10.18800/themis.202301.023

EL DELITO DE *HACKING* O ACCESO ILÍCITO A SISTEMAS INFORMÁTICOS

HACKING OFFENCES OR ILLEGAL ACCESS TO COMPUTER SYSTEM

Ricardo Nicanor Elías Puelles*
Exmiembro de THĒMIS
Estudio Elías Puelles

In this article, the author examines the crime of illegal access to computer systems. To do so, he highlights the increase in reports over the last five years, analyzes the legislative proposal outlined in the Convention on Cybercrime, and reviews the legal formulas adopted by Latin American states that have adhered to the Convention. Then, the author conducts a historical study of computer intrusion crimes in Peruvian criminal legislation and analyzes different issues that arise in the current wording, concluding this section with a proposal for lege ferenda*.*

In the second part, the author notes that hackers are equated with cybercriminals, which creates prejudices or stigmas towards this community and biases in criminal investigations, which could, in turn, lead to erroneous judicial decisions.

Keywords: Illicit access; hacking; cybercrime; computer crime.

En el presente artículo, el autor analiza el delito de acceso ilícito a sistemas informáticos. Para ello, advierte el aumento de denuncias en el último quinquenio, analiza la propuesta normativa recogida en el Convenio sobre la Ciberdelincuencia y las fórmulas legislativas adoptadas en los estados latinoamericanos que se han adherido. Luego, realiza un estudio histórico del delito de intrusismo informático en la legislación penal peruana y analiza diferentes problemas que surgen en la redacción actual, finalizando esta sección con una propuesta de lege ferenda*.*

En la segunda parte, el autor advierte que se equipara a los hackers *con los ciberdelincuentes lo que origina prejuicios o estigmas sobre esta comunidad y sesgos en las investigaciones criminales, lo que podría, a su vez, ocasionar decisiones judiciales erróneas.*

Palabras clave: Acceso ilícito; hacking; cibercrimen; delito informático.

* Abogado. Estudio de posgrado en Teoría del Delito por la Universidad de Buenos Aires (Argentina). Especialista en garantías constitucionales de la investigación y la prueba en el proceso penal y Especialista en Derecho Penal y Comportamiento Humano: Avances desde la Neurociencia y la Inteligencia Artificial por la Universidad de Castilla, La Mancha (España). Maestro en Razonamiento Probatorio por la Universidad de Girona (España). Miembro de la III escuela de verano en Ciencias Criminales y Dogmática Penal Alemana por la Georg-August-Universität Göttingen (Alemania). Profesor en pregrado y en la maestría de Derecho Penal de la Pontificia Universidad Católica del Perú (PUCP). Presidente del Instituto Peruano de Razonamiento Probatorio (IPRP) y del Observatorio Peruano de Cibercriminalidad. Socio Fundador del Estudio Elías Puelles. Contacto: ricardo@eliaspuelles.com

Nota del Editor: El presente artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 20 de marzo de 2023, y aceptado por el mismo el 22 de junio de 2023.

I. INTRODUCCIÓN

La investigación de los ciberdelitos no es una labor fácil, pues, además, de la volatilidad de la prueba digital, exige que los operadores tengan ciertos conocimientos tecnológicos. Si bien el distrito fiscal de Lima Centro cuenta con una Fiscalía Corporativa Especializada en Ciberdelincuencia, cuyas labores iniciaron el 15 de febrero del 2021[1], las investigaciones en el resto del país continúan a cargo de fiscalías penales no especializadas asistidas, de ser el caso, por la 'Red de fiscales en ciberdelincuencia a nivel nacional' –la cual es muy importante, pero no suficiente–. A partir de un caso archivado, graficaré cuán útil es comprender los alcances del delito de acceso ilícito para planificar adecuadamente la investigación criminal[2].

El 29 de octubre del 2019, una ciudadana acudió a la comisaría a presentar una denuncia verbal, en los siguientes términos:

> En la ciudad de [...] siendo las 11:48:13 horas del día 29/10/2019, se presentó ante el suscrito el denunciante manifestando que el día 27/10/2019 a las 12:30:00 horas fueron víctimas del jaqueado de sus correos, por parte de personas desconocidas, quienes empleando medidas de engaño solicitaban las cuentas de correo, número de celulares y asimismo que había un trabajo de campaña de enviar fotos de chicas desnudas para campaña de cáncer de seno, a lo cual pagarían la suma de 500 soles. Cabe mencionar que la agraviada fue jaqueada de su correo el 28OCT19, a horas 21:00, desconociendo quiénes serían autores del hecho. Asimismo, refieren que dicha denuncia obre como constancia, lo que denuncia ante la Policía Nacional del Perú para los fines consiguientes, firmando la presente acta en presencia del instructor [*sic.*].

Al día siguiente, la comisaría remitió el acta de denuncia verbal al Ministerio Público. Dos semanas después, el 18 de noviembre del 2019, sin realizar actos de investigación, se archivó el caso, argumentando que no se identificó al posible autor del evento criminal:

> Ahora, respecto a la individualización de los imputados se tiene únicamente el dicho de las denunciantes, quienes refieren que se trató de sujetos desconocidos; no contando con otros elementos que permitan dicha individualización y posterior identificación, por lo que, en este estado no resulta posible sostener la tesis incriminatoria contra una persona determinada; lo que resulta necesario, pues todo proceso penal, para poder llevarse a cabo, requiere de un imputado debidamente determinado, plenamente individualizado, como presunto autor de un hecho ilícito [...] De lo mencionado hasta el momento se tiene que la acción penal no ha prescrito y existen indicios de la existencia del delito; pero no se ha identificado a su o sus autores; por lo que corresponde aplicar lo establecido en el numeral 3 del artículo 334 del Código Procesal Penal, solicitando a la Policía Nacional del Perú que, a través de sus unidades especializadas, continúe con los actos de investigación tendientes a la consecución de dicho fin. Precisándose a su vez, que el presente caso podrá ser reexaminado en el supuesto que se descubran con posterioridad nuevos elementos de convicción [...] [*sic*].
>
> Decisión Fiscal [...] 1. Que, no procede formalizar ni continuar con la investigación preparatoria contra los que resulten responsables por la presunta comisión de delito informático en agravio de [...], ordenándose el archivo de lo actuado.
>
> 2. Notificar con la presente disposición a la DIVINCRI PNP a efectos, por intermedio de sus unidades especializadas en esta clase de ilícitos, realice los actos de investigación tendientes a la ubicación del o los responsables del hecho denunciado; debiendo informar a este despacho si los resultados arribados son positivos.

Esta decisión fue notificada a la denunciante, quien no interpuso recurso de elevación de actuados –en palabras sencillas, no 'impugnó' la decisión–. De esta forma, en vez de abrir investigación preliminar, la fiscalía archivó el caso, ordenando que la carpeta sea remitida a la policía. A continuación, analizaré algunos problemas en la recepción de la denuncia verbal y en el archivo del caso:

– En primer lugar, la redacción del acta no permite conocer si nos encontramos frente a una, dos o más víctimas. Este punto es relevante para identificar el objetivo del ciberdelincuente: ¿Una persona específica, un grupo que comparte algún vínculo o, simplemente, víctimas al azar?

– En segundo lugar, el acta no recoge información adicional sobre la hora del ataque: ¿Cómo se sabe que fue a las 12:30:00? ¿Aca-

[1] Véase a la Resolución de la Fiscalía de la Nación 1503-2020-MP-FN (2020).

[2] El presente relato pertenece a una denuncia real, sin embargo, he eliminado todo dato personal que permita identificar a la víctima o la unidad policial o fiscal que estuvo a cargo.

so se recibió una alerta sobre la vulneración del sistema informático? Hubiese sido importante profundizar este punto y, así, conocer los detalles del acceso ilícito.

– En tercer lugar, no se precisan las cuentas de correo electrónico cuyas medidas de seguridad fueron vulneradas. Conocer esta información permitiría saber si nos encontramos frente a una posible brecha de seguridad o, quizás, ante un *malware* que permite capturar contraseñas o ejecutar otra acción ilícita.

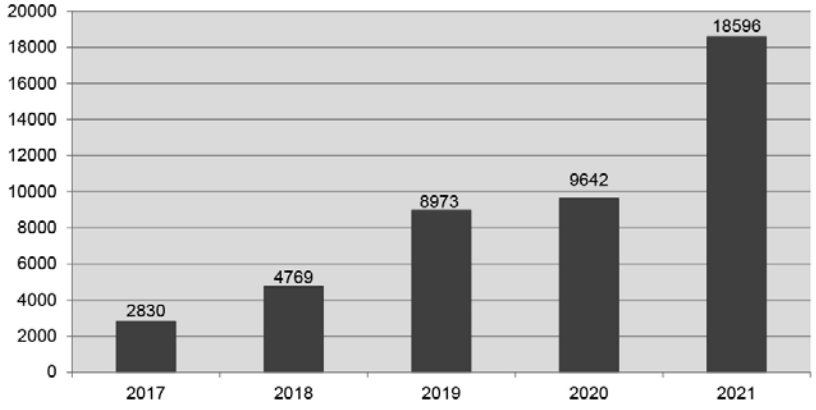
– En cuarto lugar, no se solicitó información sobre las medidas de seguridad que protegen los correos electrónicos vulnerados. Así, el agente policial que recibió la denuncia debió resolver, entre otras, las siguientes interrogantes: ¿Cuán robustas son la contraseñas?, ¿cuenta con autentificación en dos pasos? ¿Ha compartido su contraseña con alguna persona cercana?, ¿Escribe su contraseña en algún lugar al cual pueden acceder otras personas? Como veremos en esta publicación, el art. 2 de la Ley de Delitos Informáticos (en adelante, LDI), recoge las **medidas de seguridad** como uno de los elementos objetivos del tipo. Por esta razón, es importante no sólo conocer si contaba con dichas medidas sino, también, requerir más información para trazar eventuales líneas de investigación que permitiese responder si fueron vulneradas de manera física o remota.

