Reportantes de vulnerabilidades en sistemas digitales ante la ley penal argentina

DEMOCRACIA EN RED

O.D.I.A.

Fundación Vía Libre

Este trabajo es producto de la colaboración entre Democracia en Red, Fundación Vía Libre y el Observatorio de Derecho Informático Argentino (O.D.I.A), con el apoyo de Indela.
democraciaenred.org / vialibre.org.ar/ odia.legal / indela.fund

La presente versión fue escrita por Eliana Andrade, Martín Bartumeu Orpelli, Ezequiel Quaine y Alejandro Piagentini

---

DEMOCRACIA EN RED

O.D.I.A.

Fundación Vía Libre

Reportantes de vulnerabilidades en sistemas digitales ante la ley penal argentina

Contenidos

1. Introducción

Hay tres cosas que el Estado argentino -en general- y sus agencias encargadas de investigar y aplicar el derecho penal, no han tenido en consideración: la seguridad digital de los sistemas informáticos, sus vulnerabilidades y los problemas derivados de la falta o incorrecta forma de gestionarlas.

Basta repasar las noticias de los últimos diez años para confirmar la total falta de interés en desarrollar políticas en torno a la seguridad informática de los sistemas empleados por las distintas dependencias del estado.

A tal punto no se comprende la dimensión de los problemas relacionados a la temática señalada, que muchos de los "delitos informáticos" sancionados por la ley 26.388 fueron incorporados en el capítulo que tutela la violación de secretos y la información de carácter personal. Los legisladores sustituyeron el epígrafe existente en el Código Penal por "Violación de secretos y de la privacidad" para así enfatizar que el bien jurídico que los tipos penales buscan tutelar y proteger es la privacidad de la información y los datos de carácter personal.

Pero, ¿qué pasa cuando lo que está en juego es "la seguridad del sistema o dato informático" y no la privacidad o dato personal de una persona?; ¿es la "seguridad informática" (o la "indemnidad de los sistemas de transmisión de datos" o "seguridad de los sistemas informáticos" o "seguridad de las redes o sistemas de información" o "la integridad y confidencialidad de los datos y programas informáticos como elementos del sistema", o el término que ustedes gusten construir), un bien jurídico tutelado por nuestro ordenamiento penal? ¿Es correcto utilizar los tipos penales existentes para perseguir a aquellos investigadores en seguridad informática que se dedican a encontrar y reportar vulnerabilidades para contribuir a la seguridad de los sistemas, o hay otra solución?

Este reporte propone y fundamentará, en primer lugar, que la investigación y reporte de vulnerabilidades de sistemas informáticos por parte de investigadores en seguridad informática no debe ser criminalizada a través de los delitos previstos en los arts. 153 bis y 157 bis del CP. En segundo lugar, exhortará al desarrollo sostenido de políticas estatales para el reporte seguro y la divulgación coordinada de vulnerabilidades para su mejor gestión, en pos de contribuir a la seguridad de los sistemas.

1.1. La vida atravesada por códigos

Como abogados, sabemos que la vida está atravesada por códigos, pero no nos referimos a aquellos sancionados por un órgano legislativo, sino a los códigos que "corren" la transformación de nuestras vidas en los entornos digitales. Todas nuestras computadores y teléfonos corren código; la información "circula" a través de internet gracias al código; desde cosas que hacen a nuestro quehacer diario (*internet of Things*), hasta el manejo de complejos industriales que proveen servicios a las grandes ciudades.

Pero los códigos no son perfectos; como todos los sistemas, tienen vulnerabilidades, es decir, debilidades que pueden ser explotadas y así producir daños en el sistema con repercusiones económicas, sociales, jurídicas y políticas.

1.2. Las vulnerabilidades

Si bien la extensión del concepto "vulnerabilidad" puede variar según el documento consultado, podemos definirla como una debilidad en el software, el hardware o en el servicio online que puede ser explotada. La vulnerabilidad puede ser causada tanto por problemas de diseño del software como del hardware, por fallas de programación o errores de implementación, de administración y/o control, que ponen en juego la confidencialidad, integridad y disponibilidad del sistema[1].

En lo que nos respecta, no debemos olvidar que la gestión de vulnerabilidades es un proceso más dentro de las prácticas de seguridad de la información y que una vulnerabilidad explotada puede traducirse en una afectación concreta a los derechos de las personas. Es por ello, que el reporte de vulnerabilidades constituye una forma de proteger los derechos de las personas, y en tal sentido debe ser alentada por el Estado y no criminalizada.

1.3. Los investigadores que reportan vulnerabilidades

Una gama muy amplia de personas y organizaciones se encuentran abocadas a encontrar vulnerabilidades: desde los propios usuarios del sistema o producto, pasando por los desarrolladores y/o "testers", los administradores de sistemas, los investigadores amateurs y profesionales en seguridad informática, hasta equipos y divisiones militares de seguridad

[1] ver. ISO/IEC 27000 e ISO/IEC 29147.

ofensiva de estados nacionales. Y, por supuesto, delincuentes, es decir, personas que realizan las conductas tipificadas en los códigos penales.

En este reporte, optamos por abandonar la constelación de términos asociados a una práctica definida como *hacking* ético o *hacktivismo* (*white hacker*, *white hats*, etc) por los equívocos que suscitan y las connotaciones negativas que el término *"hacker/hacking"* tiene en el imaginario global. Por eso preferimos considerar al agente que reporta una vulnerabilidad como un "investigador en seguridad digital", siguiendo las caracterizaciones elaboradas por la OECD -*Security researcher*- y la ISO/IEC 29147 - *finder*-, término que consideramos más neutral y menos ambiguo que *"hacker"*.

La ISO/IEC 29147 define al *"Finder"* -buscador- como una persona u organización que identifica una potencial vulnerabilidad en un producto o servicio online. Un *"Finder"* puede ser tanto un investigador en seguridad informática, como un usuario o el mismo propietario del producto. Sea la calidad que revista, el *"finder"*, para el propósito dispuesto en el estándar internacional citado, es quien reporta o informa al dueño o responsable del producto acerca de la vulnerabilidad.

No desconocemos que la práctica de un investigador en seguridad informática involucra tareas "legalmente riesgosas" porque implica, no sólo buscar vulnerabilidades, sino que también puede comprender la realización de pruebas de funcionamiento de los controles de seguridad; el desarrollo de herramientas o programas para "explotar" las vulnerabilidades encontradas, y hasta realizar ingeniería inversa de productos (lo que supone potenciales conflictos con la legislación en materia de derechos de autor/patentes/licencias).

Los propósitos de un investigador para buscar vulnerabilidades pueden ser muy amplios, desde determinar y mejorar la calidad del software; desentrañar por qué algo falla o funciona mal; estimar riesgos de seguridad para usuarios; aprender seguridad informática (crecimiento profesional); hasta autopromoción, marketing, vanidad, entre muchos otros.

Lo importante es destacar que la actividad de los investigadores en seguridad digital que encuentran, analizan y reportan vulnerabilidades, es la que impulsa necesariamente el permanente desarrollo de los sistemas informáticos y los entornos digitales. Ello hace que se vuelvan cada vez más sofisticados y seguros frente a violaciones de datos, sustracción de información, y otros ataques a la seguridad constitutivos de maniobras que perjudican a terceros, y cuyo contenido es sin dudas criminal.

1.4. La criminalización sin distinción

Al emplear el término "criminalización" nos referimos al proceso por el cual ciertas agencias del Estado seleccionan a un reducido grupo de personas, a las que someten a su coacción con el fin de imponerles una pena.

El proceso selectivo de criminalización se desarrolla en dos etapas, denominadas respectivamente, primaria y secundaria. Criminalización primaria es el acto y el efecto de sancionar una ley penal material, que incrimina o permite la punición de ciertas personas[2]. En nuestro caso, los tipos previstos en los arts. 153 bis y 157 bis del CP.

Como consecuencia del desconocimiento de los problemas relativos a la ciberseguridad y a una deficiente técnica legislativa (tal como se demostrará en el capítulo siguiente), los investigadores en seguridad aparecen comprendidos dentro del recorte realizado por los tipos penales.

Mientras que la criminalización primaria (hacer leyes penales) es una declaración que usualmente se refiere a conductas o actos, la criminalización secundaria es la acción punitiva ejercida sobre personas concretas[3]. Es la que tiene lugar cuando las agencias policiales detectan a una persona, a la que se atribuye la realización de cierto acto criminalizado primariamente, la investiga, en algunos casos la priva de su libertad ambulatoria, la somete a la agencia judicial. Esta última legitima lo actuado, y admite un proceso que eventualmente puede concluir en la imposición de una pena.

Una legislación deficiente, sumada a una limitada comprensión del fenómeno relativo a la investigación en seguridad de los sistemas de información, una selectividad que no hace distinciones en torno a las prácticas de una comunidad[4] -como es la comunidad de infosec- y una autorización desmedida a las agencias policiales son las variables que nos llevan a casos tan elocuentes como los procesos llevados contra los investigadores Sorianello, Ortmann y Smaldone[5].

[2] ZAFFARONI, E. R.; ALAGIA, A.; SLOKAR, A., *Derecho Penal. Parte General*, ed. Ediar, Bs. As., 2002, p. 7.

[3] Ibidem., p. 8/15.

[4] SILVA SÁNCHEZ, J. M., *La expansión del Derecho penal*, ed. B de F, Montevideo – Bs. As., 2011, p. 91 y stes.

[5] Ver apéndice nro. 2 sobre jurisprudencia local.

2. Vulnerabilidades y derecho penal

2.1. El problema del bien jurídico tutelado en el capítulo III del Título V -Libro segundo- del Código Penal: ¿se tutela la privacidad o la seguridad de los sistemas de información?

Los artículos 153 bis y 157 bis del Código Penal, se ubican dentro del título quinto de delitos contra la libertad, particularmente en el capítulo tercero, ligado a la Violación de Secretos y de la Privacidad.

Entonces, una interpretación coherente con la Constitución Nacional y el propio Código Penal obligan a sostener que lo que afecta el intrusismo informático son los derechos de confidencialidad y exclusividad que el titular de la información posee sobre la misma, por lo que se vulneraría el ámbito de intimidad como extensión de los atributos de la persona[6].

Tal intelección recurre al artículo 18 de la Constitución Nacional, en cuanto refiere a la inviolabilidad de la correspondencia epistolar y los papeles privados, como derecho fundamental[7]. Ello se compagina con el principio de reserva normado en el artículo 19 constitucional, que reconoce un ámbito privado al ciudadano frente a la injerencia del Estado o los demás particulares[8].

De tal suerte, quienes sostienen que el bien jurídico que las figuras pretenderían "proteger" es la intimidad señalan que los datos almacenados en un dispositivo informático -celular, computadora, tablet, gps, etc.- están alcanzados por el derecho a la intimidad y la expectativa de privacidad[9].

[6] TERRAGNI, M. A., *Tratado de Derecho Penal. Tomo II Parte Especial I*, Ed. La Ley, Bs. As., 2012, p. 541.

[7] NINO, C., *Fundamentos de derecho constitucional*, ed. Astrea, Bs. As., 2002, p. 333; CARRIÓ, A., "Garantías constitucionales en el proceso penal", 5ª ed., Hammurabi, Buenos Aires, 2012, ps. 353 y ss.; RIQUERT, M., *Protección penal de la intimidad en el espacio virtual*, Ediar, Buenos Aires, 2003, p. 44.

[8] ABOSO, G. E., "Delitos contra la intimidad y la privacidad: acceso indebido a comunicaciones electrónicas, datos sensibles y sistemas informáticos", en Revista de Derecho Penal y Criminología ed. Thomson Reuters nro. 1775, Bs. As., del 11/08/17, p. 3.

