afectar la forma de vivir de las víctimas.[12] Por tanto, una regulación del hostigamiento digital debería también abarcar casos de hostigamiento no-digital, para evitar un tratamiento diferente de conductas igualmente merecedoras de castigo.

En tercer lugar, consideramos que los casos de *cybermobbing* requieren una solución también vinculada con los delitos contra la integridad física, debido a las consecuencias nocivas que estas conductas pueden tener en el cuerpo de las víctimas.[13] En otras palabras,

---

[10] Zaffaroni, Eugenio/Alagia, Alejandro/Slokar, Alejandro, *Derecho penal. Parte general*, Buenos Aires, Ediar, 2000, p. 116 ss.

[11] Greco, Luís, "Das Bestimmtheitsgebot als Verbot gesetzgeberisch in Kauf genommener teleologischer Reduktionen", *ZIS* 2018, 475 (476 s.).

[12] En detalle sobre el merecimiento de pena del hostigamiento Kubiciel, Michael/Borutta, Nadine, "Strafgrund und Ausgestaltung des Tatbestandes der Nachstellung (§ 238 StGB)", KriPoZ 2016, 194 (194 s.).

[13] Véase Doerbeck, Caprice, *Cybermobbing. Phänomenologische Betrachtung und strafrechtliche Analyse*, Berlín, Duncker & Humblot, 2019, pp. 225 ss.

hay que buscar una alternativa de regulación que no se concentre, únicamente, en los delitos contra la libertad.

Por estas razones, proponemos un abordaje de dos partes. Primero, propondremos una ligera modificación de los delitos contra la integridad física, para dejar en claro que ciertos casos de ciberacoso merecen ser castigados como lesiones. Como ha señalado en una reciente investigación Caprice Doerbeck,[14] esta clase de conductas en efecto merecen ser castigadas, debido a las consecuencias dañinas que genera en las víctimas, y que hay necesidad de castigo: el derecho penal actual, tal como es concebido en la Argentina o en Alemania, no es suficiente para abarcar estas conductas.[15] Ella propone, como solución, una reforma parcial de distintos ámbitos de la parte especial del derecho penal, entre ellas la incorporación de las lesiones psicológicas en la sistemática de los delitos de lesiones corporales.[16] Esta última tendría fines de clarificación, en el sentido de que si bien las lesiones psicológicas ya estarían abarcadas por los delitos de lesiones corporales en su variante de daño a la salud, en la praxis no suelen ser procesados esos casos.[17] Para dejar en claro que las lesiones psicológicas sí se subsumen en estos tipos penales, habría que hacer, entonces, una reforma parcial.

Consideramos que esta visión es correcta. Si bien ya se señaló que el tipo penal de lesiones (en principio, leves, art. 89 del Código Penal) no excluye la punibilidad de las lesiones psicológicas provenientes de acciones de hostigamiento, sí se requiere un umbral mínimo: que el daño psicológico tenga manifestaciones patológicas, de modo tal que pueda ser considerado un daño a la salud de la víctima. Además, el hecho de que en el tipo penal de las lesiones leves no se haga referencia a un daño psicológico genera que la punibilidad de las lesiones psicológicas dependa, en gran medida, de la interpretación judicial. Por eso, el mero agregado del término "salud integral" servirá para dejar en claro que al menos ciertos casos de daños psicológicos pueden configurar lesiones corporales. En particular, proponemos la siguiente redacción del artículo 89 del Código Penal:

"ARTÍCULO 89. - Se impondrá prisión de un mes a un año, al que causare a otro, en el cuerpo o en la salud integral, un daño que no esté previsto en otra disposición de este código".

[14] Doerbeck, *Cybermobbing. Phänomenologische Betrachtung und strafrechtliche Analyse*, passim.
[15] Doerbeck, *Cybermobbing. Phänomenologische Betrachtung und strafrechtliche Analyse*, pp. 328 ss.
[16] Doerbeck, *Cybermobbing. Phänomenologische Betrachtung und strafrechtliche Analyse*, p. 332.
[17] Doerbeck, *Cybermobbing. Phänomenologische Betrachtung und strafrechtliche Analyse*, p. 332.

El término "salud integral" no es nuevo y es utilizado también en otras partes del ordenamiento jurídico para hacer referencia no solo a la salud "física", sino también a la salud "psíquica". En particular, en la regulación de la interrupción voluntaria del embarazo se ha recurrido a esta terminología justamente para eso. Así, en el artículo 86, inciso 2 se establece la causa de justificación del aborto "[s]i estuviera en riesgo la vida o la salud integral de la persona gestante". Con esta regulación elegante (que no obstante ha sido "observada" por art. 1º del Decreto Nº 14/2021 B.O. 15/01/2021) no se afecta la sistemática de los delitos contra la integridad corporal, pero al mismo tiempo se deja en claro que las conductas que afecten negativamente la salud psíquica de la víctima, provenientes por ejemplo de hostigamiento digital, también configuran lesiones corporales típicas.

La segunda parte de nuestra propuesta consiste en incorporar un tipo penal de "acoso" como delito contra la libertad, siguiendo la propuesta del proyecto Macha. No obstante, hemos tomado como punto de partida la regulación alemana del delito de acoso del § 238 del Código Penal alemán.[18] La razón por la cual hemos utilizado este tipo penal como

[18] El texto del tipo penal alemán es el siguiente (traducción de Leandro Dias):
"§ 238 Acoso
(1) Será castigado con pena de prisión de hasta tres años o con pena de multa quien acose a otra persona de manera no autorizada y de forma idónea para afectar de manera no irrelevante su estilo de vida, al
1. acercarse repetidamente a la persona en cuestión,
2. utilizar medios de telecomunicación u otros medios de comunicación o intentar establecer conacto con esa persona a través de terceros,
3. mediante el uso indebido de datos personales de esta persona
a) realizar pedidos de bienes o servicios para ella o
b) hacer que terceros se pongan en contacto con ella,
4. amenazar a esta persona con atentar contra su vida, integridad física, salud o libertad, o las de uno de sus familiares o de otra persona allegada,
5. cometer un hecho de los §§ 202a, 202b o 202c en perjuicio de esta persona, de uno de sus familiares o de otra persona allegada,
6. difundir o poner a disposición del público una imagen de esta persona, de uno de sus familiares o de otra persona allegada,
7. difundir o poner a disposición del público un contenido (§ 11, párrafo 3) que sea idóneo para menospreciar a esta persona o degradarla ante la opinión pública, engañando sobre la autoría, o
8. realizar una acción comparable a los mencionados en los números 1 a 7.
(2) En casos especialmente graves del párrafo 1, números 1 a 7, el acoso será castigado con pena de prisión de tres meses a cinco años. Por lo general, se considera que el caso es especialmente grave si el autor
1. causa daños a la salud de la víctima, de un familiar de la víctima o de otra allegada a la víctima,
2. pone en peligro de muerte o de lesiones graves a la víctima, a un familiar de la víctima o a otra persona allegada a la víctima,
3. persigue a la víctima mediante múltiples actos durante un período de al menos seis meses,
4. en una acción típica conforme al párrafo 1, número 5, utiliza un programa informático cuyo propósito es espiar digitalmente a otras personas,
5. utiliza una imagen obtenida mediante un acto delictivo conforme al apartado 1, número 5, en un acto delictivo conforme al apartado 1, número 6,
6. utiliza un contenido obtenido mediante una acción típica conforme al párrafo 1, número 5 (§ 11, párrafo 3) en una acción típica conforme al párrafo 1, número 7, o
7. tenga más de veintiún años y la víctima menos de dieciséis.