– En quinto lugar, la víctima precisa que no conoce la identidad del ciberdelincuente o de quienes se encuentran detrás de este ilícito accionar –como pasa frecuentemente en este tipo de casos–. Sin embargo, esta no es una razón válida para que se archive la denuncia sin realizarse un solo acto de indagación. Así, para iniciar diligencias preliminares no se requiere identificar al responsable. El Ministerio Público pudo trazar un plan de investigación orientado al aseguramiento de las pruebas y la identificación del ciberdelincuente, pero no lo hizo. Ya sea que la víctima dejó consentir el pronunciamiento por desinterés o por ausencia de asesoría adecuada, lo cierto es que no se logró conocer quién o quiénes estuvieron detrás del ataque.

Debo precisar que el caso analizado no tiene por finalidad cuestionar la labor de la Policía Nacional del Perú o la del Ministerio Público, pues existen muchos operadores comprometidos en la lucha frontal contra la ciberdelincuencia. Más bien, se busca ejemplificar lo que sucede cuando un caso no es atendido de forma diligente.

Finalmente, considero importante traer a colación algunas estadísticas que demuestran la necesidad de abordar este delito, tanto desde el plano exegético como de investigación criminal. Como el lector intuirá, el número de denuncias por ciberdelitos ha aumentado dramáticamente en nuestro país, por lo que los operadores del sector justicia deberán, de un lado, realizar adecuadas interpretaciones jurídicas y, de otro, eficientes investigaciones en entornos digitales para evitar que la impunidad proteja a los ciberdelincuentes. A continuación, presento dos cuadros adaptados del documento denominado 'Ciberdelincuencia: Reporte de Información Estadística y Recomendaciones para la Prevención', elaborado por el Ministerio de Justicia y Derechos Humanos y publicado en agosto del 2022. El primero refleja el incremento anual de denuncias interpuestas en el Ministerio Público por la comisión de ciberdelitos entre el 2017 y el 2021. El segundo, de manera específica, el aumento de denuncias de parte interpuestas por los delitos de acceso ilícito (art. 2 de la LDI), atentado contra la integridad de datos informáticos (art. 3 de la LDI) y sistemas informáticos (art. 4 de la LDI).

Gráfico 1: Delitos informáticos denunciados en el Ministerio Público a nivel nacional, 2017-2021



Fuente: Adaptación propia a partir de 'Ciberdelincuencia. Reporte de Información estadística y recomendaciones para la prevención' (Ministerio de Justicia y Derechos Humanos, 2022, p. 4).

Cuadro 1: Delitos contra datos y sistemas informáticos denunciados en el Ministerio Público a nivel nacional según tipo de delito, 2017-2021

DELITO / ART.	2017	2018	2019	2020	2021
Art. 2: Acceso ilícito	53	70	139	209	386
Art. 3: Atentado contra la integridad de datos informáticos	25	28	56	121	82
Art. 4: Atentado contra la integridad de sistemas informáticos	2	11	11	11	20
S/A: Sin especificar	48	62	113	96	93
TOTAL	**128**	**171**	**319**	**437**	**581**

Fuente: Adaptación a partir de Ministerio de Justicia y Derechos Humanos (2022 p. 15).

II. PRIMERA PARTE. MARCO NORMATIVO Y ANÁLISIS DEL TIPO PENAL

En las líneas siguientes analizaré cómo se encuentra regulado el delito de acceso ilícito en el Convenio sobre la Ciberdelincuencia, al cual Perú se adhirió en el 2019, y comentaré brevemente los párrafos 44 a 50 del Informe Explicativo del citado Convenio, pues permiten interpretar sus alcances. Luego, citaré legislación comparada de los países de la región que también se han adherido al Convenio con la finalidad de conocer las modalidades recogidas y su afinidad con la legislación peruana. Finalmente, realizaré un breve recuento sobre la evolución del delito de acceso ilícito desde su incorporación al Código Penal (en adelante, CP), en el 2000, hasta su actualización en la LDI del 2013.

A. Regulación en el Convenio sobre la Ciberdelincuencia

El Convenio sobre la Ciberdelincuencia o Convenio de Budapest es el principal instrumento internacional en la lucha contra este fenómeno delictivo. Junto a su Informe Explicativo, fue aprobado por el Comité de Miembros del Consejo de Europa en su reunión número 109, celebrada el 08 de noviembre del 2001, y abierto a la firma en Budapest, el 23 de noviembre del 2001, con motivo de la celebración de la Conferencia Internacional sobre la Ciberdelincuencia.

Es importante destacar que el Convenio ha sido firmado y ratificado por 68 países, dentro de los cuales se encuentran países no miembros del Consejo de Europa. En América Latina, nueve países lo han ratificado con ciertas declaraciones y reservas:

Tabla 1: Países latinoamericanos que han ratificado el Convenio sobre la Ciberdelincuencia

País	Fecha de ratificación	Entrada en vigor	Declaraciones y/o reservas
1. Brasil	22 de diciembre del 2021	30 de noviembre del 2022	Sin información disponible.
2. Colombia	16 de marzo del 2020	01 de julio del 2020	Una reserva. Tres declaraciones del 16 de marzo del 2020.
3. Perú	26 de agosto del 2019	01 de diciembre del 2019	Tres reservas. Cuatro declaraciones del 26 de agosto del 2019.
4. Paraguay	30 de julio del 2018	01 de noviembre del 2018	Sin reservas. Tres declaraciones del 30 de julio del 2018.
5. Argentina	05 de junio del 2018	01 de octubre del 2018	Cinco reservas. Dos declaraciones del 05 de junio del 2018.
6. Costa Rica	22 de setiembre del 2017	01 de enero del 2018	Dos reservas. Dos declaraciones del 22 de setiembre del 2017.
7. Chile	20 de abril del 2017	01 de agosto del 2017	Cinco reservas. Dos declaraciones del 20 de abril del 2017.
8. Panamá	05 de marzo del 2014	01 de julio del 2014	Sin reservas. Tres declaraciones del 05 de marzo del 2014.
9. República Dominicana	07 de febrero del 2013	01 de junio del 2013	Sin reservas. Dos declaraciones del 07 de febrero del 2013.

Fuente: Velasco San Martín, C., & Velásquez, A. (2021, p. 81).

El Convenio está estructurado en cuatro capítulos y tiene como finalidad primordial los siguientes objetivos, los cuales se recogen en el párrafo 16 del Informe Explicativo:

a. Armonizar los elementos de los delitos conforme al derecho sustantivo penal de cada país y las disposiciones conexas en materia de delitos informáticos.

b. Establecer conforme al derecho procesal de cada país los poderes necesarios para la investigación y el procesamiento de dichos delitos, así como también de otros delitos

cometidos mediante el uso de un sistema informático o las pruebas conexas que se encuentren en formato electrónico.

c. Establecer un régimen rápido y eficaz de cooperación internacional.

Luego de haber establecido su importancia, he de indicar que Perú se adhirió al Convenio mediante Resolución Legislativa 30913 del 12 de febrero del 2019, acto ratificado a través del Decreto Supremo 010-2019-RE del 9 de marzo. Así, entró en vigor el primer día de diciembre de ese mismo año.

Ahora bien, bajo el título 'Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos', el Convenio recoge el acceso ilícito (art. 2), la interceptación ilícita (art. 3), los ataques a la integridad de los datos (art. 4), los ataques a la integridad del sistema (art. 5) y el abuso de los dispositivos (art. 6). Toda vez que esta publicación gira en torno al delito de acceso ilícito, es importante conocer cómo se encuentra regulado:

> Art. 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 seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático (Convenio sobre la Ciberdelincuencia, 2001).

El art. 40 del Convenio, se prevé que los Estados podrán declarar, en el momento de la firma o del depósito del instrumento de ratificación, aceptación, aprobación o adhesión, que se acogen a la facultad de exigir, llegado el caso, uno o más elementos complementarios previstos en los arts. 2, 3, 6.1.b), 7, 9.3 y 27.9.e). Es en uso de esta facultad que Perú realizó la siguiente declaración respecto al delito bajo estudio:

> De conformidad con lo dispuesto en el artículo 2 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que su legislación exige que el delito de acceso ilícito se cometa infringiendo medidas de seguridad (Resolución Legislativa 30913, 2019).

Cada artículo del Convenio ha sido desarrollado en el Informe Explicativo. En el caso del delito de acceso ilícito, los párrafos 44 a 50 recogen algunas ideas muy importantes que resumo a continuación y que, en algunos casos, comentaré brevemente:

- El párrafo 44 indica que el acceso ilícito es un 'delito básico' que amenaza peligrosamente o ataca la seguridad informática, compuesta por la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos. Además, se distinguen tres modalidades que suelen equipararse: (i) mera intrusión no autorizada, piratería o *hacking*; (ii) el sabotaje o *cracking;* y (iii) la intrusión en el ordenador o *computer trespass*. Así, se precisa que este delito "puede constituir un impedimento para los usuarios legítimos de los datos y sistemas y puede causar alteración o destrucción [...]" (2001, p. 13), sin embargo, he de indicar que no es condición necesaria o el paso previo indispensable para la comisión de otros ciberdelitos.