[9] FERRER, E., "La prueba obtenida a través del acceso remoto a sistemas informáticos y su validez en el proceso penal", *Revista de Derecho Penal* 1556/2020, ed. Rubinzal Culzoni, Santa Fe, 2020; y ABOSO, "La inconstitucionalidad de la requisa y el examen sin autorización judicial de datos personales almacenados en dispositivos celulares de personas detenidas-Breve reseña de los fallos `Riley vs. California´ (573 U.S. 132 (2014) y `United States vs. Brima Wurie´ (573 U.S. 212 (2012) de la Corte Suprema de Justicia de los Estados Unidos", publicado en Biblioteca Jurídica Online el Dial, el 31/7/14 (DC1D2F); VOGEL, "Informationstechnologische Herausforderungen an das Strafprozessrecht", Zeitschrift für Internationale Strafrechtswissenschaft (ZIS), Heft 8-9/2012, pp. 480 y ss.; STS, Sala de lo Penal, N° Resolución 204/2016, del 10/3/16 (Ponente Cándido Conde-Pumpido Touron); este último citado en ABOSO, G. E., "Delitos contra..., cit., p. 2.

Consecuentemente, sólo debería estar sancionado con pena aquel comportamiento que sea apto para lesionar de manera grave o significativa la confidencialidad de los datos de naturaleza personal, vale decir, los que integran el núcleo básico de la intimidad personal[10] (la "autodeterminación informativa"[11] como un nuevo derecho de autotutela de la propia identidad informática; cuya función se cifra en garantizar a los ciudadanos facultades de información, acceso y control de los datos que les conciernen[12]). A esta altura, parece lo más razonable desde una perspectiva respetuosa del Estado de Derecho, remarcar que los datos deben estar necesariamente vinculados a un sujeto de derecho, y su contenido debe ser íntimo, pues sólo así resultaría razonable considerar una afectación real[13]. Por el contrario, debemos interpretar que si ello no sucede, no podemos considerar que se afectó el bien jurídico, por lo que no habría delito.

Pero, en principio, el Código nada dice acerca de entender a "la seguridad del sistema o dato informático" como bien jurídico tutelado por los delitos mencionados.

Por otra parte, para un sector de la doctrina internacional, el delito de intrusismo viene a proteger un "nuevo valor social", que se cifra exclusivamente en la seguridad de los sistemas informáticos[14], y habrá afectación penalmente relevante -delito- en el mero acceso al sistema informático, no siendo necesario que el intruso acceda al mismo tiempo al contenido de los datos almacenados en el sistema, por lo que se vulnera sólo la "información" o el dato como tal[15], sin importar si se trata de datos íntimos o si se afectó la autodeterminación informativa del titular de los datos.

Se trata de un bien jurídico sin sustento en la Constitución ni en los Pactos Internacionales de Derechos Humanos, añadido doctrinariamente para dar respuesta a una necesidad meramente preventiva[16] (y así habilitar la criminalización secundaria de los investigadores en seguridad).

[10] ABOSO, G. E., "Delitos contra..., cit., p. 10.

[11] FALIERO, J. C., *La protección de datos personales*, ed. Ad Hoc, 2da edición, Bs. As., 2021, p. 86.

[12] PÉREZ LUÑO, A., *Derechos Humanos, Estado de Derecho y Constitución*, ed. Tecnos, Madrid, 1995, p. 378.

[13] BRENDA, E.; MAIHOFER, W.; VOGUEL H. J.; HESSE, K.; HEYDE, W., *Manual de Derecho Constitucional*, trad. López Pina, ed. Marcial Pons, Madrid, 1996, p. 131.

[14] MORON LERMA, E., *Internet y Derecho Penal: Hacking y otras conductas Ilícitas en la Red*, ed. Aranzandi, Navarra, 1999, p. 84; ROMEO CASABONA, C. M, "Política criminal de la Unión Europea sobre los ciberdelitos", *Derecho penal. Parte especial, conforme a las Leyes Orgánicas 1 y 2/2015*, Romeo Casabona, Sola Reche y Boldova Pasmar (coords.), ed. Comares, Granada, 2016, p. 270.

[15] VILLAVICENCIO TERREROS, F., "Delitos Informáticos", *Revista IUS ET VERITAS*, nro. 49, Diciembre, Lima, 2014, p. 49.

[16] COLÁS TURÉGANO, A., "El delito de intrusismo informático tras la reforma del CP español de 2015", *Revista Boliviana de Derecho Nº 21*, enero 2016, p. 216.

Tal interpretación busca punir una violación de las medidas de resguardo de redes y sistemas, apareciendo la seguridad informática como un nuevo bien jurídico colectivo o supraindividual[17], basado en la necesidad político criminal de tutelar la indemnidad de los sistemas de transmisión de datos.

La indemnidad de los sistemas informáticos, como interés sostenido desde una perspectiva transpersonalista, no es un derecho fundamental reconocido por nuestra Constitución ni Tratados Internacionales[18].

Ante este panorama, una perspectiva respetuosa del Estado de Derecho, afincada en principios de raigambre constitucional y convencional, nos lleva a rechazar por irrazonables posturas como esta última, en las que se propone crear un bien jurídico no a partir de las normas fundamentales de nuestras comunidades jurídicas, sino a partir de fundamentos ónticos o extrajurídicos coyunturales, carentes de anclaje legal. Lo cual, desde la más rudimentaria lógica de validación normativa[19], no resulta aceptable.

Ante estas apreciaciones, se estima que una exégesis de las figuras debe prescindir de esa intelección del bien jurídico, por lo que se vislumbra como más razonable y ajustada al Estado de Derecho, la interpretación que propone a la intimidad o la autodeterminación informativa como bien jurídico objeto de las normas[20].

Esta postura además, es la que da mayores garantías a la labor del investigador en seguridad.

2.2. Análisis del delito de acceso no autorizado a un sistema o dato informático

i. Antecedentes y marco normativo

a. Hacia la Convención de Budapest

[17] CARRASCO ANDRINO, M., "El delito de acceso ilícito a los sistemas informáticos", *Comentarios a la reforma penal de 2010*, dir. Álvarez García y González Cussac, ed. Tirant lo Blanch, Valencia, 2010, p. 250.

[18] ROMEO CASABONA, C. M, "Política criminal de la Unión Europea sobre los ciberdelitos", *Derecho penal. Parte especial, conforme a las Leyes Orgánicas 1 y 2/2015*, Romeo Casabona, Sola Reche y Boldova Pasmar (coords.), ed. Comares, Granada, 2016, p. 381 y ss.; MUÑOZ CONDE, F., *Derecho penal. Parte especial,* ed. Tirant lo Blanch, Madrid, 2019, p. 240 y ss.

[19] KELSEN, H., *Teoría Pura del Derecho. Introducción a los problemas de la ciencia jurídica*, trad. Robles-Sánchez, ed. Trotta, Madrid, 2011, p. 142 y stes.

[20] PIAGENTINI, A., "El delito de intrusismo informático", en *Estudios de Cibercrimen*, Ferrer (dir.), ed. Olejnik, Santiago de Chile, 2021, p. 110/2.

Uno de los primeros antecedentes de la figura utilizada para perseguir el *hacking* se remonta a un caso que tuvo lugar en 1988 en Reino Unido, cuando Edward Austin Singh fue arrestado por acceder de manera no autorizada a bases de datos ajenas desde su computadora en la Universidad de Surrey. Singh no pudo ser acusado y procesado formalmente en ese momento, porque la ley británica no regulaba esa conducta mediante el empleo de una computadora. Pero, la relevancia del caso es que motivó la sanción de una ley denominada *Computer Misuse Act 1990*, cuyo capítulo dieciocho prohibió el acceso no autorizado a un sistema de tratamiento y almacenamiento de datos[21]. Así, el primer antecedente normativo corresponde a Gran Bretaña, donde se comenzó a perseguir la intrusión indebida bajo el término de *unauthorized access*[22].

Posteriormente, el fenómeno se extendió a nivel global, donde se relevaron perjuicios generados por fallas de seguridad explotadas por delincuentes con conocimientos especiales en informática, lo cual generó la necesidad de arribar a consensos internacionales para la colaboración y persecución de este nuevo modo de delincuencia.

Fue en tal contexto en que se firmó el Convenio sobre Cibercriminalidad de Budapest, elaborado en el seno del Consejo de Europa el 23 de noviembre de 2001[23]. Se trata de un instrumento de cooperación en materia penal, que prevé descripciones de conductas prohibidas o "delitos informáticos" que los países firmantes se han comprometido a sancionar en sus sistemas jurídicos internos, con el objeto de armonizar la legislación penal global[24].

En lo referido al acceso no autorizado a un sistema informático, esa pieza establece en su artículo segundo el delito de acceso ilícito, que dice: *Artículo 2 – Acceso ilícito. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguri-*

[21] WINDER, "Computer Misuse Act: life in prison for UL hackers", IT Security Thing.com, publicado el 1/11/16 en ABOSO, G. E., "Delitos contra la intimidad y la privacidad: acceso indebido a comunicaciones electrónicas, datos sensibles y sistemas informáticos", en Revista de Derecho Penal y Criminología ed. Thomson Reuters nro. 1775, Bs. As., del 11/08/17, p. 10.

[22] JONES, B. R., "Virtual neighborhood watch: open Source software and community policing against cybercrime", The Journal of Criminal Law and Criminology, Vol. Nº 97, Nº 2 (2007), p. 605 y ss.

[23] ROIBON, M. M, "Reflexiones sobre el acceso ilegítimo a un sistema o dato informático", *Cibercrimen y Delitos Informáticos*, Ed. Erreius, Bs. As., 2018, p. 132.

[24] GARAT, S.; REALE, J., "La reforma penal en materia de cibercrimen en la República Argentina", en *Cibercrimen II*, DUPUY, D. (Dir.) y KIEFER, M. (Coord.), ed. BdeF, Montevideo-Bs. As., 2019, p. 487.

dad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.[25]

De una primera lectura, puede advertirse que la norma no impone una regulación exhaustiva y/o prescriptiva de la totalidad de los elementos de la prohibición -tipo objetivo-, sino que faculta a los Estados firmantes a diseñar legislativamente las condiciones específicas de la figura, en cuanto a infracción de medidas de seguridad, elementos subjetivos distintos del dolo atinentes a la motivación y finalidad del sujeto -ultrafinalidades, conexiones ideológicas, etc.-, y/o elementos descriptivos concomitantes de la conducta prohibida -verbo típico-. De tal suerte, el Convenio no demanda una intención especial en el autor, ni especifica el tipo de sanción que deberá imponerse -multa, inhabilitación o prisión-. En razón de ello, da un margen de discreción -en el que ahondaremos-, respecto de elementos que hora pueden reducir y precisar, hora pueden amplificar el elenco de supuestos abarcados por la prohibición; dando lugar a técnicas legislativas que pueden gravitar en precisiones que permitan el deslinde entre conductas nocivas y las que no lo son, o que éstas se diluyan de forma tosca y menos racional, acudiendo a respuestas desproporcionadas en lo que a ejercicio de poder punitivo refiere, por las que se abre una peligrosa puerta a la arbitrariedad.

En nuestro país, como antecedentes legislativos de relevancia antes de la adhesión al mencionado convenio, aparecen el anteproyecto de la Secretaría de Comunicaciones de la Nación del año 2001[26], que establecía que el que accediere ilegítimamente a un sistema o dato informático privado o público de acceso restringido -iguales términos que la legislación penal actual-, sería reprimido con una pena monetaria y sólo hablaba de una pena privativa de la libertad cuando el autor hubiera decidido avanzar más allá del mero acceso, al revelar, divulgar o comercializar la información obtenida. En sus fundamentos, se remarca la intención de apegarse al principio de mínima intervención en materia penal. Así, se posicionaba al acceso ilegítimo como una figura preparatoria y residual sólo pasible de aplicación de pena de multa.

Posteriormente, en el Anteproyecto de Reforma y Actualización Integral del Código Penal de 2006 se habían analizado las opiniones de universidades y de reconocidos juristas, con la intención de recabar diversas posturas. Consecuentemente, en su art. 146 se mantuvo una tipificación análoga a la del antecedente reseñado referida al "acceso ilegítimo" a un

[25] https://www.oas.org/juridico/english/cyb_pry_convenio.pdf visita del 18/07/20.