fuente es que este delito, introducido en el año 2007 para cubrir lagunas de punibilidad en el ámbito del acoso, luego fue modificado en varias ocasiones, a partir de los problemas que fueron surgiendo en la praxis. Así, en el año 2017 se convirtió al tipo penal original de resultado en un delito de aptitud, en el sentido de que no sería necesario un resultado lesivo, sino meramente que la conducta sea apta para afectar la libertad de las víctimas.[19] De ese modo, la punición del hecho dejó de depender de lo que terminase pasando con la víctima. Además, en el año 2021 se reformó el tipo penal con el fin de abarcar adecuadamente los casos de *cybermobbing*, es decir, de acoso llevado a cabo a través de Internet.[20]

En particular, proponemos el siguiente tipo penal:

"ARTÍCULO 149 quarter. - Será reprimido con prisión de seis meses a dos años, al que acosare a otro ilegítima e insistentemente de una forma adecuada para afectar gravemente la configuración de su vida.
Si el hecho fuese cometido a través de Internet, redes sociales, o cualquier sistema informático o medio de comunicación, la pena será de uno a tres años de prisión.
Si el autor, por medio del hecho, causare la muerte de la víctima, de un pariente de la víctima o de otra persona llegada a la víctima, la pena será de uno a diez años de prisión".

A diferencia de lo que puede observarse tanto en el proyecto Macha, como en la regulación alemana, aquí se ha optado por un tipo penal más simple y elegante, que prescinde de los llamados "medios comisivos". Esta simplificación también está basada en el proyecto de María Eugenia Vidal y otros[21] sobre el tema, en el que se propone el siguiente tipo penal: "Será reprimido con prisión de seis (6) meses a dos (2) años al que en forma reiterada e insistente acosare, intimidare, perturbare u hostigare a otro mediante el uso de cualquier medio digital, siempre que el hecho no constituya un delito más severamente penado". Dado que el hostigamiento, la perturbación y la intimidación

(3) Si el autor causa la muerte de la víctima, de un familiar de la víctima o de otra persona allegada a la víctima como consecuencia del hecho, la pena será de prisión de uno a diez años".

[19] Hilgendorf, Eric/Valerius, Brian, *Derecho Penal. Parte Especial*, t. 1, Buenos Aires, Ad-Hoc, 2022, § 4 n.º m. 75.

[20] Kindhäuser, Urs/Hilgendorf, Eric, Strafgesetzbuch. Lehr- und Praxiskommentar, 10.ª ed., Baden-Baden, Nomos, § 238 n.º m. 1.

[21] Cámara de Diputados de Argentina, Expediente 2997-D-2024, 07/06/2024, disponible en: https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2024/PDF2024/TP2024/2997-D-2024.pdf [último acceso: 15/03/2025]).

pueden ser considerados subcasos de acoso, se han condensado esas variantes típicas en una. Además, se ha incorporado una aptitud de la acción, con el fin de excluir del tipo casos de bagatela: el acoso, además de ilegítimo (no consentido) e insistente tiene que ser adecuado para afectar gravemente la configuración de la vida de la víctima.[22] Esto permite abarcar adecuadamente el universo de casos de acoso merecedores de pena, con una agravante para los casos de criminalidad informática. Además, se agrega un tipo agravado por el resultado (o "preterintencional") para aquellos ejemplos en los que el acoso tiene tal entidad que termina produciéndose la muerte de la víctima al menos como una consecuencia previsible del acoso. Incluso en casos de suicidio de la víctima, este tipo penal preterintencional podría ser aplicable, en la medida de que ese suicidio fuese previsible y la víctima no haya actuado de un modo plenamente responsable.[23]

III. Suplantación de identidad en las redes sociales

En los últimos años comenzó a discutirse en la Argentina[24] la posibilidad de crear un delito de "suplantación de identidad digital", hasta el punto de que algunos códigos contravencionales, como el de la Ciudad Autónoma de Buenos Aires, abarcan esta clase de conductas.[25] Esto responde a un fenómeno dañino reciente, que consiste en la utilización del nombre o apellido de una persona física, o el nombre o logo de una persona

[22] Hilgendorf/Valerius, *Derecho Penal. Parte Especial*, t. 1, § 4 n.º m. 89 s.
[23] Hilgendorf/Valerius, *Derecho Penal. Parte Especial*, t. 1, § 4 n.º m. 92.
[24] Véase, en detalle, Borghello, Cristian/Temperini, Marcelo, "Suplantación de identidad digital como delito informático en Argentina", *X Simposio Argentino de Informática y Derecho (SID 2012) (XLI JAIIO)*, 27 al 31 de agosto de 2012), 2012, p. 78 (78 ss.), disponible en: https://sedici.unlp.edu.ar/handle/10915/124395 [último acceso: 15/03/2025]; Mitelli, Noelia/Orloff, Magdalena, "La sustitución de identidad", en Riquert (ed.), *Sistema penal e informática*, vol. 4, Buenos Aires, Hammurabi, 2021, pp. 143 (147 ss.).
Moyano, Lucas, *Ciberdelitos*, Buenos Aires, Hammurabi, 2024, pp. 115 ss.
[25] "Artículo 78 - Suplantación digital de la Identidad - Quien utiliza la imagen y/o datos filiatorios de una persona o crea una identidad falsa con la imagen y/o datos filiatorios de una persona mediante la utilización de cualquier tipo de comunicación electrónica, transmisión de datos, página web y/o cualquier otro medio y se haya realizado sin mediar consentimiento de la víctima, siempre que el hecho no constituya delito, es sancionado con una multa de Ciento sesenta (160) a cuatrocientas (400) unidades fijas o uno (1) a cinco (5) días de trabajo de utilidad pública o de uno (1) a cinco (5) días de arresto.
Las sanciones se elevan al doble cuando:
a. La conducta sea realizada con la finalidad de realizar un banco de datos con la información obtenida.
b. La víctima fuera menor de dieciocho (18) años, mayor de 70 años, o con discapacidad.
c. La contravención sea cometida por el/la cónyuge, ex cónyuge, o a la persona con quien mantiene o ha mantenido una relación de pareja, mediare o no convivencia.
d. La contravención sea cometida por un familiar de hasta el cuarto grado de consanguinidad o segundo grado de afinidad.
e. La contravención sea cometida con el objeto de realizar una oferta de servicios sexuales a través de cualquier medio de comunicación.
El consentimiento de la víctima, siendo menor de 18 años, no será considerado válido.
Acción dependiente de instancia privada con excepción de los casos donde la víctima fuere menor de 18 años de edad.
No configura suplantación de identidad el ejercicio del derecho a la libertad de expresión".