- El párrafo siguiente resalta la importancia de las medidas de seguridad para la prevención del acceso ilícito. Sobre este punto, es importante recordar que nuestro país exige la vulneración de las medidas en referencia para su configuración típica.

- En el párrafo 46, se define el término 'acceso' como 'la entrada a un sistema informático o a alguna parte del mismo (*hardware*, componentes, datos almacenados del sistema instalado, directorios, datos relativos al tráfico y datos relacionados con los contenidos)'. Además, se precisa que esta definición incluye:

  > El ingreso a otro sistema informático, al que esté conectado a través de redes de telecomunicaciones públicas, o a un sistema informático que esté conectado a la misma red, como una LAN (red de área local) o una Intranet (red interna) que opere en el seno de una organización (2001, p. 14).

- El párrafo siguiente precisa que la conducta debe ser cometida de manera 'ilegítima' y que este no es el caso del acceso autorizado para realizar una verificación o protección del sistema informático, ni tampoco al ingresar a sistemas que permiten el acceso libre y abierto al público. Sobre este punto, he de indicar que la LDI fue modificada para incluir expresamente los términos 'deliberada' e 'ilegítimamente', pese a que no era necesario –como más adelante se explicará–.

- El párrafo subsiguiente nos recuerda que el mantenimiento de un sitio web o la aplicación de herramientas estándar provistas en los protocolos y programas de comunicación no es *per se* ilegítima. Grafica este punto con

el uso de *cookies*, ya que pueden ser rechazadas o eliminadas por el usuario que accede a las páginas.

– El párrafo 49 resalta la controversia que existe sobre la tipificación del mero intrusismo ya que la legislación de algunos países no sanciona el acceso que no crea peligro alguno en el usuario o que ayuda a detectar 'agujeros' o puntos débiles de los sistemas de seguridad. No es el caso peruano, pues, como veremos más adelante, sí sanciona esta modalidad.

– Finalmente, el párrafo 50 remarca que los Estados tienen la posibilidad de tipificar el acceso ilícito, en los términos recomendados en la primera parte del art. 2 del Convenio, agregar o matizar los alcances de la segunda parte. Es importante recordar que Perú incorporó la 'vulneración de medidas de seguridad' como elemento adicional del tipo penal.

B. Legislación comparada

Conocer la regulación del delito de acceso ilícito en la legislación del resto de países latinoamericanos que se adhirieron al Convenio de Budapest[3], así como en España por su gran influencia en la materia, permitirá comparar su marco punitivo y conocer modalidades no previstas en Perú.

Tabla 2: Países latinoamericanos que se adhirieron al Convenio de Budapest

País	Legislación	Tipo penal
Países latinoamericanos que se adhirieron al Convenio de Budapest		
Brasil	Código Penal, modificado por la Ley 14 155 (2021).	**Art. 154 A.-** Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
Colombia	Código Penal, modificado por la Ley 1273 (2009).	**Art. 269 A.-** Acceso abusivo a un sistema informático. 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.
Paraguay	Código Penal, modificado por la Ley 4439 (2011).	**Art. 146 B.-** Acceso indebido a datos. 1. El que sin autorización y violando sistemas de seguridad obtuviere para sí o para terceros, el acceso a datos no destinados a él y especialmente protegidos contra el acceso no autorizado, será castigado con pena privativa de libertad de hasta tres años o multa. 2. Como datos en sentido del inciso 1°, se entenderán solo aquellos, que se almacenan o transmiten electrónicamente, magnéticamente o de otra manera no inmediatamente visible.
Argentina	Código Penal, modificado por la Ley 26.388 (2008).	**Art. 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 financieros.
Costa Rica	Código Penal, modificado por la Ley 8148 (2001).	**Art. 196.-** Será reprimida con pena de prisión de seis meses a dos años, la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos. La pena será de uno a tres años de prisión, si las acciones descritas en el párrafo anterior, son realizadas por personas encargadas de los soportes: electrónicos, informáticos, magnéticos y telemáticos.

[3] El orden de los países no es aleatorio sino que inicia con Brasil –cuya adhesión es la más reciente– y continúa hasta República Dominicana –la más antigua adhesión de la región–.

País	Legislación	Tipo penal
Chile	Ley 21459 (2022).	**Art. 2.-** El que, sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales. Si el acceso fuere realizado con el ánimo de apoderarse o usar la información contenida en el sistema informático, se aplicará la pena de presidio menor en sus grados mínimo a medio. Igual pena se aplicará a quien divulgue la información a la cual se accedió de manera ilícita, si no fuese obtenida por éste. En caso de ser una misma persona la que hubiere obtenido y divulgado la información, se aplicará la pena de presidio menor en sus grados medio a máximo.
Panamá	Código Penal (2010).	**Art. 289.-** Quien indebidamente ingrese o utilice una base de datos, red o sistema informático será sancionado con dos a cuatro años de prisión.
República Dominicana	Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología (2007)	**Art. 6.-** Acceso Ilícito. El hecho de acceder a un sistema electrónico, informático, telemático o de telecomunicaciones, o a sus componentes, utilizando o no una identidad ajena, o excediendo una autorización, se sancionará con las penas de tres meses a un año de prisión y multa desde una vez a doscientas veces el salario mínimo.
Otras referencias		
España	Código Penal, modificado por la Ley Orgánica 1/2015 (2015).	**Art. 197** *bis*.- 1. El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

Fuente: Elaboración propia

C. Legislación nacional

A continuación, analizaré el delito de acceso ilícito en la legislación penal peruana. Para ello, iniciaré explicando su incorporación al CP, luego, el camino que siguió para su inclusión en la LDI y, finalmente, analizaré el tipo penal vigente.

1. Antecedentes normativos

Ocho años después de la promulgación del CP de 1991, se presentaron dos proyectos de ley que originaron la incorporación del 'Capítulo X. Delitos Informáticos' al ordenamiento[4]:

– **Proyecto de Ley 5071/99-CR**, presentado el 18 de agosto de 1999 por el congresista Jorge Muñiz Ziches. Esta iniciativa recogió la redacción más cercana del tipo penal bajo estudio[5].

– **Proyecto de Ley 5132/99-CR**, presentado el 31 de agosto de 1999 por la congresista Ivonne Susana Díaz Díaz. Cobijó una modalidad del delito de acceso ilícito que no prosperaría[6].

Cuatro meses después, ambos proyectos obtendrían un dictamen unánime favorable por parte de la Comisión de Reforma de Códigos del Congreso de la República, debiendo resaltar que no hubo debate sobre el bien jurídico tutelado ya que se aceptó, sin dudas o cuestionamientos, que se trataba del patrimonio. No obstante, en atención a las observaciones remitidas por el Poder Ejecutivo, se tuvo que aprobar un texto sustitutorio. Así, finalmente, una modalidad del delito de acceso ilícito fue recogida en el art. 207-A CP:

> Art. 207-A CP.- El que utiliza o ingresa indebidamente a una base de datos, sistema o red de

[4] Sobre la evolución de la legislación en materia de cibercrimen, véase a Elías Puelles (2017).

[5] Artículo 208-A.-

> El que indebidamente utilice o ingrese a una base de datos, sistema o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información será reprimido con pena privativa de libertad no mayor de dos años, o con prestación de servicios comunitario de cincuentidós a ciento cuatro jornadas (1999).

[6] Artículo 2.-

> El que con ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, lo interfiera o acceda a él, será reprimido con pena privativa de libertad no mayor de tres años (1999).

> computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuentidós a ciento cuatro jornadas.
>
> Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas (1991).

El art. 207-A CP, incorporado el 17 de julio del 2000, sancionaba el acceso indebido sin exigir la ruptura de medidas de seguridad, pero sí requería una finalidad delictiva posterior para su configuración, erigiéndose como un delito de tendencia interna trascendente. Esta norma fue derogada el 22 de octubre del 2013 con la promulgación de la LDI[7].

2. Génesis legislativa

A mediados del 2011, se recibió la primera propuesta legislativa que generaría cambios significativos en la lucha peruana contra ciberdelincuencia. Si bien fueron ocho proyectos que desembocaron en la promulgación de la LDI, solo dos se refirieron al delito de acceso ilícito:

– **Proyecto de Ley 34/2011-CR**, presentado el 11 de agosto de 2011 por el congresista Juan Carlos Eguren Neuenschwander. Esta iniciativa propuso un cuerpo normativo independiente por el nivel de especialidad que tiene la informática y la posibilidad de incluir disposiciones procesales para facilitar su investigación.

  Respecto al delito bajo análisis: (i) No exigía la vulneración de medidas de seguridad; (ii) incluía la interceptación e interferencia de sistemas informáticos como conductas prohibidas; (iii) no recogía el abuso de confianza como modalidad de acceso indebido[8].

– **Proyecto de Ley 2520/2012-PE**, presentado el 26 de julio de 2013 por el Presidente de la República Ollanta Humala Tasso. Esta iniciativa recogió la redacción exacta del tipo penal que originalmente fue incluido en la LDI[9].