[26] http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

banco de datos, cuya perspectiva punitivista y restrictiva de libertades en entornos digitales la tornó foco de las primeras críticas[27].

Ya a partir de la perspectiva de lo que representó para la regulación de nuestro país ser signatario del Convenio de Budapest se avizoran como antecedentes inmediatos el Programa Nacional contra la Criminalidad Informática creado en la Subsecretaría de Justicia y Política Criminal del Ministerio de Justicia y Derechos Humanos de la Nación[28], y a la Comisión Técnica Asesora en materia de Cibercrimen[29]. Fue gracias al impulso de los mencionados organismos que el Congreso sancionó la ley 27.411 de adhesión al Convenio de Budapest en el mes de noviembre de 2017[30]. Posteriormente, la sanción de la 26.388, que incluyó nuevos tipos penales y adaptaciones a supuestos informáticos dentro de títulos ya existentes en el Código Penal[31], con la que se ha establecido la prohibición del acceso informático no autorizado.

Respecto de la discusión parlamentaria previa, en punto a la necesidad de insertarla en la norma de fondo, no existió ninguna fundamentación particular, tratándose de una figura que carecía de antecedentes y que, como se vio, concretamente en sede parlamentaria registraba proyectos donde se la consideraba un acto preparatorio no punible (es decir que no correspondía que sea siquiera considerado delito) -proyecto 0117-S-2000 y anteproyecto de 2006-, así como otros donde se la penalizaba (se consideraba que la conducta sí era delito)-proyectos 0064-CD-2002; 3873-CD-2006; 5084-CD-2006 y 5864-CD-2006-.

Al debatirse la mencionada ley 26.388, las voces parlamentarias por unanimidad aludieron a que el delito de acceso ilegítimo se encuentra entre los reconocidos por las Naciones Unidas, por lo que se la considera como una figura clásica del catálogo de delitos informáticos a cuyo Convenio se ha adherido[32]. De tal suerte, y sin más análisis, se insertó el segundo tipo integrante del Capítulo III sobre la Violación de Secretos y de la Privacidad, conforme al artículo 5 de la Ley 26.388, y ubicado en el artículo 153 bis del Código Penal argentino:

[27] ROSENDE, E. E., "El intrusismo informático. Reflexiones sobre su inclusión al Código Penal", *Crisis y futuro de la legislación penal*, ed. AAPDP-Ediar, Bs. As., 2008, p. 13.

[28] GARAT, S.; REALE, J., "La reforma..., cit., p. 487/8.

[29] ABOSO, G. E., "Delitos contra la intimidad y la privacidad: acceso indebido a comunicaciones electrónicas, datos sensibles y sistemas informáticos", en Revista de Derecho Penal y Criminología, La Ley, ed. Thomson Reuters nro. 1775, Bs. As., del 11/08/17. p. 1.

[30] GARAT, S.; REALE, J., "La reform..., cit. p. 490.

[31] Ibídem, p. 506.

[32] RIQUERT, M. A.; GUTIERREZ, R.; RADESCA, L. C. "El delito de acceso ilegítimo a sistema o dato informático (intrusismo informático simple), en Revista de Derecho Penal y Criminología, La Ley, ed. Thomson Reuters nro. 109, Bs. As., del 02/12/13, p. 2.

ARTICULO 153 BIS. - Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financiero.

A partir de la descripción típica modelo del Convenio de Budapest, el legislador argentino puso en vigencia este nuevo delito de mera actividad y peligro abstracto; que no requiere resultado lesivo, y en caso de que este ocurra - si el dato o sistema informático accedido de manera no autorizada sufre alguna alteración o daño-, la prohibición cede, dando paso a figuras más graves como el daño informático -artículo 183 párr. 2º del Código Penal argentino-.

Regulaciones análogas tienen lugar en distintos países de la región[33], cuyas repercusiones casuísticas han tenido un tenor similar a las acaecidas en el foro local[34].

A continuación, se analizarán los elementos del tipo objetivo y subjetivo de la letra del Código Penal argentino, así como las agravantes, y otros supuestos especiales de aplicación.

ii. Verbo típico: acceder

Acceso

Según la Real Academia Española el término "acceder" en sus acepciones tercera y cuarta, indica la acción de entrar en un lugar o pasar a él; y tener acceso a algo, especialmente a una situación, condición o grado superiores, o llegar a alcanzarlos[35].

Al tratarse de sistemas informáticos caracterizados por la inmaterialidad de la información, las referencias espaciales quedarán a un lado, pero la definición nos servirá para indicar el franqueo de un cierto límite o portal.

[33] Ver apéndice nro. 1 sobre legislación regional compara.

[34] Ver apéndice nro. 2 sobre jurisprudencia local.

[35] https://dle.rae.es/acceder consulta del 28/07/20.

El verbo típico se verifica desde el instante mismo en que se alcanza la información, hace referencia al mero acceso, sin referencia a peligro concreto para ésta.

A diferencia de la conducta de daño informático regulada en el segundo párrafo del artículo 183 del Código Penal argentino, no se requiere resultado para la consumación -que el autor haya alterado, destruido o inutilizado los datos o programas informáticos-. Y es que, como se vio en anteriores acápites, en la mayoría de los casos el "hacker" accede de manera no autorizada a la base de tratamiento y almacenamiento de datos ajenos, públicos o privados, con el objeto de probar su habilidad de eludir protocolos que protegen al sistema de accesos no autorizados[36].

La figura adverbial "por cualquier medio", que acompaña al verbo núcleo, amplía las hipótesis fácticas penalmente reprochables a lo que se ha reconocido como la antesala para la comisión de otros delitos cuyos medios comisivos son variados -estafa, daño, sustracción de datos personales, secretos comerciales, etc.-. Por esa razón, la aparición de la tipicidad es residual, pues sólo será de aplicación "si no resultare un delito más severamente penado"[37].

En efecto, el acceso puede ser realizado mediante distintos métodos, ya sea remotamente; con una clave no permitida o sustraída; utilizando los datos concernientes al sujeto pasivo, como si fuera el legítimo usuario del sistema; mediante la instalación de un programa espía o *spyware*[38], de manera presencial, accediendo efectivamente al sistema mediante el mismo hardware utilizado por su titular, entre otros.

Así, existe una vertiente doctrinaria que opina incluso que puede darse el supuesto de que el autor del delito lo haga simplemente leyendo el contenido de la pantalla de una computadora -sin el permiso del titular de la misma[39]-; lo cual no sólo presentaría enormes dificultades probatorias en el caso concreto, sino que además puede presentar problemas de imputación objetiva y subjetiva, que tornan de dudosa aplicación la figura a tal extremo.

[36] ABOSO, G. E., "Delitos contra la intimidad y la privacidad: acceso indebido a comunicaciones electrónicas, datos sensibles y sistemas informáticos", en Revista de Derecho Penal y Criminología ed. Thomson Reuters nro. 1775, Bs. As., del 11/08/17, p. 1.

[37] PALAZZI, P. A., "El delito de acceso ilegítimo a un sistema informático", en *Cibercrimen II*, DUPUY, D. (Dir.) y KIEFER, M. (Coord.), ed. BdeF, Montevideo-Bs. As., 2019, p. 41.

[38] ROIBON, M. M, "Reflexiones sobre el acceso ilegítimo a un sistema o dato informático", *Cibercrimen y Delitos Informáticos*, Ed. Erreius, Bs. As., 2018, p. 13.

[39] Ibídem.

El tipo comprende además la conducta de quien, estando autorizado, excede sus funciones y accede a un sistema o dato informático. El agente puede ser, en este supuesto, un sujeto de confianza o la persona encargada del procesamiento de datos, pero el acceso particular excede la autorización otorgada en razón de su función o rol[40].

iii. Análisis de los elementos del tipo objetivo:

Sistemas y datos informático

Lo que debe entenderse universalmente como dato o sistema informático, está definido por los incisos a) y b) del artículo 1 del Convenio sobre Cibercriminalidad de Budapest, donde se sostiene que el sistema informático debe considerarse [*t]odo dispositivo aislado o conjunto de dispositivos interconectados o unidos, que aseguran, en ejecución de un programa, el tratamiento automatizado de datos*. De otra parte, el dato informático será *toda representación de hechos, informaciones o conceptos expresados bajo una forma que se preste a tratamiento informático, incluido un programa destinado a hacer que un sistema informático ejecute una función*[41].

De manera más llana, se ha sostenido que el sistema o dato informático es un conjunto de información que no se encuentran fácilmente accesible, sea porque pueden no estar conectados a la red, o porque se hallan resguardados bajo contraseña o clave de ingreso[42].

A su vez, en nuestro derecho interno, la Ley 25.326 de Protección de Datos Personales del año 2000, en su artículo 2, dispone que "datos informatizados" son [*l]os datos personales sometidos al tratamiento o procesamiento electrónico o automatizado* y, a su vez, que los "datos personales" son la *información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables*, mientras que "datos sensibles" serán aquellos [*p]ersonales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual*, debiéndose entender por "tratamiento de datos" las [*o]peraciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias*[43].

[40] ABOSO, G. E., "Delitos contra..., cit., p. 11.

[41] https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

[42] PALAZZI, P. A., "El delito..., cit., p. 102/3.

[43] RIQUERT, M. A.; GUTIERREZ, R.; RADESCA, L. C. "El delito..., cit., p. 3.

Nos explica la especialista en seguridad de datos personales Johanna Faliero que *[l]os datos son una entidad de carácter objetivo, que resultan de la representación de hechos en la forma de palabras, números o letras. La información por su parte, es el resultado del procesamiento organizado de datos del cual se obtiene un significado, el procesamiento convierte a los datos en información útil e involucra actividades, equipamiento y sujetos. Si bien en términos corrientes los vocablos "dato" e "información" se utilizan indistintamente, la diferencia entre uno y otro radica en su funcionalidad y alcance; toda información está compuesta por datos, y todo dato puede brindar alguna medida de información*[44] (...) *Un dato, en términos técnicos estrictos es un registro, una representación formal de algo (una idea, un hecho, un concepto, una cosa, etc.). Es decir, es un factor objetivo sobre algo determinado, tal como lo implica la etimología de su vocablo dato proviene del vocablo latino "datum", en simples términos, lo dado*. (...) *Los datos son un conjunto esencial de hechos referenciales que tienen poca o nula utilidad si no se encuentran en relación, es decir, cuando no son agregados con otros datos o sujetos a un procesamiento, lo cual les añade contenido. Los datos son la unidad atómica componente de la información, son hechos aislados. Mientras que la información es un conocimiento basado en datos procesados.(...) El procesamiento de datos es el acto de manipular datos de algún modo, independientemente de las actividades que se involucren en ello, que permitan asignarle significado y transformarlos así en información. El procesamiento de datos involucra una serie de acciones y operaciones diversas, que hacen uso de un sistema de procesamiento de datos, el que dispone de recursos, para convertirlos en información útil. La información son datos transformados en significativos y útiles. (...) El tratamiento informatizado de datos es, en pocas palabras, un sistema. Es decir, un grupo de componentes interrelacionados que buscan la consecución de un objetivo común mediante la aceptación de insumos ("input") -los datos-, y la implementación de un proceso organizado, para que por resultado ("output") se obtenga un producto -la información-. Este sistema que procesa datos, los captura y codifica en un formato reconocible para su procesamiento, y efectúa otra codificación en formato reconocible para que el usuario en su contacto directo con la interfaz, los encuentre inteligibles además de comprensibles*[45].

Por su parte, La ley de Protección de Datos Personales define en su artículo 2 el tratamiento de datos como las *[o]peraciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias*.

[44] BURGIN, M., "Data, information and Knowledge", *Information*, vol. 7, nro. 1, 2004, p. 47/57

[45] FALIERO, J. C., *La protección de datos personales*, ed. Ad Hoc, 2da edición, Bs. As., 2021, p. 45/8.

Acceso restringido

Al requisito de que se trate de un sistema o dato informático, se le adiciona el hecho de que deba ser de acceso restringido, esto es privado, no abierto al público en general. Siendo que ante permiso, consentimiento o aquiescencia del titular del dispositivo, lógicamente, la conducta se tornaría atípica[46].