jurídica, sin autorización y en general como antesala de distintos hechos delictivos, como estafas, robos o agresiones sexuales.[26] Dentro de este marco surge la pregunta de si corresponde crear un delito específico para criminalizar esta conducta en el ámbito previo a la comisión de otro delito. Esto es, en efecto, lo que se ha planteado en el último Proyecto de Reforma al Código Penal:[27]

"ARTÍCULO 492. Se impondrá prisión de TRES (3) a SEIS (6) años y SEIS (6) a VEINTICUATRO (24) días-multa, al que a través de Internet, redes sociales, cualquier sistema informático o medio de comunicación, adoptare, creare, se apropiare o utilizare la identidad de una persona física o jurídica que no le pertenezca, con la intención de cometer un delito o de causarles un perjuicio a la persona cuya identidad se suplanta o a terceros".

Creemos que esta propuesta es, en principio, convincente.[28] La suplantación de la identidad de otras personas en redes sociales y otras partes de Internet puede generarles un grave sufrimiento a las víctimas.[29] Esto puede verse ya en los casos usuales en los que se utiliza la identidad de otra persona, tras conseguir acceso a la cuenta de una aplicación de mensajería, para "tomar prestado" dinero de los contactos más estrechos de la víctima. Además, esta propuesta está en línea con nuestra visión de que es preferible una descripción general de la conducta prohibida y no una extremadamente detallada. Así, otros proyectos con estado parlamentario, como el de Danya Tavela,[30] pero también otros,[31] presentan una regulación mucho más detallada, que debería evitarse:

"Artículo 108 quinquies. Suplantación digital de la Identidad - Será reprimido con prisión de seis meses a dos años la persona que se apoderare e utilizare la imagen y/o datos filiatorios de otra persona humana, fallecida o no, o la persona que crea una identidad falsa con la imagen y/o datos filiatorios de otra persona mediante la utilización de cualquier tipo de comunicación electrónica,

[26] Mitelli/Orloff, *Sistema penal e informática*, vol. 4, pp. 143 (147).
[27] Otros antecedentes nacionales en Mitelli/Orloff, *Sistema penal e informática*, vol. 4, pp. 143 (149 ss.).
[28] Para un análisis parcialmente coincidente con este, véase Mitelli/Orloff, *Sistema penal e informática*, vol. 4, pp. 143 (152 ss.); Sueiro, Carlos Christian, "La criminalidad informática en el Proyecto de Ley de Reforma al Código Penal de la Nación del año 2019 (Decreto PEN 103/2017)", *ElDial.com*, DC2E98, 31/08/2021, 1 (11 ss.).
[29] Sobre cómo estas conductas pueden configurar casos de violencia de género, véase Zerda, María Florencia, *Violencia de género digital*, 2.ª ed., Buenos Aires, Hammurabi, 2024, pp. 143 ss.
[30] Cámara de Diputados de Argentina, Expediente 3720-D-2024, 11/07/2024, disponible en: https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2024/PDF2024/TP2024/3720-D-2024.pdf [último acceso: 15/03/2025]).
[31] Solo a modo de ejemplo, véanse los proyectos de María Eugenia Vidal y otros (Expediente 2997-D-2024, ya citado, propuesta de artículos 139ter, quinquies y sexties), así como el de Mónica Macha (Expediente 6318-D-2024, ya citado, propuesta de artículo 139ter).

transmisión de datos, página web y/o cualquier otro medio digital y se haya realizado sin mediar consentimiento de la víctima con la intención de causar un perjuicio a la persona cuya identidad se suplanta o a terceros y/o obtener un beneficio.

Las sanciones se elevan al doble cuando:

a. Cuando la conducta se cometiere con un fin de lucro o con la finalidad de realizar un banco de datos con la información obtenida.

b. Cuando el hecho se cometiere con el objeto de cometer un delito.

c. Cuando la persona afectada fuera menor de 18 años, mayor de 70 años, o con discapacidad.

d. Cuando el hecho se cometiere por persona que esté o haya estado unido a la víctima por matrimonio, unión convivencial o similar relación de afectividad, mediare o no convivencia.

e. Cuando el hecho se cometiere con el objeto de realizar una oferta de servicios sexuales a través de cualquier medio de comunicación.

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

La presente acción es dependiente de instancia privada con excepción de los casos donde la víctima fuere menor de 18 años de edad o incapaz".

Por tanto, consideramos que la base de la regulación debe buscarse en el último Proyecto de Reforma del Código Penal. Sin embargo, creemos que este tipo penal debe ser modificado en distintos sentidos. En primer lugar, la pena es demasiado alta, en particular si se la compara con la pena actual para el delito básico de supresión o alteración del estado civil de otro del artículo 138 del Código Penal (1 a 4 años).[32] Si suprimirle formalmente[33] el estado civil a alguien tiene esa pena baja, "hacerse pasar" por otro en Internet no puede tener una pena ostensiblemente más alta, sino que ha de ser incluso más baja por razones de proporcionalidad. En segundo lugar, consideramos que debe evitarse la descripción de distintas modalidades del hecho que se superponen parcialmente. En el tipo penal, tal como fue redactado en el Proyecto de Código Penal, podría haberse utilizado simplemente el verbo "utilizar", que abarcaría a las otras modalidades sin problemas. De todos modos, creemos que el verbo "suplantar" es más abarcador y lo suficientemente claro como para delinear adecuadamente la conducta delictiva. En tercer

[32] Sorprenden, entonces, las afirmaciones de quienes consideran que la pena es demasiado leve: Mitelli/Orloff, *Sistema penal e informática*, vol. 4, pp. 143 (154). Una pena más alta es incompatible con el sistema actual de protección de la identidad en el Código Penal y sus penas. Pero incluso si no hubiese un problema de compatibilidad y de proporcionalidad de las penas en un sentido ordinal, sí se generarían problemas de proporcionalidad *cardinal*. Este tipo penal, en última instancia, no requiere un daño efectivo a la reputación de la víctima, quien ni siquiera tiene por qué enterarse de lo sucedido. Querer ampliar la pena hasta el punto de superar a varios delitos de lesiones corporales (arts. 89, CP, ss.) no es convincente.