3. Regulación actual

Como he señalado anteriormente, la LDI adoptó los nueve capítulos sugeridos en el Proyecto de Ley 34/2011-CR, propuesta que, bajo el nombre de 'Delitos contra los sistemas de información y las Tecnologías de la Comunicación', recomendó la tipificación de cinco delitos: (i) Intrusismo informático; (ii) Sabotaje informático; (iii) Intrusismo o sabotaje de sistemas o tecnologías de información con medidas de seguridad o información especial; (iv) Prestación de equipos y servicios con fines de intrusismo o sabotaje; y (v) Espionaje informático. Sin embargo, fue el Proyecto de Ley 2520/2012-PE el que terminó por imponer su propuesta de redacción. Este último proyecto recomendó incorporar el Título V-A al CP o 'Atentado contra los datos y sistemas informáticos', el cual tendría cuatro capítulos, de los cuales me interesa resaltar el primero, pues recoge el delito de acceso ilícito.

El capítulo II de la LDI se denomina 'Delitos contra datos y sistemas informáticos' y agrupa el delito de acceso ilícito (art. 2 de la LDI), el atentado contra la integridad de datos informáticos (art. 3 de la LDI) y atentado contra la integridad de sistemas informáticos (art. 4 de la LDI). Un lector acucioso podría preguntar: ¿Se atentan contra los datos informáticos al acceder sin autorización a un sistema? Sostengo que no; sin embargo, ¿por qué fueron agrupados de esta manera? Porque se emplea el título propuesto en el Proyecto de Ley 2520/2012-PE que, a su vez, se inspira en el Convenio de

---

7 Al respecto, Durand, R. señala:

> En el artículo 207-A si bien se sanciona la utilización o ingreso indebido a una base de datos o sistemas informáticos, con la finalidad de diseñar, ejecutar, interferir, interceptar, existirán problemas para distinguir el denominado *hacking* blanco, máxime cuando el propio legislador concibe como finalidad del ingreso el acceso, luego no puede darse una conducta de ingresar para acceder. No obstante, debemos señalar que en cuanto al aspecto subjetivo, el primer párrafo del artículo 207-A exige las finalidades antes descritas como elementos subjetivos de intención trascendente, no siendo necesario su realización material (2002, p. 311).

8 Art 3.- Intrusismo Informático. El que sin la debida autorización acceda, intercepte o interfiera un sistema de información o una tecnología de información, será reprimido con una pena privativa de libertad no menor de uno ni mayor de tres años (2011).

9 Art 208-A.- Acceso ilícito.

> El que accede sin autorización a todo o en parte de un sistema informático siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.
>
> Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado (2013).

Budapest pero que recortó la expresión completa, la que le hubiera dado sentido: 'Delitos contra la **confidencialidad**, la **integridad** y la **disponibilidad de los datos** y **sistemas informáticos**'.

Un mes después de la promulgación de la LDI, entre otras, se recibieron dos propuestas legislativas que modificaron diversos delitos –entre ellos, el acceso ilícito–, a saber:

– **Proyecto de Ley 2991/2013-CR**, presentado el 25 de noviembre de 2013 por el congresista Juan Carlos Eguren Neuenschwander. Esta iniciativa propuso incorporar las expresiones 'deliberada e ilegítima' ya que, según su autor, la LDI "no cumple con algunos de los estándares previstos en el Convenio sobre la Cibercriminalidad (Convenio de Budapest) en el sentido de no haber incorporado en la redacción típica de los delitos [...] la calidad de deliberada e ilegítima de la conducta" (2013)[10].

– **Proyecto de Ley 2999/2013-CR**, presentado el 27 de noviembre de 2013 por el congresista Mauricio Mulder Bedoya. Esta iniciativa propuso también incluir los elementos deliberado e ilegítimo. Además, sugirió suprimir el abuso de confianza como modalidad de acceso ilícito y castigar la vulneración de medidas de seguridad como figura agravada[11].

Como el lector habrá notado en la sección 'legislación comparada', ninguno de los países que se adhirieron al Convenio de Budapest recogió la fórmula aprobada por el legislador peruano, pues dicha incorporción, de un lado, reduce el ámbito de sanción y, de otro, es innecesaria. El siguiente cuadro compartivo permitirá conocer cómo se encuentra redactado, desde el 2014, el delito bajo análisis.

Tabla 3

Art. 2 LDI (original)	Art. 2 LDI (actual o vigente)
Fecha de publicación: 21 de octubre del 2013	Fecha de modificación: 10 de marzo del 2014
El que accede sin autorización a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.	El que **deliberada e ilegítimamente** accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.
Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado.	Será reprimido con la misma pena, el que accede a un sistema informático excediendo lo autorizado.

Fuente: Elaboración propia

A continuación, analizaré la fórmula legal escogida por el legislador peruano y finalizaré con una propuesta normativa.

a. Perú sanciona el mero intrusismo, hacking blanco o de desafío.

El Convenio de Budapest propuso una fórmula básica de acceso ilícito: "*el acceso deliberado e ilegítimo a todo o parte de un sistema informático*", dejando a cada Estado Parte la facultad de exigir que el delito se cometa: (i) infringiendo medidas de seguridad; (ii) con la intención de obtener datos informáticos y otra intención delictiva y (iii) en relación con un sistema informático conectado a otro sistema informático. Perú declaró que nuestra LDI "**exige que el delito de acceso ilícito se cometa infringiendo medidas de seguridad**" (Resolución Legislativa 30913, 2019); es decir, señaló que los elementos (ii) y (iii) no integran la configuración de nuestro tipo penal. Como ya he mencionado, hemos transitado por dos modelos distintos.

El actual art. 2 de la LDI sanciona el acceso ilícito cometido a través del quebrantamiento de medidas de seguridad, pero no exige una motivación delictiva adicional. En otras palabras, no requiere un elemento subjetivo distinto del dolo. En junio

[10] Art. 2.-

El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con la vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

Será reprimido con la misma pena, el que accede a un sistema informático excediendo lo autorizado (2013).

[11] Art. 2.-

El que accede de manera deliberada e ilegítima a todo o en parte de un sistema informático, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

Será reprimido con pena privativa de libertad de tres a cinco años y con noventa días-multa siempre que el delito se realice con la vulneración de medidas de seguridad establecidas para impedirlo (2013).

del 2014, cuestioné esta opción legislativa y mantengo mi posición: debería exigirse esa finalidad adicional que, incluso, es sugerida como opción por el Convenio de Budapest. No toda lesión al bien jurídico protegido debe traer la misma respuesta estatal: ¿Por qué debemos acudir al Derecho Penal frente a cualquier intrusismo informático? Lo graficaré con algunos ejemplos, sin embargo, le pido al lector que elimine de su mente aquellos accesos ilícitos que tienen una finalidad delictiva posterior pues ese tipo de acciones sí merece reproche penal y, precisamente, es lo que postulo desde la promulgación de la LDI:

– Algunos *Smart TV* permiten proteger el acceso con una contraseña, es decir, si no cuentas con la clave, no podrás utilizarlo para ver televisión. Ahora bien, pensemos en el siguiente caso: A es el jefe de un estudio jurídico y ha colocado una contraseña a todos los televisores de su oficina. B adivinó la clave '12345' y cada vez que A se retira a almorzar, él y sus compañeros ven televisión en el directorio. ¿Por qué B debe ser reprimido penalmente? ¿Acaso no sería suficiente con despedirlo o amonestarlo?

– C y D son compañeros de departamento. C se encuentra muy molesto con D, pues desde que amanece permanece absorto en su *Play Station* 5 (PS5) y no realiza las tareas de limpieza que han acordado. Pese a que han charlado en más de una oportunidad, su conducta es igual. Entonces, C ha colocado una clave de inicio de sesión a su PS5. D, al tercer intentó, adivinó la contraseña: '0000'. Es así como logra ingresar y seguir jugando. ¿El Derecho Penal debe intervenir para sancionar esta actuación?

– E es alumno del curso de Bases Romanistas del Derecho. Se encuentra muy angustiado, pues no sabe cómo le fue en la evaluación escrita. Cuando su profesor F va por un café, E ve un *post it* pegado en el teclado con la contraseña de acceso. Rápidamente ingresa al ordenador y ve su calificación, luego de lo cual cierra sesión. ¿No será suficiente el castigo que reciba por parte de su universidad? ¿Por qué deber ser reprimido penalmente?

– G y H son novios. El último fin de semana hicieron senderismo en las Lomas de Lachay. Al llegar a casa, G 'cayó rendido' y olvidó enviarle las fotografías que tomó con su celular a H. Esta última, para no despertarlo, desbloqueó el celular con la huella de G mientras dormía. Revisó las fotografías y apagó el celular –feliz por las tomas que habían conseguido–. ¿H es una ciberdelincuente? ¿La unidad especializada de la policía y la fiscalía fueron creadas para investigar este tipo de casos?

En estos cuatro ejemplos tenemos: (i) sistemas informáticos –Smart Tv, PS5, computadora, teléfono celular–; (ii) medidas de seguridad quebradas –contraseñas–; (iii) ausencia de consentimiento para el ingreso o acceso; y (iv) voluntad para ingresar a un sistema sin autorización. Tal y como se encuentra redactado nuestro tipo penal, los cuatro casos se subsumen en el art. 2 LDI. Estos ejemplos son casos de 'mero intrusismo', pues no importa la finalidad por la que ingresó el sujeto activo, ya que se castiga el simple acceso indebido. Mi crítica no busca despenalizar el delito de acceso ilícito sino incluir la finalidad delictiva posterior, es decir, tipificarlo como un delito de tendencia interna trascendente[12] –hasta que no ocurra un cambio legislativo, se deberá acudir al principio de lesividad al analizar este tipo de casos para evitar la sobrepenalización–.