Así, lo determinante es que el sistema no sea de acceso público, y que al mismo tiempo exista una medida de seguridad que impida el libre ingreso -contraseña, clave, autenticación por identificación dactilar o facial, etc.-. Por lo que el tipo exige que sea sorteada una protección específicamente dispuesta para impedir el acceso a terceros en general. Además, ello supone que si nos encontramos ante un dato o sistema de libre acceso, no habrá tipicidad[47].

La casuística demuestra que el acceso suele cometerse mediante el uso de algún programa que quiebre la restricción del sistema o del dato, y tal restricción ha sido interpretada como una medida de resguardo de la intimidad de estos.

El jurista Aboso, siguiendo criterio de la Sala II de la Cámara Federal Criminal y Correccional, incluye el acceso a datos restringidos dentro de un sistema informático de acceso público[48], como podrían ser datos sensibles de usuarios que se pudieran almacenar en redes públicas. Esto aparece como acertado, desde el prisma de la intimidad de los particulares afectados.

Por otra parte, la tipicidad queda excluida cuando el acceso se realiza de manera coetánea con la autorización, consentimiento o aquiescencia del sujeto pasivo. En la medida en que la falta de autorización debida es un elemento normativo del tipo, por lo que el acuerdo previo con terceros legitima el accionar y elimina el tipo objetivo. Tal autorización puede ser formulada de cualquier forma aunque, por lo general, cuando se trata de un permiso previo, se ve traducida en un contrato de prestación de servicios de seguridad informática[49].

Consecuentemente, si es un dato o sistema de libre acceso, no habrá tipicidad -no hay delito-. En otras palabras, se requiere la interposición

[46] BOUMPADRE, J. E., *Manual de Derecho Penal. Parte especial*, ed. Astrea, Bs. As., 2017, p. 371

[47] PALAZZI, P. A., "El delito..., cit. p. 42.

[48] ABOSO, G. E., *Código Penal de la República Argentina. Comentado, concordado con jurisprudencia*, Ed. B de F, Bs. As., 2012, p. 76.

[49] RIQUERT, M. A.; GUTIERREZ, R.; RADESCA, L. C. "El delito..., cit., p. 3.

de una medida asegurativa tendiente a verificar una identidad digital o credencial en particular. Se entiende que esa medida busca proteger la relación de disposición que -como bien jurídico intimidad o autodeterminación informativa- tiene una persona -física o jurídica- con los datos o la información que integra un sistema informático. Si aquel sistema no tiene dispuesta una medida asegurativa o defensiva idónea para prevenir la explotación de vulnerabilidades, sino que la propia estructura de sus datos se expone -desde el propio navegador de cualquier usuario o mediante un software de *scanneo* tradicional- y es así reconocido como vulnerable, sin necesidad de maniobras destinadas a neutralizar medidas asegurativas y acceder al sistema, entonces estimamos que de ningún modo puede haber tipicidad objetiva. En otras palabras, si los datos no están mínimamente asegurados mediante la interposición de una medida que los proteja, no hay delito.

Incluso, puede considerarse que, más allá de la atipicidad dada por la ausencia del mencionado elemento descriptivo, en casos en los que los códigos o bibliotecas sean versiones antiguas inseguras -códigos respecto de los cuales se ha divulgado vulnerabilidades en el ámbito de la programación-, tal circunstancia podría considerarse como una total ausencia de barreras de seguridad. Asimismo, tal desidia en la actualización de los sistemas informáticos en un contexto de permanente evolución y desarrollo como el informático, entendemos se traduciría en una auto-puesta en peligro del titular de los datos, que descartaría la posibilidad de imputación objetiva. De tal suerte que tampoco podría considerarse que hubiera delito en tal caso.

En nuestro país, los parámetros mínimos para considerar que la información se encuentra asegurada en los organismos del sector público nacional, han sido recientemente fijados por el Decreto 641/2021 del 25 de junio de 2021 mediante el que la Jefatura de Gabinete de Ministros instauró los Requisitos Mínimos de Seguridad de la Información para los Organismos del Sector Público Nacional, elaborado en base a estándares nacional e internacionalmente reconocidos, tales como las normas IRAM-ISO/IEC 27001, 27002 y 20000-1. Allí se especifican pautas mínimas de autenticación, autorización, control de accesos, uso de herramientas criptográficas, niveles y medidas de seguridad informática, mantenimiento, actualización y hasta gestión de incidentes de seguridad.

Entendemos que las pautas allí vertidas deben funcionar como parámetros básicos que deben existir objetivamente para considerar que el acceso a un sistema informático se encuentra restringido y no abierto al público. Así, en caso de que no se vean abastecidos tales requisitos mínimos, no puede considerarse que hubiera restricción alguna, por lo que tampoco podría ser típica la conducta, descartándose el delito.

iv. Análisis del tipo subjetivo:

El problema del dolo: supuestos en que la persona desconocía que el acceso no estaba autorizado.

La expresión "a sabiendas" nos posiciona frente a una figura dolosa, por lo que debe existir conocimiento de los elementos del tipo objetivo. Es decir que debe poder comprobarse que el agente al menos sabía que el acto en el que incurría era un acceso ilegítimo -que carecía de derecho, permiso, autorización o consentimiento para acceder-.

La redacción del primer párrafo referido a la figura básica consagra la punición de la conducta de quien con conocimiento y sin autorización o excediéndola, accede por cualquier medio a un sistema o dato informático de acceso restringido, dejando fuera accesos accidentales, causales o imprudentes.

Se trata de un tipo de dolo directo, en el que tampoco cabría imputación subjetiva a título de dolo eventual.

Así, deja fuera por medio de este requerimiento cognitivo -"a sabiendas"-, la punición de todo acceso fortuito, casual o imprudente. Este condicionamiento subjetivo es sólo compatible con el dolo directo, excluyendo al eventual[50]. Así, pues, se trata de un delito que se perfecciona con inequívoca dirección intencional y conocimiento que se está impedido de hacerlo[51].

El tipo no requiere elementos subjetivos distintos del dolo, esto es, de tendencia interna trascendente -ultrafinalidades usualmente destacadas con la preposición "para" o "con el fin de"- o peculiar o con cierto ánimo. Por ello, cualquier otra finalidad que la descripta sería propia de algún delito más grave, y de allí que se ha caracterizado al sujeto activo como el autor que procura eliminar los pasos de seguridad del sistema para ver el contenido de la información protegida.

Tampoco son requeridas ultrafinalidades o disposiciones de ánimo, que podrían ser propias de delitos más graves ante los que la figura cede -daño o estafa informática-. Esto último, a nuestro entender, resultaría deseable en miras a ganar mayor razonabilidad, y sobre todo para descartar casos de investigadores informáticos con efectos inocuos, como supuestos penalmente irrelevantes.

[50] RIQUERT, M. A., "Una mirada actualizada sobre el hacking o intrusismo informático en el Código Penal argentino", *Revista de Derecho Penal y Criminología*, nro. 5, ed. Thomson Reuters La Ley, del 04/11/2021.

[51] PARMA, C.; ALVAREZ DOYLE, D.; MANGIAFICO, D., *Derecho Penal. Parte especial*, ed. Hammurabi, Bs. As., 2019, p. 360.

De lo dicho, resulta lógico indicar que el error -déficit en el conocimiento o falta en la representación- sobre un elemento del delito excluiría el dolo y la responsabilidad penal en general, dado que no se encuentra previsto el tipo culposo. La posibilidad de incurrir en error está admitida, en especial cuando el autor accede a un sistema informático desconociendo su carácter restringido. También puede suceder que el que accede al sistema informático lo haga por indicación de un tercero, a quien tiene erróneamente por titular de ese sistema[52]. En ambos ejemplos la tipicidad subjetiva es descartada, pues no se admite imprudencia, no pudiéndose considerar que se cometió delito.

v. Agravantes

En el segundo párrafo del artículo 153 bis del Código Penal, observamos la agravante relativa a la ejecución en perjuicio de bienes o servicios públicos, toda vez que estos son considerados merecedores de una especial protección. Observándose que la solución es análoga a la adoptada en el caso del agravante del daño informático del artículo 184 incs. 5 y 6 del Código Penal.

En cuanto al concepto de "servicio público", Sáez Capel y Velciov lo definen como *[t]odo aquel que se encuentre destinado a servir a la población en forma más o menos generalizada, a un número de personas indeterminado, más allá de que su prestación corra por cuenta del Estado o de particulares*[53].

Desde el Derecho administrativo, se ha entendido que se trata de las prestaciones indispensables para saciar las necesidades humanas -vida digna-, que ineludiblemente el Estado ha de asegurar, en miras a garantizar el bienestar general; no tratándose sólo de los Derechos Civiles y Políticos, sino también los Económicos, Sociales y Culturales[54].

El fundamento de la mayor penalidad reside en la naturaleza de los organismos protegidos, públicos o de servicio público. Se reconoce en esos casos el peligro de que a través del acceso no autorizado se obtengan grandes cantidades de información que resulte altamente sensible para los ciudadanos[55], y pueda afectar el goce de derechos fundamentales que

[52] ABOSO, G. E., "Delitos contra..., cit., p. 11/2.

[53] SÁEZ CAPEL, J. - VELCIOV, C. E., "Comentario al art. 153 bis", *Código Penal y normas complementarias. Análisis doctrinal y jurisprudencial*, Tomo 5, Baigún y Zaffaroni (dirs.), ed. Hammurabi, Bs. As., 2008, p. 747.

[54] BALBÍN, C. F., *Curso de Derecho Administrativo. Tomo I*. Ed. La Ley, Bs. As., 2008; y FERNÁNDEZ, B., "Breve reflexión sobre el Servicio público", en SAIJ, Bs. As., 25/02/14.

[55] BOUMPADRE, J. E., *Manual de Derecho Penal. Parte especial*, ed. Astrea, Bs. As., 2017, p. 372.

el Estado debe garantizar -alimentación, educación, salud, empleo, transporte público, etc.-.

Asimismo, la pena se agrava para los casos en que tenga lugar el acceso a un proveedor de servicios públicos o financieros. En este punto, Palazzi señala que el término "proveedor de servicios financieros" es más amplio que el de entidad financiera -art. 2, ley 21.526-, pudiendo incluirse un agente de bolsa, una casa de cambios o un medio de pago online o de recaudación. Ponderándose la trascendencia que tal proceder tendría para las finanzas y transacciones económicas. Interpreta el mencionado autor que se da una tutela especial a las finanzas y el dinero[56], como principales objetos de vulneración.

Se observa que esta agravación será aplicada sólo en casos en los que la intrusión sea "en perjuicio" del organismo público, habiéndose dejado a un lado organismos públicos no estatales, como colegios profesionales.

2.3. Análisis del delito de acceso no autorizado a bancos de datos personales

ARTICULO 157 BIS. -Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que: 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales; 2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley. 3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años.

A los fines del presente reporte, nos limitaremos a analizar el inciso primero dado que las conductas reprimidas en los restantes incisos exceden el mero acceso.

i. Análisis del verbo típico "acceder":

Vale el análisis realizado en el apartado anterior ya que la acción típica es también "acceder", es decir, penetrar, ingresar o introducirse, a un banco de datos personales.

[56] PALAZZI, P. A., "El delito..., cit., p. 56.

Puede concretarse por cualquier medio ya que no se especifica modalidad de ingreso alguna, aunque el contexto de la reforma es claro en cuanto a que el legislador quiso referirse a los medios informáticos.