[33] Al respecto, todavía son dignas de ser leídas las explicaciones sobre el tema que brinda Soler, Sebastián, *Derecho Penal Argentino*, t. 3, 4.º ed., Buenos Aires, TEA, 1987, p. 392.

y último lugar consideramos que la referencia a la intención de causar un perjuicio o cometer un delito es innecesaria.[34] Ya el mero hecho de suplantar la identidad digital de una persona es una conducta lo suficientemente injusta como para merecer criminalización sin más. Así, quien suplanta la identidad de alguien, incluso sin una intención de cometer otro delito, está haciendo algo prohibido, contrario a los derechos de imagen de la otra persona y que puede afectar potencialmente su reputación, derechos de imagen y, en definitiva, su "identidad digital". La escala penal reducida, además, permitiría la criminalización de la mera supresión de identidad digital, sin que sea necesaria una intención adicional del autor.

El tipo penal que proponemos, entonces, es el siguiente:

"Artículo 138 bis: Será reprimido con prisión de seis meses a dos años al que, por un acto cualquiera, a través de Internet, redes sociales, cualquier sistema informático o medio de comunicación, suplantase la identidad de una persona física o jurídica".

IV. ¿Delito de peligro abstracto de administración de plataformas comerciales delictivas?

En el año 2021 entró en vigencia en Alemania el § 127, que criminaliza, como delito de peligro, la administración de plataformas de comercio delictivas en Internet.[35] El objetivo formal fue el de combatir el mercado negro de, por ejemplo, estupefacientes, armas y pornografía ilegal, que tiene lugar tanto a través de la *darknet* como de la Internet abierta.[36] No obstante, el objetivo real más bien estuvo centrado en eliminar ciertas dificultades probatorias en estos casos: dado que es complejo acreditar la responsabilidad accesoria de quien administra estos sitios *web* respecto de los hechos puntuales cometidos por los usuarios, se ha decidido criminalizar la administración del sitio sin más, con independencia de los hechos individuales cometidos por los usuarios.[37]

En concreto, el tipo penal alemán es el siguiente:[38]

---

[34] De este modo creemos que quedan disipadas las objeciones que se le hicieron al Proyecto de Reforma del Código Penal, en el sentido de que el elemento subjetivo distinto del dolo restringía en demasía la punibilidad. Así Mitelli/Orloff, *Sistema penal e informática*, vol. 4, pp. 143 (154).

[35] Hilgendorf, Eric/Valerius, Brian/Kusche, Carsten, *Computer- und Internetstrafrecht,* 3.ª ed., Berlin/Heidelberg, Springer, 2023, § 3 n.º m. 474.

[36] En detalle sobre el proceso legislativo inmediatamente anterior a la entrada en vigencia del tipo penal Kusche, Carsten, *Doping, redes sociales y fake news*, Buenos Aires, Editores del Sur, 2022, pp. 43 ss.

[37] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 475.

[38] Traducción de Marcelo Sancinetti.

"§ 127. Explotación de plataformas comerciales delictivas en Internet

1) Quien explota una plataforma comercial en Internet, cuya finalidad esté dirigida a hacer posible o favorecer la comisión de hechos antijurídicos, será penado con pena privativa de libertad de hasta cinco años o con pena de multa, si el hecho no está conminado con pena más grave en otras disposiciones.

Son hechos antijurídicos en el sentido de la oración 1:

1. los crímenes

2. los delitos según:

a) los §§ 86, 86a, 91, 130, 147 y 148, párrafo 1, número 3, los §§ 149, 152a y 176a, párrafo 2, § 176b, párrafo 2, § 180 párrafo 2, el § 184b, párrafo 1, oración 2, § 184c, párrafo 1, § 184l, párrafo 1 y 3, los §§ 202a, 202b, 202c, 202d, 232 y 232a, párrafos 1, 2, 5 y 6, según el § 232b, párrafos 1, 2 y 4, en conexión con el § 232a, párrafo 5, según los §§ 233, 233a, 236, 259 y 260, según el § 261, párrafos 1 y 2, en las condiciones mencionadas en el § 261, párrafo

2, oración 2, así como según los §§ 263, 263a, 267, 269, 275, 276, 303a y 303b,

b) el § 4, párrafo 1 a 3, de la Ley Anti-Doping,

c) el § 29, párrafo 1, oración 1, número 1, también en conexión con el párrafo 6, así como párrafos 2 y 3 de la Ley de Estupefacientes,

d) el § 19, párrafos 1 a 3, de la Ley de Control de sustancias básicas,

e) el § 4, párrafos 1 y 2, de la Ley sobre Nuevas sustancias psicoactivas,

f) el § 95, párrafo 1, números 1 y 2, de la Ley de Medicamentos,

g) el § 52, párrafo 1, números 1 y 2, letras b y c, párrafos 2 y 3, números 1 y 7, así como párrafos 5 y 6, de la Ley de Armas,

h) el § 40, párrafos 1 a 3, de la Ley de Explosivos,

i) el § 13 de la Ley de Materias Primas,

j) el § 83, párrafo 1, números 4 y 5, así como párrafo 4 de la Ley de Protección del patrimonio cultural,

k) los §§ 143, 143a y 144, de la Ley de Marcas, así como

l) los §§ 51 y 65 de la Ley de Diseño.

2) Una plataforma comercial de Internet, en el sentido de esta disposición, es cualquier infraestructura virtual en el área de libre acceso, así como en el ámbito de Internet de acceso restringido por precauciones técnicas, que ofrezca la oportunidad de ofertar o intercambiar personas, bienes, servicios o contenidos (§ 11, párrafo 3).