Cierto sector de la doctrina nacional considera que el fundamento político criminal de este delito radica en ser el paso previo 'obligatorio' para atentar contra sistemas informáticos[13]. Discrepo respetuosamente de esta posición, por dos razones:

[12] El jurista peruano Oré Sosa (2022, p. 193) también advierte algunos problemas al castigar actuaciones de escasa potencialidad lesiva,

> [...] por el solo afán de superar un reto personal o para evidenciar la especial vulnerabilidad de los sistemas informáticos (agujeros) de algunas entidades públicas o privadas. Habrá que ver si, en casos como estos, puede excluirse la imputación apelando al criterio de la disminución del riesgo. En cualquier caso, no pasarán de constituir supuestos marginales o excepcionales, más aún si se concibe esta figura como un delito de mera actividad que se consuma en el momento mismo en que se vulnera la medida de seguridad (2022, p. 193).

Sobre el mero intrusismo, Peña Cabrera Freyre señala también: "Finalmente, parece que la tipificación quiere ser más incriminante, en tanto no se exige, como lo hacía la legislación anterior, un propósito ulterior, que no tenía que manifestarse en el mundo fenoménico para dar por realzada la acción típica" (2015, p. 161).

[13] Autores como Vega Aguilar, J., & Arévalo Minchola, M. mencionan:

> La tipificación tiene fundamento criminológico: Al analizar la ciberdelincuencia, se analiza también la modalidad criminal y en el caso de sistemas informáticos, todo acto de alteración, daño y/o modificación de este va a partir de un acceso ilícito como primer acto (2022).

(i) No es la opción legislativa adoptada en Perú. Me explico, quienes consideran que el delito de acceso ilícito facilita la comisión de otros delitos, están pensando en una fórmula legislativa distinta a la que se recoge en la LDI, es decir no en el 'mero intrusismo' sino en el 'acceso ilícito como delito de tendencia interna trascendente' –que es la propuesta legislativa más adecuada, desde mi perspectiva, pero no la recogida en nuestro país–. Bajo esta mirada, no se castigaría el acceso ilícito por el sólo hecho de ingresar sino por ingresar con una intención delictiva adicional; (ii) No se necesita acceder ilegalmente a un sistema informático para atentar contra este. Por ejemplo, puedo enviar por correo electrónico un *malware*, *software* dañino, infectarlo y perjudicar el funcionamiento del sistema informático sin haber accedido ilegalmente. De la misma forma, puedo acceder ilegalmente con una finalidad ilegal sin llegar a cometer otro delito. Es por esta razón que considero inadecuado afirmar que el delito de acceso ilícito es el paso previo de otro delito: habrá casos en que esto suceda, pero también otros en los que no. Tratémoslo como son: delitos independientes que, en algunas ocasionen, confluirán.

b. El bien jurídico penalmente protegido.

Este tópico no es pacífico, pues algunos autores sostienen que se salvaguarda la intimidad personal o familiar, la intimidad informática, el domicilio informático o la privacidad[14], entre otros. Sin embargo, este problema interpretativo surge por la ubicación del tipo penal analizado por los juristas. Así, por ejemplo, en España, el *hacking* blanco o acceso ilícito sin ulterior finalidad se encuentra en el Título de los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad de domicilio. De ahí que sea importante conocer su ubicación en el ordenamiento penal para analizarlo adecuadamente.

Como recordará el lector, el art. 207-A CP –que tipificó la primera modalidad de acceso ilícito en nuestro ordenamiento, hacia el 2000– se incorporó al Título de delitos contra el patrimonio, lo que dificultó comprender su objeto de protección. Esto se superó en el 2013 ya que el legislador lo ubicó en el Capítulo de los delitos contra los datos y sistemas informáticos de la LDI.

Personalmente, en atención a la ubicación del delito estudiado, su naturaleza –es un ciberdelito puro–, así como la adhesión del Perú al Convenio de Budapest[15], considero que se protege la seguridad de la información, de manera general, y la **confidencialidad** de los datos y sistemas informáticos, de forma específica[16]. En efecto, los delitos ubicados sistemáticamente en el primer capítulo de la LDI sancionan los actos cometidos contra tres propiedades de la seguridad informática: confidencialidad, integridad y disponibilidad[17]. No obs-

---

Los autores continúan afirmando:

> Esto es, para la comisión del delito de atentado contra la integridad de sistemas informáticos, obligatoriamente se debe haber dado un acceso ilícito. Pero dentro de esta secuencia criminal, entonces, existe justificación tanto para criminalizar el atentado concreto de sistemas informáticos, así como el simple acceso ilícito, ya que en este último caso lo que se penaliza no es la modificación o destrucción del sistema, sino el solo hecho de penetrarlo de manera ilegítima. El fundamento criminológico tendrá una forma de adelantamiento de la barrera de punición, entendiendo que no se puede dejar impune ninguna de las secuencias que recorre el plan criminal del ciberdelincuente para hacerse con datos y partes de un determinado sistema informático (2022, p. 251).

14 Sobre este punto, véase a el acápite denominado "Ubicación sistemática del nuevo artículo 197 bis CP e implicaciones en la determinación del bien jurídico protegido" de Hernández Díaz (2019, pp. 269-276). También véase a el análisis realizado sobre el art. 197 bis. de Sáenz Delgado, E. (2021, p. 277).

15 El Convenio incluye el delito de acceso ilícito en el Título de delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.

16 Sobre el particular, Rueda Martín, M.A. menciona:

> Desde nuestro punto de vista, esta es la línea correcta para definir el bien jurídico protegido en la tipificación de las conductas que consisten en un acceso ilícito a sistemas informáticos, si bien es cierto que es necesario distinguir, por un lado, la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos y, por otro lado, de los datos propiamente dichos [...] El bien jurídico aludido y que se refiere a la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos constituye una barrera de contención de riesgos para otros bienes jurídicos que se pueden encontrar involucrados en la función social que desempeñan tales sistemas y redes informáticas: la intimidad personal y familiar, el patrimonio, etc. (2009, pp. 175 y 179).

17 En esta línea, Espinoza Calderón sostiene que se protege la 'ciberseguridad'. Sobre este punto, señala que:

> la legitimidad del tipo penal que proscribe dichas acciones se evidencia una vez que la mencionada disposición es entendida como la prohibición de acceder a la seguridad de la información contenida en los sistemas de tratamiento automatizado de datos, que justamente es ell bien jurídico tutelado, advertido el particular contexto generado a raiz del apresurado desarrollo de las tecnologías de la información y de la comunicación (era de la informática) (2022, p. 70).

Por su parte, Palomino Ramírez, W. señala:

> Desde ya, puede señalarse que el acceso ilícito, el atentado a la integridad de datos o sistemas informáticos (ars. 3 y 4), la interceptación de datos informáticos (art. 7), y el abuso de mecanismos y dispositivos informáticos (art. 10) se

tante, sólo el acceso ilícito protege específicamente la confidencialidad[18], en tanto que los atentados contra los datos y sistemas informáticos hacen lo propio con su integridad y disponibilidad.

Al respecto, es importante diferenciar cuatro conceptos[19]:

- **Seguridad informática**, seguridad de la información o seguridad de los sistemas. Es la capacidad de resistir ataques a la disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad de los datos y sistemas informáticos. En la misma línea, según la Política Nacional de Ciberseguridad del Perú, la seguridad de la información se entiende como la preservación de la confidencialidad, integridad y disponibilidad.

- **Confidencialidad**. Es la característica consistente en que la información no se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. Así, se garantiza que dicha información sea accesible sólo a aquellos usuarios autorizados a tener acceso a la misma.

- **Integridad**. Es la característica consistente en que el activo de información no ha sido alterado de manera no autorizada. De este modo, se salvaguarda la exactitud y totalidad de la información, así como sus métodos de procesamiento.

- **Disponibilidad**. Es la característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. Permite garantizar que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo deseen.

Cierto sector de la doctrina nacional considera que el bien jurídico protegido es la integridad informática, "entendiendo a esta como el conjunto de datos o sistemas informáticos que debieran mantenerse incólumes e intactos ante intentos de acceso que no son permitidos o resultan ilegítimos" (Vega Aguilar, J., & Arévalo Minchola, M., 2022, p. 255). Considero que no es así, pues Perú sanciona el mero intrusismo o hacking blanco, es decir, no se exige que el ciberdelincuente haya ocasionado algún daño o generado algún peligro. En caso de que la integridad informática fuese mermada, ya no nos encontraríamos frente al delito bajo estudio sino ante los previstos en los art. 3 y 4 de la LDI.

c. Primera modalidad de acceso ilícito.

El primer párrafo del art. 2 LDI sanciona el *hacking* blanco, acceso ilícito sin ulterior finalidad o mero intrusismo.

El **sujeto activo** puede ser cualquier persona, ya que el tipo penal no exige que cuente con funciones o características especiales. Como desarrollaré más adelante, debemos evitar suponer que este tipo de delitos son cometidos por personas que poseen conocimientos especializados, pues no necesariamente es así[20].

Por **acceso a todo o parte de un sistema informático** se entiende el ingreso o entrada a todo el sistema informático o a una sección independiente de este (*hardware* o sus componentes, BIOS o *Basic Input-Output System*; UEFI o *Unified Extended Fir-*

destinan a la protección de la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos. Así lo indica el apartado 43 del IECC (2014, p. 139).

A su turno, Oré Sosa, E. y Velasco, E., & Sanchís, Cr. menciona que "son delitos que protegen más que la información, la seguridad de la información, en la creencia de que hoy en día, es a través de estas tecnologías que protegemos nuestra privacidad frente a terceros" (2022, p. 191; 2019, p. 180).