Pero el mero ingreso no constituiría delito, se requiere que el autor tome conocimiento de los datos, del contenido de la información, ya que sólo mediante esto último podría afectarse la intimidad personal del titular del dato. Sin embargo, parte de la doctrina sostiene que el afectado por la conducta es el titular del banco de datos que, con el mero acceso, ve violentado el secreto que debe presidir la recolección, preservación y procesamiento de datos.

ii. Análisis de los elementos del tipo objetivo:

El inciso refiere "a sabiendas o ilegítimamente" y, agrega "o violando sistemas de confidencialidad y seguridad de datos". La redacción ha sido criticada por redundante ya que si se violan sistemas de confidencialidad, resulta obvio que se lo hace a sabiendas y careciendo de derecho. No se requiere el apoderamiento de los datos personales, basta con el acceso a ellos. En este sentido, la esfera de reserva se vulnera atacando al banco mismo, quebrantado las seguridades con que se lo ha dotado para impedir el conocimiento de terceros.

Banco de datos

De conformidad con lo previsto por el art. 2 de la Ley N° 25.326 se encuentran abarcados al banco, un archivo, registro o base de datos personales.

La citada ley estipula que por "archivo, registro, base o banco de datos" -en forma indistinta- se entiende al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera fuera la modalidad de su formación, almacenamiento, organización o acceso.

La misma ley define los términos empleados; así, por "datos personales" ha de entenderse la información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables; por "datos sensibles", aquellos datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual; y por "datos informatizados", aquellos datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.

iii. Sujeto pasivo

Resulta ser el titular del banco de datos (persona física o jurídica) mientras que, sin perjuicio de ellos, puede entenderse que en todas lo es el titular de los datos reservados que son ilegítimamente accedidos, revelados o modificados por inserciones.

El art. 2 de la Ley 25326 indica que "responsable de archivo, registro, base o banco de datos" es la persona física o de existencia ideal pública o privada que es titular de un archivo, registro, base o banco de datos; por "titular de los datos" ha de entenderse toda persona física o de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la propia ley; mientras que "usuario de datos" es toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.

iv. Análisis del tipo subjetivo:

La frase "a sabiendas" resulta indicativa de que se trata de un supuesto que demanda dolo directo. El sujeto activo debe conocer el alcance y la ilegitimidad de su accionar, ejecutando la acción sin ningún permiso y obteniendo información personal indebida sin el consentimiento del titular.

2.4. El ejercicio de la acción penal en relación a los delitos previstos en los arts. 153 bis y 157 bis del Código Penal

Ambos delitos son de acción privada, conforme lo normado por el inc. 2° del art. 73 del Código Penal argentino. Esto quiere decir que sólo podrá darse impulso al proceso penal cuando el titular del sistema, dato informático o banco de datos que demostrara ser afectado o damnificado por el presunto acceso ilegítimo, decida instar la acción e iniciar así el proceso. Lo que popularmente conocemos como "presentar cargos".

Este régimen de acción privada parecería tener su sentido en la interpretación personalísima del bien jurídico -intimidad, privacidad o autodeterminación informativa-, brindándole al sujeto titular del derecho afectado la posibilidad de decidir que se inicie o no un proceso penal contra el agresor.

Tal disposición parece coherente para la figura simple y la interpretación jurídica del bien que se pretende tutelar. Sin embargo, se observa una cla-

ra incongruencia del legislador con relación al agravante del segundo párrafo del art. 153 bis, referido a bienes y servicios públicos. Probablemente, resultado no querido de la criticable técnica de sucesivos "parches" modificatorios al Código Penal que, en el caso de la Ley 26.388 omitió considerar repercusiones en cuanto a la acción penal[57].

Más allá de la tesis del olvido legislativo y la opinión de algún sector de la doctrina que sostiene que la acción es pública y que puede promoverse de oficio cuando lo perjudicado es un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros (art. 143 bis *in fine* del Código Penal) o los datos son almacenados en bancos de datos públicos (art. 157 bis del Código Penal); estimamos que una interpretación contraria a lo normado en el art. 73 citado vulneraría el principio de legalidad en perjuicio del eventual inculpado. Ello en cuanto impondría un régimen diverso a la acción, distinto al normativamente dispuesto por el legislador, que perjudicaría al imputado permitiendo que sea el Estado quien dé impulso al proceso en su contra a través del órgano de acusación pública, prescindiendo de la voluntad particular del sujeto pasivo afectado por el presunto delito.

2.5. Un proyecto de reforma del art. 153 bis

En el marco de la conferencia internacional de seguridad Ekoparty, realizada en el 2020, surgió un proyecto de reforma que busca incorporar al tipo del art. 153 bis el siguiente párrafo: *Estará exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público. También quedará exento quien obrando de buena fe y en el marco de una investigación de seguridad de la información, comunicare la vulnerabilidad encontrada al propietario del sistema informático.*

Más allá del empleo de ciertos términos ambiguos - *"propósito inequívoco de proteger un interés público"-*, la propuesta busca otorgar un marco de protección para el investigador en seguridad informática, que descubre y reporta una vulnerabilidad -aunque no se especifica la modalidad del reporte-; regulando una exención de responsabilidad penal.

Este tipo de iniciativas son las que consideramos sana, de cara a la conformación de una ciudadanía digital responsable y a tono con las modificaciones permanentes que se dan en el ámbito de los sistemas de información a nivel global.

[57] RIQUERT, M. A.; GUTIERREZ, R.; RADESCA, L. C. "El delito..., cit., p. 6.

2.6. Conclusiones acerca de los delitos analizados y el proyecto de ley

El problema del bien jurídico tutelado por los tipos penales

Lo que estaba protegido en el capítulo del Código Penal analizado era la incolumidad de: a) la intimidad de la correspondencia y de los papeles privados y, b) los secretos y la libre comunicación entre las personas; y con la incorporación de los "delitos informáticos", la información personal que se hallare registrada en un sistema o banco de datos personales (privacidad).

Pero no está protegida la "seguridad de los sistemas", razón por la cual el mero acceso al sistema, sin afectación al bien jurídico protegido no justificaría la persecución penal.

Los tipos penales y la conducta del investigador en seguridad digital

Los delitos analizados son de peligro abstracto (ese peligro no integra el tipo objetivo), cuya constitucionalidad es cuestionada. Los delitos de peligro abstracto no pueden equipararse a los delitos de mera actividad, pues ello implicaría consagrar una presunción *iure et iure* respecto de la peligrosidad de la conducta.

Por ello se sostiene que existe una presunción *iuris tantum* que admite prueba en contrario, es decir, puede demostrarse que la acción en concreto carece de la peligrosidad presumida por el legislador de manera general. Esto obligaría al juez a analizar la idoneidad de la acción para afectar el bien jurídico mediante la comprobación en el caso de esa peligrosidad general.

El accionar del investigador en seguridad digital consiste en testear sistemas informáticos para descubrir sus vulnerabilidades —sin conocer el contenido— e informarlas al titular para solucionarlas. A pesar de superar las medidas de seguridad existentes y carecer de autorización del administrador del sistema, lo cierto es que no posee una peligrosidad que habilite su sanción. Así se advierte una conducta que carece de lesividad (art. 19 CN), dado que contribuye a la evolución de los niveles de seguridad informática en beneficio de toda la comunidad y así resguarda la privacidad de los datos contenidos en esos sistemas. De tal manera, al demostrarse que la acción presenta esas características debe entenderse que resulta atípica, por lo que no habrá delito.

Sumado a ello, es evidente que si el agente tiene autorización para el acceso y respeta sus límites la conducta deviene irrelevante. Esto ocurre, por ejemplo, cuando el titular brinda el consentimiento para el acceso de un experto, a fin de verificar la seguridad del sistema. Aquí, la formulación normativa "sin la debida autorización" constituye, por tanto, un elemento normativo de recorte expreso que permite diferenciar las conductas típicas de las que no lo son. Algunas figuras penales sólo pueden ser perpetradas contra la voluntad del titular del bien jurídico. Por este motivo, aquellos delitos prevén de manera explícita la falta de acuerdo del damnificado como requisito de tipicidad.

Los delitos analizados no realizan una distinción respecto de las distintas formas de acceso a un sistema o banco informático y mucho menos respecto de la motivación o finalidad del testeo de vulnerabilidades. De este modo, el acceso puede realizarse mediante la utilización de cualquier medio -ingeniería social para obtener las claves de un usuario del sistema, o aprovechando deficiencias de seguridad del sistema verificadas tras un *scanneo* de sus códigos, utilizando sistemas de fuerza bruta, etc.- y con finalidad delictiva o altruista, pues la ley no distingue entre unos y otros, y castiga cualquier acceso por igual.

Es por ello que Riquert -jurista especializado en temas de ciberdelincuencia- concluye que deberían excluirse del tipo penal los casos de investigadores en seguridad informática que acceden mediante claves poco seguras o puertos abiertos en un servidor o red informática, con herramientas de software dedicadas a tal fin para el testeo y con el objetivo de resguardar, reestablecer o mejorar el sistema[58].

En igual sentido opina el especialista Palazzi, quien destaca que deben quedar fuera de la prohibición las conductas de testeo de seguridad de falencias de redes informáticas en el marco de investigación académica, casera o empresaria, muchas veces realizado además con consentimiento de la "víctima", que tiene como objetivo la detección de errores en el aseguramiento de los datos y en miras a su subsanación. Opina además que debería quedar fuera de la prohibición también la denominada ingeniería inversa o reversa, que es la destinada a obtener información técnica a partir de un producto accesible al público, con el fin de determinar de qué está hecho, qué lo hace funcionar y cómo fue fabricado, actividad que evidentemente no se relaciona con la "privacidad", sino con la protección de la propiedad intelectual[59].

[58] RIQUERT, M. A., "Una mirada actualizada sobre el hacking o intrusismo informático en el Código Penal argentino", *Revista de Derecho Penal y Criminología*, nro. 5, ed. Thomson Reuters La Ley, del 04/11/2021.

[59] PALAZZI, P. A., "Análisis de la ley 26.388 de reforma al Código Penal en materia de delitos informáticos", *Revista de Derecho Penal y Procesal Penal*, ed. Lexis Nexis, nro. 7/08, p. 1217.

Lamentablemente, estas opiniones calificadas no pasan de ser más que modos de interpretar la aplicación de la ley, que no la modifican ni obligan a los operadores del sistema judicial a cambiar sus prácticas al respecto.

Debemos destacar, junto a la opinión de los mencionados especialistas, que no cabe duda de que el descubrimiento de una vulnerabilidad podría conllevar a un potencial daño, sabotaje o pérdida de información. Además, en los casos en los que no resulta clara la existencia de autorización previa para el testeo, podría el operador quedar amparado por una situación de necesidad, sacrificándose la confidencialidad hacia él en pos de evitar directamente la pérdida de la información confidencial, es decir, con el bien u objetivo mayor de resguardar el sistema que tiene por fin, precisamente, preservar la información de carácter reservado[60].

Consecuentemente, se presenta esta compleja problemática de separar por vía de la interpretación algo que la letra de la ley no distingue, en miras a deslindar entre una actividad nociva y otra positiva; para establecer el límite de lo que debe considerarse prohibido y delictivo, de lo que es ejercicio propio de una actividad de desarrollo y experimentación informática, e incluso de una buena ciudadanía digital.

Este problema fue pasado por alto por la ley argentina. Como vimos, l,a persecución penal de todo acceso autónomo no autorizado fue regulada aplicando un lenguaje poco específico e insertando una figura normativa general que en lugar de abordar el problema de manera concienzuda y específica, atendiendo a todas sus aristas y distinciones, recurrió a la potestad última con la que cuenta el Estado, como es el ejercicio de la coacción física mediante la criminalización generalizada de cualquier tipo de acceso a un sistema o dato informático.

Entendemos que del mismo modo que no todos los tipos de testeo de vulnerabilidad o accesos son idénticos, y tampoco tienen la misma finalidad, no puede el Estado brindar un único tipo de respuesta. Menos aún si esa única reacción es la más severa y perjudicial para los derechos de los ciudadanos que detectan vulnerabilidades en particular, y para el sano desarrollo del área de ciberseguridad en general.

[60] RIQUERT, M. A., "Una mirada actualizada sobre el hacking o intrusismo informático en el Código Penal argentino", *Revista de Derecho Penal y Criminología*, nro. 5, ed. Thomson Reuters La Ley, del 04/11/2021.