3) Será penado con pena privativa de libertad de seis meses a diez años quien, en el caso del párrafo 1, actúe en forma habitual o como miembro de una banda que se haya conformado para la comisión continuada de tales hechos.

4) Será penado con pena privativa de libertad de un año a diez años quien, al cometer un hecho del párrafo 1, actúe con la intención o a sabiendas de que la plataforma comercial de Internet tiene la finalidad de hacer posible o favorecer la comisión de crímenes".

Ante esta clase de regulaciones surgen dos preguntas, además de la ya clásica objeción al recurso a una redacción basada en una casuística muy detallada. La primera se vincula a la legitimidad misma de una criminalización así: ¿es legítimo utilizar el derecho penal material solamente para resolver problemas probatorios?[39] Podemos asumir que la respuesta a esta pregunta es afirmativa, aunque los problemas constitucionales que han generado delitos que adoptaron esa estructura, como el enriquecimiento ilícito, permitirían dudar de eso.[40] Pero incluso si eso fuese posible, todavía hay que responder la pregunta de si es necesaria una disposición de esta clase para abarcar las conductas penalmente relevantes.

Desde nuestra perspectiva, un tipo penal de esta clase no es necesario,[41] por los siguientes motivos. Por un lado, muchas de las actividades prohibidas por el derecho penal accesorio, como la venta de drogas, ya incluyen disposiciones ampliatorias de la punibilidad en el estadio previo a la lesión del bien jurídico.[42] Por otro lado, incluso en los ámbitos en los que no existe tal extensión de la punibilidad, las reglas de participación ya son lo suficientemente flexibles como para poder responsabilizar penalmente a los que administran plataformas delictivas.[43] Solo a modo de ejemplo: está aceptada la complicidad por omisión[44] (si existiese una posición de garante, que bien podría existir en caso de sitios *web* creados, por ejemplo, para contratar servicios de sicarios),[45] la complicidad meramente psíquica,[46] e incluso en la Argentina es punible la complicidad

[39] Cf. Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 476.
[40] En detalle respecto de la discusión argentina Sancinetti, Marcelo, *El delito de enriquecimiento ilícito de funcionario público (art. 268, 2, C.P.)*, 3.ª ed., Buenos Aires, Ad-Hoc, 2014, passim. En detalle respecto de la discusión alemana Kliegel, Thomas, *Der Straftatbestand der unerlaubten Bereicherung*, Baden-Baden, Nomos, 2013, passim.
[41] Probablemente de un modo diferente Kusche, *Doping, redes sociales y fake news*, pp. 48 ss.
[42] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 475.
[43] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 475.
[44] Hilgendorf, Eric/Valerius, Brian, *Derecho Penal. Parte General*, 2.ª ed., Buenos Aires, Ad-Hoc, 2017, § 11 n.º m. 98 ss. En la discusión en habla hispana, recientemente López Warriner, "La calidad de intervención por omisión del garante por responsabilidad institucional", *Revista de Derecho Penal y Procesal Penal* 2016, 1864 (1864 ss.), quien incluso va más lejos, al considerar a estos casos (al menos en supuestos de responsabilidad institucional), como autoría.
[45] Véase, al respecto Kusche, *Doping, redes sociales y fake news*, pp. 23 ss.
[46] Hilgendorf/Valerius, *Derecho Penal. Parte General*, 2.ª ed., Buenos Aires, Ad-Hoc, 2017, § 9 n.º m. 147. En la discusión en habla hispana, recientemente Sanromà, Oriol, "La complicidad psíquica", *InDret: Penal* 4 (2023), 221 (223 ss.).

"secundaria" (artículo 46 del Código Penal), es decir, aquella que se produce incluso si la contribución no fue necesaria para realizar el delito.

Si se tiene en cuenta lo señalado, entonces los casos de administración de sitios *web* creados únicamente con fines delictivos ya estarán abarcados al menos por las reglas de complicidad, cuando no por reglas de autoría respecto de tipos penales autónomos, como el de facilitación de estupefacientes a título gratuito (art. 5, in fine, Ley N° 23.737). Y si no están abarcados, surge la pregunta de por qué deberíamos castigarlos. Se podría decir que administrar un sitio *web* comercial dirigido a la comisión de delitos graves es algo peligroso en sí mismo y que merece ser castigado.[47] No obstante, es difícil apreciar cómo ese peligro puede ser diferente al peligro característico de un acto de complicidad en esos delitos. Además, surgen preguntas complejas de aplicación de la ley con un tipo penal como el alemán. ¿La mera administración de un sitio *web* de esa clase ya merece castigo, independientemente de lo que hagan sus usuarios? ¿Y qué sucede con los llamados sitios de "uso doble", es decir, que no están destinados únicamente a la comisión de hechos lesivos, sino que también incluyen fines lícitos?[48] En regulaciones como la alemana, la determinación de si es posible punir la administración de una plataforma comercial de uso doble depende en gran medida del caso concreto.[49] Darle esa posibilidad de uso relativamente discrecional del derecho penal a jueces y fiscales quizá no sea lo más recomendable. Estas consideraciones adquieren todavía una mayor firmeza, si se tiene en cuenta que la Argentina es un país en el que el derecho de libertad de expresión (también en Internet) tiene un alcance mucho más amplio que en países de derecho continental, como Alemania, y los sitios *web* están en gran medida pensados para el ejercicio de la libertad de expresión.

Ante esta situación, consideramos que se debe ser prudente en la criminalización y, de hecho, evitar la sobrecriminalización. Por consiguiente, no consideramos indispensable incluir un tipo penal de esta clase en una reforma de los delitos informáticos y consideramos que las reglas de autoría y participación, en especial las de complicidad, ya brindan herramientas suficientes de persecución penal. Si eso genera problemas de prueba, entonces quizá deba modificarse el procedimiento, no el derecho penal material.

V. Protección adicional contra ataques informáticos

[47] Otra perspectiva en Kusche, *Doping, redes sociales y fake news*, pp. 59 s.
[48] Sobre este tema, véase Kusche, *Doping, redes sociales y fake news*, pp. 51 s.
[49] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 482.

1. Ciberataques

Por último, deben ser realizadas algunas consideraciones sobre la regulación de los ciberataques en la Argentina, así como sobre la protección de la intimidad. En ambos ámbitos, el legislador argentino ha tomado oportunamente medidas de criminalización, a partir de las reformas que realizó sobre criminalidad informática. En especial, la reforma del año 2008, basada en el llamado Convenio de Budapest, criminalizó en gran medida las conductas incorrectas que podrían ser utilizadas para realizar un ciberataque o afectar de otro modo la propiedad o la intimidad de las personas mediante el uso de medio digitales. Surge la pregunta si es necesario realizar una reforma más profunda al respecto, para cubrir más lagunas de punibilidad.