18 En esa línea, Villavicencio Terrero, F. señala:

> Esta figura penal de acceso ilícito **sanciona la violación de la confidencialidad**, que se realiza a través del acceso no autorizado al sistema, vulnerando las medidas de seguridad establecida para evitar que ajenos ingresen a un sistema informático; por el verbo rector acceder se entiende el hecho de entrar en un lugar o pasar a él, que en esta figura se entiende el acto de entrar sin autorización del titular a un sistema [el resaltado es mío] (2014, p. 291).

19 Para esta labor empleo tanto el Real Decreto 3/2010, del 08 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica de España como los Términos y definiciones recogido en la Política Nacional de Ciberseguridad del Perú.

20 Al respecto, Espinoza Calderón, V. ha señalado:

> Su comisión requiere de un agente que tenga un buen dominio de la materia, ya que estos conocimientos son aprovechados para cometer o cooperar con la comisión de delitos. En algunos casos dicha actividad persigue fines de lucro, en otras es tomado solamente como un reto de competencia entre *hackers*. Existen grupos de aficionados que se dedican a *hackear* en nuestro país, como, por ejemplo, determinados grupos de *gamers* o jugadores de videojuegos en línea que eventualmente realizan *hacking* como entretenimiento (2022, p. 73).

Discrepo respetuosamente de esta posición, pues, de un lado, no se requieren conocimientos tecnológicos avanzados para su comisión –recordemos los ejemplos que desarrollé líneas atrás– y, de otro, se estigmatiza a la comunidad *hacker*.

mware Interface, sistema operativo, aplicaciones, etcétera). Es importante recordar que no importa la intención ulterior del sujeto activo, por ejemplo, obtener datos informáticos pues se castiga el mero intrusismo o acceso ilícito.

La conducta debe **vulnerar medidas de seguridad establecidas para impedirlo**. Una defensa, salvaguarda o medida de seguridad es cualquier medio empleado para eliminar o reducir un riesgo. Su objetivo es reducir las vulnerabilidades de los activos, la probabilidad de ocurrencia de las amenazas y/o el nivel de impacto en la organización[21]. Las medidas de seguridad pueden ser activas o pasivas. Las primeras buscan anular o reducir el riesgo de la amenaza de manera preventiva (antes del incidente) o a través de su detección (durante el incidente). Las segundas buscan reducir el impacto cuando se produce el incidente, por lo que también se les conoce como medidas de corrección. El tipo penal se refiere a la trasgresión de las medidas de seguridad activas de prevención como la autenticación de usuarios, el control de acceso a los ficheros, el cifrado de datos sensibles, entre otros.

Si bien las medidas de seguridad pueden ser físicas o lógicas, considero que este tipo penal sanciona solo la vulneración de las segundas. Así, por ejemplo, si dejo mi computadora encendida y sin ningún tipo de medida de seguridad lógica, pero cierro la puerta de mi oficina para mantener alejados a terceros (seguridad física), no responderá penalmente por el delito de acceso ilícito quien irrumpe con un duplicado de la llave o fuerza la chapa de ingreso y logra ver el contenido de mi información. Llego a esta conclusión, tomando en consideración el art. 1 de la LDI, pues precisa que nuestra legislación especial busca sancionar las conductas cometidas a través de las TICs[22]:

> Art. 1 LDI.- La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia (2013).

Ahora bien, al analizar la tipicidad subjetiva, se aprecia que este delito no admite figuras culposas, es decir, solo puede ser cometido **dolosamente**. Además, se precisa que se debe actuar **deliberadamente** –elemento que se encuentra enlazado con el fuero interno del agresor–. De esta manera, la redacción descartaría no sólo las conductas culposas sino también las que se ejecuten con dolo eventual. Considero que es un desacierto que generará problemas de aplicación.

Se debe recordar que los términos 'deliberada' e 'ilegítimamente' se incluyeron en la modificación de la LDI –adhesión sugerida en los proyectos de ley 2991/2013-CR y 2999/2013-CR-, pues, según los proponentes, nuestra legislación no cumplía con los estándares previstos en el Convenio de Budapest. No obstante, si revisamos el párrafo 39 del Informe Explicativo del citado instrumento, veremos que se sugirió que la conducta sea deliberada, entendiéndola como dolosa –y no para precisar qué grado de conocimiento deben exigir los Estados, como cierto sector de la doctrina nacional interpreta[23]–:

> Todos los delitos contenidos en el Convenio deben ser cometidos de manera 'deliberada' para que se aplique la responsabilidad penal. En ciertos casos un elemento deliberado específico forma parte del delito. Por ejemplo, en el artículo 8 que trata del delito de fraude informático, la intención de obtener un beneficio económico es un elemento constitutivo del delito. Quienes redactaron el Convenio llegaron al acuerdo de que el significado exacto del término "deliberado" debería ser interpretado conforme a las leyes de cada país (Vega Aguilar, J., & Arévalo Minchola, M., 2022, p. 264).

Es más, si revisamos la legislación de los países latinoamericanos que se adhirieron al Convenio

21 Véase a Gómez Vieites (2014, p. 68).

22 Al analizar doctrina española, encuentro que cierto sector considera que la medida de seguridad vulnerada puede ser tanto lógica como física. Sin embargo, considero que se arriba a esta conclusión, porque el delito se ubica en el CP y no una norma especial, en un capítulo que protege la intimidad y no la confidencialidad informática, y, finalmente, porque adolecen de una norma que delimite el ámbito de protección –como el art. 1 LDI–. En esa línea, Hernández Díaz, L. menciona:

> No obstante, como ya hemos mencionado, a pesar de que lo característico del *hacking* es el acceso a los sistemas de información, o parte de los mismos, neutralizando las medidas de seguridad mediante conductas telemáticas, nos encontramos ante un delito de medios indeterminados y, por tanto, la descripción típica no excluye la sanción de conductas de acceso de carácter puramente fisico. Así, cabría, por ejemplo, sancionar a quien accede a un ordenador guardado por su legítimo propietario dentro de un cajón cerrado con llave, aunque tras forzar el cajón solo tenga que encender el dispositivo para así acceder a este sistema de información (2019, p. 281).

23 Vega Aguilar, J., & Arévalo Minchola, M. han dicho: "consideramos que la introducción del término 'deliberadamente' ha venido a complementar el aspecto subjetivo, dotando con claridad la exigencia de presentación de dolo directo para la comisión del referido delito" (2022, p. 264).

de Budapest, veremos que ninguno ha incluido los términos 'deliberada' e 'ilegítimamente' en su redacción.

De otro lado, considero que no podemos ignorar que la conducta además de ser dolosa debe ser deliberada[24]; sin embargo, nuestra interpretación ha de maximizar sus alcances para no mermar la lucha contra la ciberdelincuencia. De esta forma, sugiero que la única conducta excluida debe ser aquella perpetrada con dolo eventual, admitiendo tanto el dolo directo o de primer grado como el dolo de consecuencias necesarias o de segundo grado[25]. Una eventual reforma legislativa debería eliminar este término de su configuración.

Finalmente, la antijuricidad se ve reforzada con el elemento **ilegítimamente**, ya que se sancionan únicamente las conductas que no tienen una causa de justificación. Al igual que con la expresión deliberada, considero que su inclusión es innecesaria. El párrafo 38 del Informe Explicativo del Convenio precisa por qué se sugirió su inclusión en el derecho interno:

> Una particularidad de los delitos incluidos es el requisito expreso de que la conducta en cuestión sea llevada a cabo de manera 'ilegítima'. Esto refleja la idea de que la conducta descrita no siempre es punible per se, sino que puede ser legal o justificada, no sólo en aquellos casos en que corresponde aplicar una defensa legal clásica, como el consentimiento, la defensa propia o la necesidad, sino también cuando otros principios o intereses conducen a la exclusión de la responsabilidad penal. El término 'ilegítimo' deriva su significado del contexto en que está utilizado. Así, sin restringir la manera en que las Partes pueden aplicar el concepto en su derecho interno, puede referirse a una conducta realizada sin facultades para hacerlo (ya sean de orden legislativo, ejecutivo, administrativo, judicial, contractual o consensual) o a una conducta que no está de otro modo comprendida dentro de las justificaciones, excusas y defensas legales establecidas o los principios pertinentes con arreglo a las leyes nacionales (2003, p. 5).

Al igual que en el caso anterior, este término debería suprimirse en una futura modificación legislativa.

d. Segunda modalidad de acceso ilícito

El segundo párrafo del art. 2 prevé la modalidad conocida como abuso de confianza, prevista también en la legislación de Argentina, Chile, Colombia y República Dominicana. El **sujeto activo** del segundo párrafo del delito de acceso ilícito también es uno común, no especial.

De la misma manera, nos encontramos frente a una **conducta dolosa**; sin embargo, a diferencia del primer párrafo, no se exige que la actuación sea deliberada. En consecuencia, sin mayor razón que justifique el trato diferenciado, se sanciona tanto el dolo de primer y segundo grado, como el dolo eventual.

En este caso, el sujeto activo no vulnera las medidas de seguridad establecidas para impedir el acceso, pues ingresa con la autorización conferida por el usuario. Así, este ilícito se configura cuando **excede la autorización brindada**, es decir, realiza acciones que no fueron acordadas previamente. Por ejemplo, si llevo mi laptop al servicio técnico por alguna falla específica y proporciono las claves de acceso para que realicen las pruebas correspondientes, el técnico cometerá este delito si, por ejemplo, accede a mis correos electrónicos o archivos personales, pues la autorización conferida no incluye tales permisos.

e. Circunstancias agravantes.