El ejercicio de la acción penal

Si bien ambos delitos son de instancia privada, lo que obliga a la víctima a investigar por su cuenta la conducta imputada e impulsar el proceso; no desconocemos que para sortear tal circunstancia, o la víctima denuncia otros delitos que sí son de acción pública (ej, daño informático) o es la propia agencia judicial (Ministerio Público Fiscal/ juzgado de instrucción) quien justifica una intervención por fuera de las prescripciones del art. 73 del CP, alegando un bien jurídico inexistente, y así desplegar el poder de las agencias encargadas de la criminalización secundaria.

El proyecto de reforma del art. 153 bis

Sucintamente, corresponde señalar que la propuesta es compatible con los argumentos tratados en este apartado. De tener éxito, implicaría consolidar en forma expresa al elemento de recorte implícito existente en la formulación normativa actual del art. 153 bis del Código Penal. Sin duda, ello permitiría sintetizar la interpretación aquí desarrollada en la letra de la ley y así disminuir la discusión sobre la atipicidad del proceder del investigador en seguridad informática.

3. Políticas públicas a diseñar para desincriminar las acciones del investigador en seguridad

3.1. En materia penal

a. Modificar los arts. 153 bis y 157 bis del CP.

i. Objetivo de máxima: buscar que las conductas desplegadas por los investigadores en seguridad informática resulten atípicas o queden eximidas de responsabilidad penal. Para ello se podría crear un supuesto, como el estudiado en el proyecto de ley analizado; o incluir un "ultraintencionalidad" (elemento subjetivo), que exija "algo más" que el mero acceso.

ii. Objetivo de mínima: cambiar la pena de prisión por pena de multa, circunstancia que habilitaría la aplicación del art. 64 del Código Penal.

b. Modificar la interpretación de los arts. 153 bis y 157 bis del CP vigentes.

i. Objetivo de máxima: lograr que los órganos de investigación (Ministerio Público Fiscal) a través de las Instrucciones Generales que diseñan y fijan los alcances de la política criminal, tengan en consideración las distinciones señaladas y analizadas en relación a la investigación de casos relativos a reportes de vulnerabilidades y seguridad informática. Ello, a fin de sentar criterios e instruir a los fiscales de investigación a discriminar los casos en los que no resulta procedente el ejercicio de la acción por tratarse de un reporte de vulnerabilidad.

3.2. En materia regulatoria: incorporar disposiciones -tanto para el sector público como para el privado- acerca de la gestión, tratamiento y divulgación coordinada de vulnerabilidades en materia de seguridad informática

La gestión de las vulnerabilidades es un proceso necesario dentro de las prácticas de seguridad de la información. En los sistemas provistos por terceros, instalar las actualizaciones de seguridad de manera sistemática es una actividad común para las organizaciones, y en general esto se conoce como gestión de parches o actualizaciones. Sin embargo, buscarlas, identificarlas, y mitigarlas de manera continua no siempre suele ser un proceso estándar, en algunos casos las empresas reguladas deben hacerlo por cumplimiento de un sector regulado o alguna norma de orden administrativo o legal.

Las organizaciones -estatales y privadas- deben tener su proceso de gestión de vulnerabilidades, y en la actualidad existen estándares que incentivan la búsqueda de vulnerabilidades por parte de investigadores independientes, estableciendo programas de Divulgación Coordinada de Vulnerabilidades (CVD en inglés). Estos programas tienen la finalidad de que los organismos del Estado atiendan los reportes de investigadores para su análisis y mitigación.

i. Tratamiento de vulnerabilidad en el orden internacional.

En la Unión Europea, la Directiva comunitaria denominada "Seguridad de la Información y de las redes 2"[61] (*Network and Information Security* versión 2, NIS2), con el objetivo de elevar los niveles de seguridad establecidos por la primera edición de la Directiva NIS[62], contempla la obligatoriedad de

[61] Proyecto de Directiva NIS2, Network Information Security https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

[62] Directiva europea NIS, 2016. Un Marco para la ciberseguridad https://www.enisa.europa.eu/topics/nis-directive

coordinar la divulgación de las vulnerabilidades como una práctica para fortalecer la seguridad de la Unión. Fue la Agencia europea para la Seguridad de la Información y las Redes (*European Network and Information Security Agency, ENISA,* creada en 2004), quien se encargó de los estándares sobre Divulgación Coordinada de Vulnerabilidades[63], publicada ya desde 2018.

En Estados Unidos, la Orden Ejecutiva de mayo de 2021[64] que trata sobre "La mejora de la Ciberseguridad de la Nación" estableció directivas para el tratamiento de las vulnerabilidades en varios aspectos, instaurándose luego por la Agencia de Ciberseguridad y Seguridad de la Infraestructura (*Cybersecurity & Infrastructure Security, CISA*) un programa para que las agencias del gobierno federal atiendan los reportes de vulnerabilidades como una forma de mejorar la seguridad de la información para el gobierno. El programa[65] de la Agencia de Ciberseguridad para las Infraestructuras CISA coordina la atención y la divulgación pública de vulnerabilidades (*Coordinated Vulnerability Disclosure, CVD*) en productos y servicios con los proveedores afectados.

Estos ejemplos de regulaciones surgen después de muchos años de falta de atención del problema de las vulnerabilidades como parte de la seguridad hacia el público general.

Desde la Organización Internacional de Estándares (ISO) en conjunto con la Comisión Electrotécnica Internacional (IEC), se elaboró el estándar ISO/IEC 29147[66] "Divulgación de Vulnerabilidades", un documento que proporciona requisitos y recomendaciones a los proveedores y destaca que: "la divulgación de vulnerabilidades permite a los usuarios realizar una gestión de vulnerabilidades como se especifica en ISO/IEC 27002:2013[67], 12.6.1[1]. La divulgación de vulnerabilidades ayuda a que los usuarios a proteger

[63] ENISA. Guía de Divulgación Coordinada de Vulnerabilidades (CVD) https://www.enisa.europa.eu/news/member-states/WEB_115207_BrochureNCSC_EN_A4.pdf

[64] Executive Order on Improving the Nation's Cybersecurity, may 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[65] Programa de divulgación coordinada de CISA Cybersecurity & Infraestructure Security Agency, Estados Unidos, https://www.cisa.gov/coordinated-vulnerability-disclosure-process

[66] Visualización introductoria de la norma ISO/IEC 29147 Divulgación de Vulnerabilidades, desde el repositorio de Comisión Electrotécnica Internacional, organismo que emite la publicación en conjunto con la Organización Internacional de Estándares. https://webstore.iec.ch/preview/info_isoiec29147%7Bed2.0%7Den.pdf

[67] ISO/IEC 27002 es un conjunto de buenas prácticas en materia de controles para la gestión de seguridad de la información en una organización que ISO y IEC han definido como buenas prácticas y lograr un mínimo de prácticas que hacen a la seguridad de un Sistema de información. Esta norma es una más de la serie de normas ISO/IEC 27000. https://www.iso.org/standard/54533.html

sus sistemas y datos, priorizar sus inversiones en prácticas defensivas y evaluar mejor el riesgo. El objetivo de la divulgación de vulnerabilidades es reducir el riesgo asociado con la explotación de vulnerabilidades. La coordinación de divulgación de vulnerabilidades es especialmente importante cuando se ven afectados varios proveedores."

ii. Tratamiento de vulnerabilidad en el orden nacional.

En la Administración Pública Nacional de la Argentina, las primeras normas administrativa que menciona la necesidad de dar tratamiento a las vulnerabilidades es la Política Modelo de Seguridad de la información que se introdujo primero la Decisión Administrativa 669/2004[68], en la que se establecía que los organismos del Sector Público Nacional debían dictar o adecuar sus políticas de seguridad, conformar Comités de Seguridad en la Información y asignar funciones responsabilidades en relación con la seguridad, la Política modelo de ese momento, y la Disposición 6/2005[69] en la que se publicó la política Modelo y por la cual ya se recomendaba dar seguimiento y tratamiento por los riesgos que podrían causar.

Mediante el Decreto 641/2021 se estipularon los requisitos mínimos de seguridad de la información para los organismos del sector público nacional se refiere. Si bien dicha normativa constituye un piso para los organismos enumerados e impone como deberes: *"identificar y gestionar adecuadamente las vulnerabilidades, así como el proceso de gestión de actualizaciones de todo el software utilizado. En los casos que el mismo sea provisto por terceros, contar con una política de actualización para evitar que se afecte la operación"* y *"gestionar de manera apropiada los reportes de vulnerabilidades y recomendaciones de actualización"* (punto nro. 8 referido a "Seguridad operativa"); nada dice acerca de cómo un investigador independiente debe reportar una vulnerabilidad advertida.

iii. Necesidad de trabajar en un protocolo de Divulgación Coordinada de Vulnerabilidades.

[68] DA 669/2004. Solicita que los organismos del sector público nacional Aprueben su política de Seguridad de la Información en base a la Política de Seguridad Modelo, http://servicios.infoleg.gob.ar/infolegInternet/anexos/100000-104999/102188/texact.htm

[69] Disposición 6/2005 de la ex Oficina Nacional de las Tecnologías de la Información que aprueba la Política Modelo de Seguridad de la Información para organismos de la APN. http://servicios.infoleg.gob.ar/infolegInternet/anexos/105000-109999/108672/norma.htm y https://www.unpa.edu.ar/sites/default/files/descargas/Administracion_y_Apoyo/4.%20Materiales/2018/RECT/Vigentes/124-T053-P/PSI_Modelo%20de%20Pol%C3%ADtica%20de%20Seguridad%20de%20la%20Inf_Jul-15.pdf texto de la política Modelo.

La instauración de un protocolo o programa -tanto a nivel nacional como provincial- para promover el desarrollo de políticas coordinadas en materia de vulnerabilidades se torna imperiosa para brindar una mayor protección y así legitimar las acciones de los investigadores en seguridad digital.

4. Propuesta FVL para divulgar reportes de vulnerabilidades

La fundación promueve el desarrollo de la seguridad informática mediante la creación de una plataforma que habilita el reporte anónimo de vulnerabilidades. Una vez recibido el aviso, a fin de evitar una comunicación errada o innecesaria, verifica que la vulnerabilidad exista. En caso afirmativo lo comunica al titular del sistema.

El proceso de divulgación podría resumirse de la siguiente manera:

1) Un investigador en seguridad digital advierte/descubre una vulnerabilidad en un programa, sistema o registro informático perteneciente al Gobierno de la Ciudad Autónoma de Buenos Aires o al Gobierno Nacional.

2) Reporta dicha vulnerabilidad a la plataforma de la Fundación Vía Libre.

3) Las condiciones de vulnerabilidad son verificadas por personal de la Fundación.

4) Se presenta un pedido de acceso a la información ante el organismo / ente estatal para que informe si:

    a. se conocía la vulnerabilidad;

    b. si fue reparada, de ser así Vía Libre lo verifica;

    c. las medidas de seguridad implementadas (Las medidas que se tomen deberán, brindar a corto plazo la implementación o una mejora tangible a sus herramientas o mecanismos);

    d. los procesos para la gestión de vulnerabilidades que consideren la identificación, evaluación, tratamiento y comunicación de las medidas de seguridad en la infraestructura tecnológica, mediante la ejecución de pruebas de penetración o intrusión y de escaneos de vulnerabilidades. Se deberán remediar todas las brechas de seguridad no solo las clasificadas como críticas y de alto riesgo.

Sobre la posible responsabilidad de la Fundación, cabe señalar que la ley nro. 27.401 limita la responsabilidad penal de las personas jurídicas exclusivamente a los delitos previstos en los arts. 258, 258 bis, 265, 268 y 300 bis del Código Penal, por lo que una eventual investigación penal sólo podría recaer sobre los responsables de la fundación y/o aquellas personas involucradas en el área/proyecto vinculado al reporte de vulnerabilidades.

Ahora bien, el accionar puede circunscribirse a repetir los pasos del investigador en seguridad digital, anonimizar al agente y comunicar la vulnerabilidad.