Sobre este tema, debe decirse que la protección penal ofrecida por el derecho penal argentino es, en líneas generales, adecuada.[50] En especial, tipos penales como los de acceso indebido (artículo 153 del Código Penal) y de daño informático (artículo 183, segundo párrafo) permiten captar los casos más importantes de ciberdelincuencia y esto puede verse reflejado en los intentos de reforma integral recientes. Así, el último Proyecto de Código Penal, que establece una sección especial dedicada a los delitos informáticos, mantiene en lo esencial la estructura de regulación de los delitos informáticos actualmente vigentes.[51] Por supuesto, se incorporan ligeras modificaciones, en especial circunstancias agravantes que hoy en día no están presentes y que tienden, por ejemplo, a la mayor protección de ciertos datos y bienes estatales.[52] Pero el núcleo regulativo se mantiene estable.

A su vez, hemos recibido un borrador del grupo de trabajo actual sobre la reforma integral del código, en la que se siguen esencialmente los lineamientos del último Proyecto de Código Penal, más allá de algunas incorporaciones y de un aumento general de penas. Estas decisiones puntuales, vinculadas a las necesidades de pena actuales en la Argentina, deben ser tomadas, por supuesto, en el marco de una reforma integral, que vincule los

[50] Véase Schurjin Almenar, Daniel, "Delitos informáticos en Argentina", *Revista Pensamiento Penal* (ISSN 1853-4554), Marzo de 2022, N.º 412, 1 (3): "En la Argentina una parte de dichas manifestaciones [nota de los autores: manifestaciones = creciente comisión de conductas disvaliosas por medio de tecnologías de la información y comunicación] resulta de susceptible abordaje por el sistema de administración de justicia en materia penal, dado que existen herramientas normativas suficientes para su tratamiento, desde que en 2008 se sancionó la ley de delitos informáticos (N° 26.388), mediante la cual introdujeron diversas reformas al Código Penal, para que quedase en condiciones de ofrecer alternativas ante ese tipo de comportamientos criminales".

[51] Cf. Schurjin Almenar, *Revista Pensamiento Penal*, 1 (3).

[52] Para un panorama de conjunto, véase Schurjin Almenar, *Revista Pensamiento Penal*, 1 (4 ss.); Sueiro, *ElDial.com*, 1 (6 ss.).

delitos informáticos con el resto de los delitos de un modo orgánico. Debido a que el marco actual de regulación de los ciberdelitos en este ámbito es, al menos en líneas generales, adecuado, consideramos que hay que ser prudentes en esta propuesta puntual. La existencia de eventuales lagunas penales tampoco es tan importante, teniendo en cuenta que el Derecho Penal debe seguir el ya mencionado principio de *ultima ratio*: no toda conducta lesiva debe ser criminalizada, ya que el Derecho Penal actúa como último recurso del Estado.[53] Por esa razón, no propondremos mayores cambios en estos ámbitos y dejaremos en manos de quienes trabajan en una reforma integral las modificaciones necesarias según las necesidades de pena que sean constatadas.

No obstante, sí consideramos que, con independencia de una reforma integral, dos tipos penales deberían ser incorporados al Código Penal argentino incluso si no se reformase integralmente el código. Se trata del tipo penal de obstaculización e interrupción del acceso a un sistema informático ajeno y del tipo penal de diseminación de información peligrosa.

El primer tipo penal ya estaba presente en el Proyecto de Reforma del Código Penal y tiende a criminalizar la realización de "ciberataques" que impiden u obstaculizan el acceso a sistemas informáticos.[54] En particular, el tipo penal fue redactado del siguiente modo:

"ARTÍCULO 497.- Se impondrá prisión de UNO (1) a CINCO (5) años, al que ilegítimamente y sin autorización de su titular, mediante cualquier artificio tecnológico, mecanismo de cifrado o programas maliciosos, obstaculizare o interrumpiere el funcionamiento de un sistema informático ajeno o impida a los legítimos usuarios el acceso a los datos del sistema, siempre que el hecho no importe un delito más severamente penado".

Consideramos que este tipo penal va en la dirección correcta, debido a que el daño que causan los ciberataques no puede ceñirse únicamente a las afectaciones a la intimidad o a la causación de daños respecto de cosas materiales o datos, sino también a la imposibilidad de acceder a sistemas informáticos necesarios para la vida cotidiana actual. Esta disposición que actualmente se está discutiendo en la doctrina argentina, entonces, tiene sentido y merece aprobación.[55] No obstante, aquí realizaremos algunas

[53] Cf. Hilgendorf/Valerius, *Derecho Penal. Parte General*, 2.ª ed., § 1 n.º m. 40 s.
[54] Al respecto Schurjin Almenar, *Revista Pensamiento Penal*, 1 (15 s.).
[55] En un sentido similar Sueiro, *ElDial.com*, 1 (24).

modificaciones a la redacción, en especial con fines de simplificación. En cuanto a la clasificación sistemática, consideramos que en el Código Penal argentino actual este tipo penal debe ser configurado como una modalidad del tipo de interrupción o entorpecimiento de comunicaciones (artículo 197), con la siguiente redacción:

"ARTÍCULO 197.- Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida.
En la misma pena incurrirá el que ilegítimamente obstaculizare o interrumpiere el funcionamiento de un sistema informático ajeno o impida a los legítimos usuarios el acceso a los datos del sistema, siempre que el hecho no importe un delito más severamente penado".