Le son aplicables las cuatro circunstancias previstas en el artículo 11 de la Ley 30096: (i) Cometer el delito como integrante de una organización criminal; (ii) Cometer el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función; (iii) Cometer el delito con la finalidad de obtener un beneficio económico; y (iv) Comprometer fines asistenciales, la defensa, la seguridad y la soberanía nacionales.

---

[24] Al respecto, Peña Cabrera Freyre, A. señala:

> La expresión 'deliberadamente' en el tipo subjetivo del injusto es una valla que el legislador no debió colocar. El dolo es consciencia y voluntad de la realización típica, de manera que -a nuestro entender- basta que el agente sepa con rayana exactitud que está invadiendo una base de datos ajena para dar por confirmado el tipo penal [...] Al constituir un elemento subjetivo del injusto ajeno al dolo, debe graficar algo distinto a este último, situación que no apreciamos en el tipo penal, pues dicho elemento no dice nada distinto al dolo, por lo que lo único que va a generar es problemas interpretativos, ya que algunos pretenderán argumentar que la intención no fue intencional. En una propuesta de lege ferenda este elemento debe ser excluido de la composición típica en cuestión (2015, p. 161).

En la misma línea, véase a Pérez López, J. (2019, p. 112).

[25] Para Oré Sosa, E. (2022, p. 193) y Vega Aguilar, J., & Arévalo Minchola, M. (2022, p. 263), el término 'deliberado' circunscribe el castigo únicamente a conductas cometidas con dolo directo o de primer grado.

f. Propuesta normativa.

A partir del análisis previamente realizado, propongo modificar el delito de acceso ilícito, eliminando los elementos 'deliberada' e 'ilegítimamente', incluyendo un elemento subjetivo trascendente –como recoge el ordenamiento chileno– y precisando el alcance del acceso ilícito, generado por el quebrantamiento del abuso de confianza –siguiendo la fórmula de Argentina, Colombia, España, y República Dominicana–:

> Art. 2.- Acceso ilícito
>
> El que accede a todo o parte de un sistema informático, con la finalidad de obtener datos informáticos u otra intención delictiva, mediante la vulneración de las medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.
>
> Será reprimido con la misma pena, el que, con la finalidad de obtener datos informáticos u otra intención delictiva:
>
> 1. Accede a todo o parte de un sistema informático excediendo lo autorizado.
> 2. Se mantiene en un sistema informático contra la voluntad de quien tenga el legítimo derecho a excluirlo.

III. SEGUNDA PARTE. LOS PREJUICIOS EN TORNO A LA COMUNIDAD HACKER PUEDEN AFECTAR LA INVESTIGACIÓN

A. El tratamiento del término *hacker* en los medios de comunicación

Como he indicado desde el inicio de este trabajo, el delito analizado recibe diversas denominaciones: acceso indebido, acceso ilícito, intrusismo informático, *hacking*[26]. Sin embargo, esta última denominación ha ensombrecido la labor de los *hackers* bajo el manto del prejuicio, pues se les equipara con los ciberdelincuentes[27]. Si tomamos el inicio de la pandemia como punto de referencia, veremos que los medios de comunicación peruanos han reportado ataques cometidos por ciberdelincuentes bajo titulares que aluden a *hackers*:

- EE. UU. acusa a *hackers* chinos de intentar robar investigación de vacunas contra el COVID-19[28].
- Del príncipe nigeriano al *hacker* más buscado: la tenebrosa historia de Hushpuppi[29].
- *Bitcoin* - La billetera con $ 690 millones que se disputan *hackers* de todo el mundo[30].
- COVID-19 - Acusan a *hackers* chinos de robar información sobre potencial vacuna de España[31].
- Cuidado: descubren una vulnerabilidad de Windows que permite a los *hackers* tener control total de tu PC[32].
- Cuidado: *hackers* prometen ayudar a vacunarse contra el COVID-19 y roban datos personales[33].
- Cuidado: *hackers* comienzan a estafar con la venta de vacunas falsas contra el COVID-19[34].
- Los tramposos de *Call of Duty: Warzone* son el nuevo objetivo de los *hackers* para distribuir *malware* de forma sencilla[35].
- *Hackers* publican datos de usuarios de más de 500 millones de cuentas de Facebook[36].

26 Véase a Riquert, M. (2017, p. 222).

27 A nivel local, el trato sinonímico de *hacker* con ciberdelincuente lo vemos en Oré Sosa:

> El legislador adelanta las barreras de protección del bien jurídico porque sanciona como delito consumado las conductas de intrusismo sin esperar a que se produzca el último propósito del *hacker* (retiros de dinero de cuentas bancarias, el tráfico de un secreto empresarial o de una información reservada, etc.) (2022, p. 193).

En sentido contrario, Vega Aguilar, J., & Arévalo Minchola, M se refieren al respecto como: "*Hacker:* Experto en informática capaz de entrar en sistemas cuyo acceso es restringido. No necesariamente con malas intenciones" (2022, p. 520).

28 Véase a Equipo Editorial del diario El Comercio (13 de mayo del 2020).

29 Véase a Equipo Editorial del diario El Comercio (07 de julio del 2020).

30 Véase a Equipo Editorial del diario El Comercio (10 de septiembre del 2020).

31 Véase a Equipo Editorial del diario El Comercio (18 de septiembre del 2020).

32 Véase a Equipo Editorial del diario El Comercio (07 de noviembre del 2020).

33 Véase a Equipo Editorial del diario El Comercio (09 de enero del 2021).

34 Véase a Equipo Editorial del diario El Comercio (10 de marzo del 2021).

35 Véase a Equipo Editorial del diario El Comercio (02 de abril del 2021).

36 Véase a Equipo Editorial del diario El Comercio (05 de abril del 2021).

– *Hackers* rusos se infiltraron en emails de fiscales de EE.UU.[37]

– *Poly Network* - Los *hackers* que devolvieron casi la mitad de la millonaria suma que habían robado[38].

– Los *hackers* rusos y el creciente peligro de que interfieran en las elecciones alemanas[39].

– Compras *online*: estos son los tipos de fraudes más utilizados por *hackers*[40].

– EE. UU. ofrece recompensa de 10 millones de dólares por los *hackers* de 'Darkside'[41].

– El grupo de *hackers* 'LAPSUS$' roba credenciales de firmas de código de 'Nvidia' para descargar *malware*[42].

B. Breves reflexiones sobre sesgos y prejuicios

¿Por qué debe preocuparnos esta diferencia? Porque prejuzgamos negativamente un grupo social y porque los operadores jurídicos –policías, fiscales y jueces– deben evitar los sesgos tanto en la investigación criminal como en la valoración probatoria. Así, debemos evitar estigmatizar un colectivo de ciudadanos que cultivan habilidades tecnológicas que, quizás, no comprendemos totalmente. En el Internet User´s Glossary de 1983, la Internet Engineering Task Force definía al *hacker* como "aquella persona que disfruta tener una comprensión profunda del funcionamiento interno de un sistema, computadora o redes". Pese a ello, en el 2014, la Real Academia de la Lengua Española incluyó el término '*hacker*' al diccionario, pero utilizó solo una acepción: 'pirata informático'. Tres años después, reconoció la segunda acepción –que subsiste hasta el día de hoy–: "Persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora".

Llegado a este punto debo diferenciar dos conceptos útiles en la investigación criminal, pues permitirán identificar los errores en los que podrían incurrir las víctimas y los testigos al describir un suceso delictivo: la memoria episódica y la memoria semántica. La primera está relacionada al recuerdo de sucesos y elementos, en un determinado espacio temporal y espacial –por ejemplo, cuando la víctima señala que el 01 de febrero del 2022 ingresó a su cuenta de ahorros y advirtió que sustrajeron S/ 15 mil, está evocando su memoria episódica–. La segunda está relacionada con el significado de la información y del conocimiento, prescindiendo del contexto espaciotemporal –por ejemplo, cuando se define el concepto '*hacker*'–. La profesora italiana Giuliana Mazzoni precisa que en la memoria semántica se encuentran conceptos organizados bajo la denominación de 'esquemas' y 'guiones' o '*scripts*'. Los esquemas se refieren a elementos singulares, mientras que los guiones a eventos sociales:

> Tomemos, por ejemplo, el concepto de 'ladrón'. Cada uno de nosotros tiene en la memoria semántica una representación esquemática del concepto "ladrón" que contiene toda una serie de elementos generales, básicos e indispensables para su comprensión. Estos elementos se refieren a aspectos como "los comportamientos y acciones que hacen de un hombre un ladrón": un ladrón no realiza un trabajo 'honrado', un ladrón roba las cosas de los demás, un ladrón miente cuando se le acusa, etc. Estos elementos son esenciales en la definición de ladrón y se activan siempre que uno piensa en un ladrón. Sin embargo, además de los comportamientos necesarios que ayudan a distinguir entre quienes ladrón y quien no lo es, en el concepto de ladrón se pueden encontrar características y elementos opcionales que pueden activarse o no cuando uno piensa en el concepto abstracto de ladrón. Algunas personas insertan siempre en el esquema conceptual de ladrón otros elementos que deberían ser simplemente opcionales, por ejemplo, el concepto de 'napolitano', o el de 'drogadicto'. Para estas personas, tales elementos forman parte integrante del concepto, están en su esquema como elementos obligatorios y, por tanto, se activan conscientemente, aunque también inconscientemente, en el momento en que piensan en un ladrón [...] (2010, p. 31).