Por los mismos argumentos brindados en el apartado anterior, la repetición de la maniobra del investigador por parte de la fundación, a fin de verificar la entidad del problema de seguridad, resultaría atípica.

Asimismo, al ser atípico el proceder del investigador corresponde descartar la participación de los responsables de FVL en la maniobra por anonimizar al agente, toda vez que, indistintamente se estudie conforme el estándar de la teoría de la accesoriedad limitada (acción típica y antijurídica) o mínima (acción típica), lo cierto es que no hay injusto.

Esta respuesta permanece inalterable al tratar su responsabilidad por encubrimiento. La inexistencia de un delito precedente (acción típica, antijurídica y culpable) constituye la ausencia de un requisito típico de la figura e implica que la puesta a disposición de una plataforma digital anónima para el ingreso de reportes sea penalmente irrelevante.

Finalmente, en cuanto a la comunicación de la vulnerabilidad, autores como Palazzi entienden que el mero hecho de dar a conocer a terceros la existencia de fallas de seguridad informática en cualquier sistema -aun en el supuesto de que ayudara a cometer accesos ilegítimos- no configura una apología del delito previsto en el art. 153 bis del Código Penal, ya que este proceder constituye un ejercicio de la libertad de expresión.

En consecuencia, resulta evidente que la simple puesta en conocimiento del inconveniente de seguridad al titular del sistema por parte de la Fundación Vía Libre —sin difusión a terceros— está exenta de intervención alguna del Derecho penal.

Cabe advertir que las conclusiones doctrinarias y dogmáticas hasta aquí esbozadas, no deben entenderse más que como las interpretaciones de la ley que sus autores estiman -por los argumentos expuestos- más adecuadas al marco del Estado constitucional de derecho. Sin embargo, no pueden considerarse *per se* como mayoritarias ni universalmente aceptadas, así como tampoco capaces de obturar una posible intervención de las agencias estatales para iniciar una investigación penal y ser objeto de medidas cautelares.

En todo caso, el trabajo aquí realizado guarda la pretensión de acercar argumentos para un ejercicio racional del Derecho penal, en miras a proteger una actividad que aparece como vital para el desarrollo de entornos informáticos más seguros de cara a una mejora de nuestra ciudadanía digital.

APÉNDICE I - Legislación Comparada en la Región

PAÍS	NORMATIVA	CONTENIDO
PARAGUAY	Art. 174 CP – Reforma CP año 2011	El que lesionando el derecho de disposición de otro sobre datos los borrara, suprimiera, inutilizara o cambiara, será castigado con pena privativa de libertad de hasta dos años o con multa. En estos casos, será castigada también la tentativa. Como datos, en el sentido del inciso 1º, se entenderán solo aquellos que sean almacenados o se transmitan electrónica o magnéticamente, o en otra forma no inmediatamente visible.
CHILE	Art. 2 – ley 19 223	El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.
COLOMBIA	Art. 269A - Ley 1273	El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

PAÍS	NORMATIVA	CONTENIDO
URUGUAY	Art. 2 – Ley N 19223	El que con ánimo de apoderarse, usar, o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.
VENEZUELA	art. 6 - LECDI - 2001	Toda persona que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.
BRASIL	Art. 154-A CP (Redacción incorporada por Ley 14.155/2021)	Invadir un dispositivo informático para uso de terceros, esté conectado o no a la red informática, con el fin de obtener, manipular o destruir datos o información sin la autorización expresa o tácita del usuario del dispositivo o instalar vulnerabilidades para obtener ventaja.
BOLIVIA	Art. 363 ter - CP	El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días.

PAÍS	NORMATIVA	CONTENIDO
ECUADOR	Art. 234 – CP	La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.
PERÚ	Art. 207 CP – Reforma 2000	El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa.

APÉNDICE II - Jurisprudencia

1. **Joaquín Sorianello, Fiscalía Penal, Contravencional y de Faltas n° 7, Ciudad de Buenos Aires, 28 de julio de 2016**
2. **Gaspar Ariel Ortmann, Juzgado Criminal y Correccional Federal n° 11, sentencia del 30 de noviembre de 2020**
3. **Javier Smaldone, Juzgado Criminal y Correccional Federal n° 9, sentencia del 24 de noviembre de 2021**

1. Joaquín Sorianello

Exp. JUSCABA PCyF 0312757-00-00/15. Legajo "MPF 00083322 s/ nombre s/ infr. art(s) 183, 2° párr-daños informáticos-Código Penal"

Fiscalía Penal, Contravencional y de Faltas n° 7, Ciudad de Buenos Aires, 28 de julio de 2016

Joaquín Sorianello, programador, diez días antes de las elecciones generales para Jefe de Gobierno de la Ciudad de Buenos Aires del año 2015, denunció que había detectado fallas en el sistema de seguridad de la empresa Magic Software Argentina SA (MSA), empresa elegida para implementar la boleta electrónica en las elecciones locales.

A pesar de dar el aviso de las vulnerabilidades encontradas a la propia empresa, recibió una denuncia en su contra. La noche del viernes anterior a los comicios, la Policía Metropolitana allanó su casa. En el allanamiento se incautaron, entre otros elementos, una Macbook Pro, cuatro discos rígidos, pendrives y memorias.

Luego de un largo proceso, el 26 de julio del año siguiente, la Fiscalía en lo Penal, Contravencional y de Faltas 7, decidió archivar el caso porque, a su criterio, el hecho resultaba atípico (art. 199, inc. a, Código Procesal Penal de la Ciudad de Buenos Aires, actual 211, inc. a).

Dictamen de la Fiscalía que resuelve archivar el caso

La fiscalía determinó que el hecho a investigar era el ocurrido el 25 de junio de 2015, cuando autores ignorados accedieron remotamente al sistema informático de la empresa Grupo MSA SA, alteraron su normal funcionamiento y obtuvieron información interna, que luego fue publicada en una serie de links. Encuadró la conducta en el delito de daño informático, previsto en el art. 183, párr. 2, del Código Penal.

Agrega que, de la prueba producida por el área de Cibercrimen de la Policía Metropolitana sobre los servidores de Grupo MSA SA, se constató que en esa fecha el servidor de la firma había sido objeto de al menos cuatro accesos indebidos a su sistema informático, que ocasionaron daños diversos. Remarcó que dos de esos accesos habían sido realizados desde el exterior y los dos restantes desde Argentina.

Añade que, en virtud de las tareas de investigación realizadas, se ordenó el allanamiento del domicilio de Sorianello y se secuestraron "elementos de interés del caso", sobre los que se ordenó un estudio pericial a fin de determinar si desde los dispositivos secuestrados se había ingresado al servidor de la empresa y, en caso afirmativo, la maniobra desarrollada, además de si contaban con algún archivo con información sensible que perteneciera a Grupo MSA SA, entre otros puntos de pericia presentados por la defensa de Sorianello.

Destaca que del informe realizado se detectaron 91 accesos al servidor de la empresa, sin encontrarse ningún archivo de interés o dato sensible de la empresa denunciante.

Con relación al evento "powned", detalla que, en términos de informática, significa que "el pequeño" (una persona) encuentra una vulnerabilidad a "un grande" (una empresa), donde se utiliza colocar una bandera (como símbolo) para informar que el sistema desarrollado por la empresa es vulnerable, lo que no genera ningún daño o alteración al sistema en cuestión. Resalta que ello se condice con la conversación mantenida entre Sorianello y un empleado de la empresa denunciante.

En ese marco, concluye que Sorianello había entrado al sistema, pero sin causar ningún daño, y que su actuación había sido provocada por la intención de alertar las fallas y debilidades que este presentaba.

En ese sentido, concluye que "si bien se acreditó que Joaquín Sorianello ingresó al sistema informático de la empresa `Grupo MSA´, no lo hizo de manera indebida ni causó daño alguno, sino que, por el contrato, lo hizo para dar aviso a la firma de que el sistema de seguridad era vago y podía ser vulnerado con facilidad". En ese marco, decide el archivo de la causa.

2. Gaspar Ariel Ortmann

Expte. Nro. 8143/2019, "Ortmann, Gaspar Ariel s/ averiguación de delito"

Juzgado Criminal y Correccional Federal n° 11, sentencia del 30 de noviembre de 2020

Gaspar Ariel Ortmann, ingeniero en sistemas, dedicaba parte de su tiempo a buscar distintos tipos de vulnerabilidades en sistemas de seguridad, que luego reportaba con intención de robustecer esta área tecnológica.

El 3 de octubre de 2019, desde la computadora de su casa, ingresó a la plataforma de Homebanking del Banco Nación, desarrollada y operada por Red Link SA, se autenticó con sus credenciales y, mediante y modificó la cotización del dólar dentro de su navegador. Luego, realizó múltiples operaciones de compraventa de dólares.

Ortmann se grabó a sí mismo realizando estas transacciones. Luego de ello, comunicó por email a Red Link SA (responsable de seguridad de dicho sitio web) de las operaciones realizadas. Ante el silencio guardado por Red Link SA, Ortmann intentó comunicarse con funcionarios del Banco Nación por email, LinkedIn y WhatsApp, sin recibir respuesta.

El día 23 de octubre de ese año, presentó en una sucursal del Banco Nación una nota por mesa de entradas explicando su accionar, la vulnerabilidad detectada y acompañando las capturas de pantallas que documentaban lo dicho.

Luego de ello, el 30 de octubre, el Banco Nación lo denunció ante el fuero penal y Ortmann fue procesado.

Las actuaciones se iniciaron el 31 de octubre de 2019 con la denuncia de la representante del Banco de la Nación Argentina. El Juzgado Criminal y Correccional 11 caratuló la causa como "Averiguación de Delito". El proceso se llevó a cabo, se tomaron los testimonios e informes periciales correspondientes.

El 30 de noviembre de 2020, poco más de un año después, el Juez a cargo desestimó el caso.

La sentencia

Por un lado, el Juzgado tiene en cuenta que los hechos no causaron ningún daño a los sistemas informáticos del Banco Nación y de Red Link SA. Al respecto, tiene en cuenta que las modificaciones que permitieron alterar el valor de cotización de compraventa de dólares fueron realizadas en la computadora de Ortmann, desde la cual accedió a su sesión personal de homebanking, por lo que se vieron afectadas las operaciones realizadas desde dicho usuario y no en el sistema en general.

En ese sentido, remarca que el sistema operado por Red Link presentaba previamente, por sí mismo, una deficiencia en materia de seguridad que fue descubierta y utilizada por Ortmann, no generada por él. Añade que no existieron otros casos en los que se hubiera manipulado la cotización del dólar, lo que permitiría descartar que esas conductas hayan podido causar alguno de los resultados lesivos previstos en el art. 183, segundo párrafo, del Código Penal.

Por otro lado, refiere que tanto la sesión de homebanking como las cuentas bancarias pertenecían a Ortmann, quien era cliente de la entidad al menos desde diciembre de 2017, circunstancias que, a entender del Juzgado, evidencian que lo hecho por Ortmann no configura acceso indebido a un sistema informático según lo previsto en el art. 153 bis del Código Penal.

A continuación, evalúa si los hechos investigados configuran el tipo penal previsto en el art. 173, inc. 16, del Código Penal, el cual prevé un tipo de defraudación especial mediante la utilización de cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

En este punto, tiene en cuenta que los representantes de Banco Nación y Red Link SA manifestaron que Ortmann les había notificado por distintos medios (Redes Sociales, teléfonos, WhastApp, correos electrónicos) que había realizado las operaciones que luego fueron denunciadas, lo que también se desprendía de las constancias aportadas por Ortmann. Resalta que uno de esos mensajes había sido enviado el mismo día en que se realizaran las operaciones al Gerente General de Red Link SA.

Añade que, al no tener respuesta a los diferentes avisos que realizara, Ortmann presentó el 23 de octubre de 2019 una nota ante el Banco de la Nación Argentina en la que acompañó los distintos mensajes de notificación que había enviado a través de diferentes plataformas.