Lo primero que debe decirse de esta redacción es que se ha simplificado la acción delictiva, que según nuestra propuesta consiste únicamente en obstaculizar o interrumpir. Mencionar modalidades de la acción ("mediante cualquier artificio tecnológico, mecanismo de cifrado o programas maliciosos") tiene el problema de que en el futuro pueden aparecer casos de obstaculización o impedimento realizados de otro modo y que, por tanto, quedarán impunes. A su vez, se ha dejado únicamente el adverbio "ilegítimamente" en lugar de "ilegítimamente y sin autorización", ya que resulta evidente que una acción sin autorización es ilegítima. Estas modificaciones han sido realizadas, en definitiva, con fines de simplificación y, por un lado, harán más accesible el tipo penal a un público general. Por otro lado, también simplificará el aprendizaje del derecho y su aplicación por parte de jueces y fiscales.
En cuanto a la pena, se considera apropiado, por razones de proporcionalidad ordinal,[56] mantener la escala penal de la interrupción u obstaculización general de comunicaciones. El objetivo de este tipo penal es captar el ilícito que se produce cuando se interrumpe u obstaculiza el acceso a un sistema informático, independientemente de si puede considerarse eso una "comunicación" en un sentido relevante. Así, impedir el acceso a un sistema informático, incluso si iba a ser utilizado sin fines de comunicación con otra persona, adquiere relevancia penal. No resulta evidente por qué estos casos, entonces, deberían tener más pena que los casos de interrupciones de comunicaciones. En caso de

[56] Cf. Von Hirsch, Andrew, "Proportionality in the Philosophy of Punishment", *Crime and Justice* 16 (1992), 55 (75 ss.). Sobre la discusión más reciente, véase también Basso, Gonzalo, *Determinación judicial de la pena y proporcionalidad con el hecho*, Madrid, Marcial Pons, 2019, pp. 244 ss.

que la pena sea considerada demasiado baja, sería necesario realizar una reforma integral que aumente la pena de todos los delitos de esta clase y, posiblemente, también las penas del resto de los delitos del Código Penal. Razones de "proporcionalidad ordinal" impiden, por tanto, utilizar la escala penal propuesta en el Proyecto de Reforma.

Por supuesto, y como ha señalado parte de la doctrina, la pena debería ser mayor en ciertos casos, como aquellos que se realizan desde un país a otro con el fin de producir graves perjuicios.[57] Esto está garantizado por la cláusula de subsidiariedad establecida en el tipo penal. Solo a modo de ejemplo: si el ciberataque puede ser considerado como una conducta típica de un crimen internacional, como un crimen de guerra, entonces regirán las disposiciones respectivas del derecho penal internacional, con penas superiores según la ley 26.200 (con las penas del artículo 10 para los crímenes de guerra).[58]

2. Difusión de información para crear listas negras y "doxear"

Para cerrar este informe, consideramos que una decisión reciente del legislador alemán puede ayudar a cubrir lagunas de punibilidad importantes en la Argentina. En particular, en los últimos años se ha expandido el fenómeno de las listas negras de enemigos[59] y del llamado "doxing": casos en los que se difunden públicamente, en especial a partir de Internet, datos personales, por diversos motivos ilícitos.[60] Así, en ocasiones se recurre a esta práctica para intimidar a enemigos políticos, otras veces para hostigar a alguien o dañar su reputación.[61]

El legislador alemán decidió prohibir en 2021 esta clase de conductas,[62] con independencia de si terminan causándole un daño a la víctima, ya por el hecho de que la revelación de esos datos implica una forma agravada de violación a la intimidad que coloca a la víctima en una situación de indefensión ante posibles autores indeterminados de otros delitos.[63] En particular, el nuevo § 126a dice lo siguiente:[64]

"§ 126a. Difusión peligrosa de datos personales

[57] Así, en particular, Sueiro, *ElDial.com*, 1 (24 s.).
[58] Probablemente coincidente Sueiro, *ElDial.com*, 1 (24).
[59] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 138.
[60] En detalle Kubiciel, Michael/Großmann, Sven, "Doxing als Testfall für das Datenschutzstrafrecht", *NJW* 2019, 1050 (1050 s.).
[61] Véase Moyano, Lucas, *Ciberdelitos*, Buenos Aires, Hammurabi, 2024, p. 111.
[62] Más detalles en Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 138.
[63] Sobre la estructura del tipo penal alemán, véase Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 143.
[64] Traducción de Marcelo Sancinetti.

1) Quien, públicamente, en una reunión o por la difusión de un contenido (§ 11, párrafo 3), difunda datos personales de otra persona, de tal manera que resulte apropiada para poner en peligro a esa persona o a una persona cercana a ella y, según las circunstancias, destinada a ello, la exponga a sufrir:

1. un crimen dirigido contra ella o
2. un hecho antijurídico de otra índole dirigido contra ella, contra la autodeterminación sexual, la incolumidad corporal, la libertad personal o contra una cosa de valor significativo,

es penado con pena privativa de libertad de hasta dos años o con pena de multa.

2) Si se trata de datos no accesibles al público en general, la pena es privativa de libertad de hasta tres años o pena de multa.

3) El § 86, párrafo 4, rige en lo correspondiente".

Esta disposición merece aprobación. Cuando se publican en Internet estas listas negras o se "doxea" abiertamente a alguien, los resultados dañinos son impredecibles, muchas veces acompañados de sutiles amenazas, en especial si se revelan datos sensibles como la dirección de la persona y sus familiares.[65] Para castigar adecuadamente estos casos (hoy en día impunes en Argentina),[66] incluso si no termina produciéndose ninguna consecuencia que vaya más allá de la revelación pública de información, proponemos el siguiente tipo penal, en línea con el alemán:

"Artículo 153 ter.

Será reprimido con una pena de prisión de uno a tres años el que públicamente, en una reunión o por medio de una difusión de contenido digital, difunda datos personales de otra persona, de manera tal que ello resulte adecuado para causarle un perjuicio a esa persona o a una persona cercana a ella.

No son punibles los actos realizados en ejercicio de derechos constitucionales u otros intereses legítimos".

A diferencia de otros delitos de violación de secretos, aquí la pena es un poco más alta por el carácter peligroso en abstracto de la acción: se trata de un delito de aptitud o idoneidad, que no requiere un resultado lesivo separado de la acción.[67] Además, hemos decidido simplificar el tipo penal en relación con el alemán: no es necesaria una intención

[65] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 139 s.
[66] Así también Moyano, Lucas, *Ciberdelitos*, Buenos Aires, Hammurabi, 2024, p. 111.
[67] Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 143 s.

de que la víctima se vea expuesta a un delito de cierta clase, sino solamente que la conducta sea adecuada para causar un perjuicio. Por supuesto, los casos de exposición a un delito por parte de terceros también están incluidos en el tipo, siempre que la conducta ponga en peligro abstractamente alguno de estos bienes jurídicos. Esta cláusula, además, permite otorgarle un poco más de determinación al tipo penal, cuya aptitud tiene que estar vinculada a la causación de un perjuicio de la víctima y no solo al sufrimiento de un peligro indeterminado.[68] Finalmente, se ha incluido una cláusula de impunidad en casos de ejercicio de intereses legítimos, equivalente a la propuesta para el delito de difusión de *deepfakes* denigrantes. De este modo, quedan saldadas eventuales objeciones basadas en el alcance de, por ejemplo, el derecho de libertad de expresión en la Argentina.[69] Además, esto permite solucionar un grupo de casos de difícil solución para el tipo penal alemán: la publicación de informes objetivos e informativos sobre, por ejemplo, las faltas cometidas por personas públicas.[70] La cláusula de protección de intereses legítimos deja impunes estos casos sin mayores problemas.

VI. Conclusión

Para concluir esta última conferencia, podemos resumir nuestra propuesta del siguiente modo:

1) Para castigar adecuadamente los casos de ciberacoso, es necesaria una ligera modificación del delito de lesiones leves, así como la creación de un tipo penal de acoso como delito contra la libertad.

2) Un tipo penal de suplantación de identidad también resulta necesario para castigar adecuadamente los casos que, sin dar lugar a una lesión formal al estado civil de una persona, son adecuados para dañar su "identidad digital".

3) No consideramos necesaria la creación de un tipo penal de administración de plataformas de comercio delictivo, dado que las reglas de autoría y participación, así como las reglas especiales del derecho penal accesorio, parecen ser suficientes para castigar estos casos.

4) Un tipo dirigido a criminalizar ciberataques que impiden o dificultan el acceso a sistemas informáticos también luce necesario dada la realidad actual.

---

[68] Para una crítica a esta característica del tipo penal alemán Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 144.
[69] Agradecemos a Marcos Salt por señalar esta cuestión durante la presentación de este informe.
[70] Sobre esta discusión Hilgendorf/Valerius/Kusche, *Computer- und Internetstrafrecht,* § 3 n.º m. 145.

5) Por último, un tipo penal de difusión peligrosa de datos personales también sería necesario para castigar las recientes prácticas de creación de listas negras y doxeos.

Resumen de la propuesta legislativa

1) Modificación del art. 73, CP, para que los delitos de los arts. 153 bis y 157 bis pasen a ser delitos de acción pública. También el art. 153 ter deberá ser considerado de acción pública:

"Artículo 73.- Son acciones privadas las que nacen de los siguientes delitos: […] 2) Violación de secretos, salvo en los casos de los artículos 153 bis, 153 ter, 154, 157 y 157 bis"

2) Modificación del artículo 173, inc. 16, CP en tres sentidos: ampliación del tipo de fraude informático, creación de un delito de "phishing" y creación de un delito de peligro abstracto de preparación de un fraude informático:

"Artículo 173.- No obstante lo dispuesto con carácter general en el artículo anterior, se tendrán en cuenta los casos especiales de estafa, a los que se impondrá la misma pena que en el artículo 172.

[…]

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, o mediante el uso no autorizado de sus datos.

El que, con intención de perjudicar a otro, emprendiere la inducción al destinatario a revelar contraseñas u otros datos de acceso en comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, proporcionándole información falsa o mediante cualquier otro engaño, será reprimido con prisión de un mes a tres años.

El que prepare un delito según el primer párrafo de este inciso al elaborar, procurarse o procurarle a un tercero, poner en venta, conservar o entregarle a un tercero un programa de computación cuyo fin sea la comisión de un delito de esa clase será reprimido con prisión de un mes a tres años".

3) Creación del delito de difusión no autorizada de imágenes o videos íntimos (art. 155bis):

"Artículo 155bis:

Será reprimido con pena de seis meses a dos años el que de manera no autorizada pusiere a disposición de terceros fotografías o grabaciones de audio o video sexuales o de partes

íntimas de la víctima, después de haberlas producido con conocimiento de la otra parte o sin él o después de haberlas recibido de ella u obtenido de otro modo.
La pena prevista en el párrafo anterior se aumentará en un tercio en su mínimo y en su máximo: 1°) Si el hecho fuese cometido por persona que esté o haya estado unida a la víctima por relación especial de confianza
2°) Si el hecho fuese cometido con ánimo de lucro".

4) Creación del delito de difusión de imágenes denigrantes producidas o modificadas por medios informáticos (art. 117bis):
"Artículo 117 bis:
El que deshonrare o desacreditare gravemente a otra persona poniendo a disposición de un tercero imágenes o videos producidos o modificados por medios informáticos y que den la impresión de ser fieles a la realidad del aspecto, comportamiento o manifestaciones orales de esa persona, será castigado con prisión de un mes a un año.
En los casos del primer párrafo, la pena máxima de prisión se elevará a dos años si las imágenes o videos se hacen accesibles a la generalidad o si se trata de un asunto relacionado con una esfera altamente personal de la vida, como la sexualidad de la víctima.
No son punibles los actos realizados en ejercicio de derechos constitucionales u otros intereses legítimos".

5) Modificación del delito de lesiones corporales leves para incluir las lesiones psicológicas:
"Artículo 89. - Se impondrá prisión de un mes a un año, al que causare a otro, en el cuerpo o en la salud integral, un daño que no esté previsto en otra disposición de este código".

6) Creación del delito de acoso (art. 149 quarter):
"Artículo 149 quarter. – Será reprimido con prisión de seis meses a dos años, al que acosare a otro ilegítima e insistentemente de una forma adecuada para afectar gravemente la configuración de su vida.
Si el hecho fuese cometido a través de Internet, redes sociales, o cualquier sistema informático o medio de comunicación, la pena será de uno a tres años de prisión.
Si el autor, por medio del hecho, causare la muerte de la víctima, de un pariente de la víctima o de otra persona llegada a la víctima, la pena será de uno a diez años de prisión".

7) Creación del delito de suplantación de identidad en Internet (art. 138 bis):

"Artículo 138 bis: Será reprimido con prisión de seis meses a dos años al que, por un acto cualquiera, a través de Internet, redes sociales, cualquier sistema informático o medio de comunicación, suplantase la identidad de una persona física o jurídica".

8) Modificación del art. 197, CP, con el fin de crear el delito de obstaculización del funcionamiento de un sistema informático (art. 197, segundo párrafo):

"Artículo 197.- Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida.

En la misma pena incurrirá el que ilegítimamente obstaculizare o interrumpiere el funcionamiento de un sistema informático ajeno o impida a los legítimos usuarios el acceso a los datos del sistema, siempre que el hecho no importe un delito más severamente penado".

9) Creación del delito de difusión de información personal peligrosa (art. 153 ter):

"Artículo 153 ter.

Será reprimido con una pena de prisión de uno a tres años el que públicamente, en una reunión o por medio de una difusión de contenido digital, difunda datos personales de otra persona, de manera tal que ello resulte adecuado para causarle un perjuicio a esa persona o a una persona cercana a ella.

No son punibles los actos realizados en ejercicio de derechos constitucionales u otros intereses legítimos".