Considera de suma relevancia que el destino de la suma obtenida por las operaciones cuestionadas fue recuperado en su totalidad por la entidad

bancaria. En ese sentido, remarca que, si bien las cuentas de Ortmann registraron movimientos, tanto ingresos como egresos, siempre tuvieron saldo suficiente para hacer frente a la devolución total del perjuicio causado, lo que finalmente se concretó luego del proceso legal, lo que también contó con la colaboración de Ortmann.

Añade que no fueron detectadas transferencias u otro tipo de operaciones tendientes a impedir el recupero de los fondos, así como tampoco la adopción de ningún tipo de maniobra con el objeto de encubrir, enmascarar y/o dificultar el rastreo de la procedencia y origen de dichas operaciones.

Menciona que Red Link cuenta con múltiples controles que le permiten detectar este tipo de operaciones anómalas, por lo que las maniobras investigadas en ningún momento tuvieron posibilidad de ser concretadas sin ser descubiertas por los distintos sistemas de seguridad de la empresa, circunstancias que difícilmente pudo haber desconocido Ortmann dada su expertise en la materia.

Considera que Ortmann en ningún momento intentó ocultar su responsabilidad por lo sucedido sino que, por el contrario, siempre estuvo en su voluntad realizar las operaciones y que luego se supiera que había sido él quien las había llevado a cabo, todo ello con la intención de demostrar la vulnerabilidad del sistema operado por Red Link. Entiende que esto se ve fortalecido con el hecho de que en el pasado Ortmann había reportado una vulnerabilidad similar a la analizada.

Agrega que incluso algunas de las operaciones de compraventa de dólares cuestionadas habían sido realizadas en detrimento patrimonial del propio encausado, lo que también evidencia que la intención del nombrado no estaba dirigida a causar un perjuicio patrimonial a las arcas del Banco de la Nación Argentina, sino a probar las debilidades del sistema informático antes aludido.

Por último, menciona que el delito previsto en el art. 173, inc. 16, del Código Penal admite solo el dolo directo para su configuración, requiriendo el conocimiento y la voluntad de utilizar el fraude para perjudicar un patrimonio.

Con base en los argumentos expuestos y a la prueba, entiende que la conducta desplegada por Ortmann resulta atípica al no verificarse en el caso el elemento volitivo requerido por el tipo subjetivo y, en consecuencia, decreta el sobreseimiento en los términos de lo previsto en los arts. 334 y 336, inc. 3, del Código Procesal Penal de la Nación.

3. Javier Smaldone

Expte. 55276/2019 "NN s/ violación de correspondiecia, violación sist. informático art. 153 bis 1° párrafo"

Juzgado Criminal y Correccional Federal n° 9, sentencia del 24 de noviembre de 2021

El 12 de julio de 2019, un día después de las elecciones Primarias, Abiertas, Simultáneas y Obligatorias (PASO), bajo el nombre @lagorraleaks, fueron filtrados más de 700 gigabytes de información sensible de los servidores de la Policía Federal Argentina (PFA).

Javier Smaldone, investigador de seguridad digital y reconocido experto en la comunidad de infosec, ante esta filtración, escribió en su cuenta de Twitter manifestando la gravedad del hecho, recomendó no descargar la información que se había filtrado y mencionó la similitud del caso con otros hechos anteriores. Luego de ello, comenzó contra él un proceso de persecución que duró años.

Las actuaciones se iniciaron el 7 de agosto de 2019 a raíz de una denuncia formulada el 5 de agosto del mismo año por la División Investigación en Delitos Tecnológicos de la PFA, ante la Cámara Nacional de Apelaciones en lo Criminal y Correccional.

Según la denuncia, varias áreas institucionales de dicha fuerza habían sufrido una intromisión maliciosa en distintos correos de uso institucional. Detallaba que la maniobra se había iniciado con la recepción de un correo electrónico que contenía un link que redirigía a una página web. En esa página, que contaba con la imagen de fondo de la Superintendencia de Bienestar de la PFA, se presentaba un formulario donde requería el acceso mediante nombre de usuario y contraseña. Esto permitía obtener las credenciales de los usuarios (nombre de usuario, contraseña y registro de datos) y lograr así el acceso al servidor.

Entre las medidas efectuadas en el marco de la investigación se sumaron diferentes informes efectuados por la división de Ciberpatrullaje de la PFA entre los que se incluyó el monitoreo de las cuentas de twitter y de Telegram de Smaldone, ambas @mis2centavos. Además, se solicitaron listados de llamadas entrantes y salientes de distintas líneas telefónicas, entre ellas, las de Smaldone, y se le solicitó a la red social WhatsApp el reporte de todos los datos de la cuenta -incluyendo las direcciones de IP-.

Luego de las medidas de prueba se presentó un informe y con el resultado de las tareas realizadas se solicitó el allanamiento y detención, entre otras, las de Smaldone. Se le incautaron celulares, tarjetas de memoria, notebooks, pendrives, entre otros elementos.

El 17 de noviembre de 2021, luego de un extenso proceso en que Smaldone denunció irregularidades y en que más de 20 ONGs, argentinas y de la región, emitieron un comunicado dirigido al juez de la causa y a la entonces Ministra de Seguridad manifestando su preocupación y descontento por todas las violaciones constitucionales que había sufrido, el Fiscal determinó que no había elementos para vincular a los sospechosos, entre ellos Smaldone, a la causa en cuestión.

El juez, basándose en el dictamen del Fiscal, entendió que no existía acción penal que reprimir o dilucidar y, en consecuencia, sobreseyó a los imputados (art. 336, inc. 4°, y 195, 2° párr., CPCCN).

Dictamen fiscal que solicita el sobreseimiento de Smaldone

Fiscalía Nacional en lo Criminal y Correccional n° 1, 17 de noviembre de 2021

Remarca que entre las investigaciones realizadas en el marco de la causa la División Investigación de Delitos Tecnológicos de la PFA informó que había llevado a cabo ciertas averiguaciones sobre los hechos de 2017 que afectaban la cuenta particular de Twitter de la ex Ministra de Seguridad de la Nación, Patricia Bullrich, entendiendo que existía un mismo *modus operandi* que en este caso. Por ello, individualizaron a aquellos responsables del hecho señalando, entre otros, a Smaldone, de quien se contaba con sus cuentas de correo, documentos de identidad y domicilios vinculados.

En ese marco, aclara que "la vinculación con los nombrados resultaba de la apreciación que se realizaba respecto a las similitudes de las maniobras que consistían en hackear las cuentas públicas, divulgando información sensible a través de las redes sociales".

Destaca que una vez recuperada su libertad, Smaldone se presentó ante la justicia a tomar vista del expediente y hacer las presentaciones necesarias con el objetivo de mostrar su inocencia.

Remarca que "[l]uego de que se señalara a los imputados como posibles autores de los hechos, todas las medidas de prueba posteriores en la investigación giraron en torno a procurar probar su participación".

Agrega que "[d]e todas las presentaciones, se destacan los descargos

efectuados por el imputado Smaldone quien además de contrarrestar la prueba, se refirió a su vínculo con la causa 1033/17 del Juzgado Nacional Criminal y Correccional Federal nro. 2, Secretaría nro. 4, en la que se le recibió declaración testimonial no estando imputado en la misma, como afirmara oportunamente el personal policial para dar inicio a la recolección de prueba en su contra... Además alegó que muchas de las consideraciones que se aludían en los informes respecto a su cuenta de twitter eran esencialmente cuestiones políticas y opiniones o conceptos respecto de los hechos... También en uno de sus escritos cuestionó el pedido realizado a[l Juez de la causa] por parte del personal policial respecto al abonado telefónico 358602 sobre el que se requirió llamadas entrantes y salientes, las antenas de activación del servicio y la transferencia de datos del abonado en cuestión desde el 01/07/2019 y, todos los datos con los que cuenten al momento de la registración del mismo. Así afirmó desconocer el origen de la pesquisa en relación a su teléfono celular, criticando también los reportes de geolocalización que lo vinculan y las fechas sobre las cuales se pide información de su teléfono. Además indicó que algunas de las medidas dispuesta por [el Juez de la causa] a requerimiento del personal policial, no se contaron respecto de otros investigados. Y volviendo al contenido de sus publicaciones argumentó que no hubo posteos en los que el nombrado se haya adjudicado algún tipo de participación en los hechos investigados, refiriendo solamente a sus tweets en los cuales puso de manifiesto la gravedad de lo sucedido."

Remarca que el 20 de diciembre tomó intervención la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) y con fecha 22 de marzo de 2021 el Titular, Dr. Azzolin, entendió que la maniobra desplegada habría sido posible mediante la conjugación de dos vectores de ataque.

Por un lado, se habría logrado montar en los servidores web de la Superintendencia de Bienestar de la PFA. Puntualmente, una página web le solicitaba al visitante que introduzca su nombre de usuario y contraseña. Ello podría haberse logrado mediante el uso de técnicas de inyección de código PHP y/o otras que podrían haber permitido el acceso en forma ilegítima a los sistemas y la creación de la página en cuestión. La referida página se encontraba diseñada de modo tal que la información suministrada por el visitante, por medio de un formulario, fuera recopilada en un archivo que luego podía ser relevado por los autores de la maniobra.

Por otro lado, el segundo vector de ataque se desarrolló cuando los atacantes enviaron correos electrónicos a las casillas creadas sobre plataformas gratuitas de webmail por diferentes dependencias de la PFA, principalmente, cuentas de Gmail.

En ese marco, la UFECI entendió que las menciones realizadas en los

grupos de Telegram como parte de la prueba producida no constituyen elementos de suma relevancia probatoria. En ese sentido, refiere que Smaldone es una figura más o menos pública, conocida en el ámbito de la informática y la ciberseguridad, por lo que su sola mención no invita a presumir un vínculo de la naturaleza sugerida.

Así afirmó que "(...) el caso analizado tomó rápidamente estado público, por lo que no sorprende que una gran cantidad de personas relacionadas con dichos sectores haya mostrado un interés legítimo, emitido diferentes opiniones sobre lo sucedido y publicado información del caso a través de las redes sociales. Así, las publicaciones y las referencias que pudieran haber efectuado cualquiera de los nombrados sobre el caso y sus conocimientos en la materia tampoco podrían interpretarse como un indicio de su participación en los hechos...".

Destaca que el Dr. Azzolin advierte que "(...) es un conjunto de apreciaciones sin rigor científico ni anclaje concreto en elementos objetivos del caso (las evidencias recolectadas (...) parecerían dirigir la investigación hacia otras personas), que pretenden vincular a un perfil determinado de persona con un hecho. O, en realidad, a un posible perfil de persona inferido de las expresiones públicas en una red social concreta que tiene una lógica comunicacional específica...".

En conclusión, la unidad especializada en la materia entiende que la prueba recabada no se vincula con las personas señaladas en la causa.

En ese marco, el fiscal de la causa, analizando el informe producido por quienes tienen los conocimientos técnicos suficientes, afirma, en concordancia con la UFECI, que las personas que llevaron a cabo la maniobra tenían conocimientos en la materia.

Agrega que, "el solo conocimiento informático no debería ser el norte que vinculara a los autores con el hecho acontecido. Lo cierto es que, a esta altura de la investigación se han dispuesto diferentes medidas de prueba en autos a fin de lograr acreditar la veracidad de los extremos denunciados, no obteniéndose ningún dato cierto que permita identificar una maniobra delictiva atribuida a los mencionados en los informes labrados por personal policial, ni en la prueba recolectada luego de los allanamientos, elementos que fueran objeto de análisis de la Unidad Especializada en ciberdelito y que concluyera en este caso como el suscripto, según lo que se relatara anteriormente".

Por ello, ante la inexistencia de elementos que hagan variar el estado de inocencia que goza todo imputado, entiende que debe desvincularse la imputación, pues integra la garantía de defensa en juicio el derecho, de

rango constitucional, de todo imputado a obtener una decisión judicial en un tiempo razonable, deviniendo en consecuencia procedente adoptar un temperamento desincriminatorio y definitivo.

Así, solicita que se decrete el sobreseimiento conforme lo dispuesto en el art. 336, inc° 4. CPPN.