C. Los sesgos y prejuicios pueden afectar la investigación criminal y la toma de decisiones

¿Cuál es la relación de estos conceptos con los *hackers*? Bueno, los ciudadanos (víctimas o testigos)

37 Véase a Equipo Editorial del diario El Comercio (31 de julio del 2021).

38 Véase a Equipo Editorial del diario El Comercio (13 de agosto del 2021).

39 Véase a Equipo Editorial del diario El Comercio (10 de septiembre del 2021).

40 Véase a Equipo Editorial del diario El Comercio (27 de septiembre del 2021)

41 Véase a Equipo Editorial del diario El Comercio (04 de noviembre del 2021).

42 Véase a Equipo Editorial del diario El Comercio (08 de marzo del 2022).

tienen una definición (esquema) o idea del '*hacker*', difundida por las películas, las series, las noticias[43]: es un delincuente, es malo, actúa anónimamente, es joven, tiene conocimientos especializados, utiliza dispositivos o programas sofisticados, busca apropiarse de las cuentas, busca apropiarse del dinero de las personas, etcétera. El lector habrá caído en cuenta hacia donde se dirigen estas líneas: los prejuicios.

> Una forma de prejuicio, por ejemplo, consiste en juzgar a un individuo, sin conocerlo personalmente, basándose en lo que se conoce del grupo al que pertenece o en lo que se ha oído decir. Un estereotipo es un esquema de conocimiento que afecta a un grupo de personas, es decir, un tipo especial de convicción que funciona como un filtro a través del cual se criban las informaciones que uno recibe sobre el mundo o sobre individuos pertenecientes a grupos sociales diferentes del propio (Mazzoni, G., 2010, p. 45).

Así, la víctima o el testigo de un ciberdelito completará aquellos vacíos de su relato con los esquemas mentales que tiene y que, muchas veces, se originan en prejuicios. De esta forma, podría creer que quien accedió a su cuenta en redes sociales o a su correo electrónico o quien sustrajo dinero de su cuenta bancaria es un *hacker* –con las características que inconscientemente le atribuimos–.

De este modo, diferenciar adecuadamente los conceptos evitará adoptar decisiones erróneas durante la investigación criminal y en la decisión judicial. Si se piensa que los ciberdelitos sólo pueden ser cometido por '*hackers*', es decir, por personas con conocimientos altamente especializados, podríamos descartar hipótesis válidas que no calzan en estos supuestos como, por ejemplo, que el evento delictivo haya sido realizado por alguien con escasas habilidades tecnológicas. De la misma forma, al sentenciar, el juzgador podría buscar semejanzas con algún caso que previamente haya decidido. Desarrollaré estos puntos recurriendo a los **heurísticos de representatividad** y de **accesibilidad***,* así como al **sesgo de confirmación**.

Los heurísticos son atajos mentales que permiten adoptar decisiones rápidas, sin tanto esfuerzo. Si bien son útiles, a veces, nos llevan a tomar decisiones erróneas. El **heurístico de representatividad** orienta a las personas a tomar decisiones a partir de lo que ya conocen y les resulta parecido a lo que tienen que decidir[44]. Sobre este punto, Cristian Contreras, sostiene que:

> Llevado al terreno judicial, esto se vincula con que el juez tiende a resolver los asuntos de la misma manera en que lo ha hecho en los casos parecidos que le haya correspondido conocer previamente. Con esto simplifica enormemente su ejercicio intelectual y obtiene su decisión de forma más rápida, ya que confía en que los razonamientos que haya elaborado para casos semejantes son plenamente aplicables para el que ahora le corresponde resolver (2015, p. 112).

De esta forma, si la policía o la fiscalía investigó casos de acceso ilícito que involucraron técnicas especiales o sofisticadas para su perpetración y asociaron esas ideas a la intervención de *hackers*, caerían en este heurístico si, por la similitud de la modalidad, asumen en otros casos que también deben existir *hackers* detrás de los actos ilícitos indagados.

A diferencia del heurístico de representatividad, en el que el eje central es la semejanza, en el **heurístico de accesibilidad**, es la repetición. Así, cuantas más veces se reitera un acontecimiento, más fácil será recordarlo en el futuro. Siguiendo nuevamente a Contreras:

> En el plano judicial, la accesibilidad se manifiesta en que el juez tenderá a estimar más probable aquella hipótesis de los hechos que coincida con situaciones previas que pueda recordar más fácilmente, de modo que este heurístico lo llevará a pensar que en la situación actual ha sucedido lo mismo que en los ejemplos que haya podido recuperar, los que usualmente coincidirán con los casos similares que hayan acontecido en el último tiempo (2015, p. 116).

Este es un heurístico del cual deben cuidarse las unidades especializadas en ciberdelincuencia ya que, precisamente, investigar continuamente el mismo tipo de casos podría orientarlos a tratar nuevas denuncias como aquellos casos que han indagado previa y repetidamente.

Una de las consecuencias que se produce como efecto de este heurístico es el **sesgo de confirmación**, que se origina cuando alguien está tan convencido de un conocimiento, que, aunque, *a posteriori* quede absolutamente desacreditado,

[43] En esta línea, véase al subcapítulo denominado 'Introducción: del hacker cinematográfico al cibercriminal común' de Miró Llinares, F. (2012, pp. 229-231).

[44] Véase a Nieva Fenoll, J. (2010).

tiende a continuar creyendo, pese a ello, en ese conocimiento previo. En el Recurso de Nulidad 760-2020, Lima, del 05 de abril del 2021, la Corte Suprema de Justicia advirtió que los jueces deben evitar este sesgo al juzgar y sentenciar:

> En este caso se seleccionan la información y las pruebas de acuerdo con si corroboran las preconcepciones de quien juzga, en detrimento de las hipótesis contrarias. De este modo, los jueces sólo seleccionan la evidencia que confirme su hipótesis del caso y omiten aquella que sea incompatible con esta decisión. Un ejemplo de este tipo de sesgo se presenta cuando los operadores jurídicos, en el razonamiento de sus decisiones, solo citan y valoran las pruebas de la decisión que adoptaron previamente (evalúan únicamente las pruebas de cargo o únicamente las de descargo, es decir, solo valoran una parte de las pruebas actuadas) y no hacen ningún análisis de las otras pruebas (contrarias a la decisión que previamente adoptaron). Este razonamiento es claramente sesgado e irracional y, por lo tanto, carece de respaldo constitucional, pues también incurre en los vicios de motivación insuficiente y aparente (2021).

Si quien investiga un caso tiene el prejuicio 'el hacker es un ciberdelincuente' y considera que 'los ciberdelitos son cometidos hackers', entonces en las indagaciones podría buscar elementos que corroboren la siguiente hipótesis: 'el responsable de este ciberdelito debe ser un hacker'. De esta forma, sobrevalorará la información que corrobore dicha perspectiva y minimizará u obviará aquella que no lo haga. Entonces, descartará inconscientemente hipótesis igualmente válidas como: pudo ser una persona de confianza que tuvo acceso a sus credenciales de autenticación por negligencia del usuario, pudo ser una persona que no tiene conocimientos avanzados, pero que adquirió los datos de acceso en el mercado negro, pudo ser una persona cercana o que trabaje en la organización (*insiders*), etcétera.

Espero que estas breves reflexiones permitan alejarnos del prejuicio que cubre a la comunidad *hacker* y comprender que esa dicotomía entre *hacker* y ciberdelincuente puede generar problemas en la investigación y en el juzgamiento.

IV. CONCLUSIONES

Hacia mediados del 2000, Perú incorporó el acceso ilícito al CP, empleando una fórmula que exigía un propósito o finalidad delictiva, pero sin requerir la vulneración de medidas de seguridad destinadas a su protección. Esta norma se incluyó en el título de delitos contra el patrimonio, lo que limitó una adecuada interpretación.

En el 2013, se aprobó la LDI, siguiendo, hasta cierto punto, las recomendaciones del Convenio de Budapest, al cual Perú se adhirió seis años después. La regulación actual, permite afirmar que la primera modalidad adoptada reprime el *hacking* blanco, mero intrusismo o acceso ilícito sin ulterior propósito. Sin mayor discusión, a inicios del 2014, este delito se modificó para precisar que la conducta debe ser 'deliberada' e 'ilegítima'. En este artículo se explicó por qué el término deliberadamente genera problemas de aplicación y excluye, por lo menos, las conductas cometidas con dolo eventual. Además, se indicó que el término 'ilegítimamente' hace referencia a la antijuricidad, deviniendo en innecesaria su inclusión. La segunda modalidad recoge el abuso de confianza y, a diferencia de la primera, no exige que la conducta sea deliberada o ilegítima ni que se realice mediante el quebrantamiento de medidas de seguridad.

En este artículo se explicó que no se debe equiparar a los *hackers* con los ciberdelincuentes, pues, de un lado, se estigmatiza a una comunidad que surge para desafiar los límites de la tecnología y, de otro lado, porque puede generar sesgos en el investigador y, también, en quien toma las decisiones judiciales.

REFERENCIAS

Arévalo Minchola, M., & Vega Aguilar, J.A. (2022). *Ciberdelitos: Análisis en el Sistema Penal*. Editorial Iustitia.

Comité de Ministros del Consejo de Europa (2001) *Informe Explicativo del Convenio sobre la Ciberdelincuencia*. https://rm.coe.int/16802fa403

Contreras Rojas, C. (2015). *La valoración de la prueba de interrogatorio*. Marcial Pons.

Durand Valladares, R. (2002). Los delitos informáticos en el Código penal peruano. *Revista Peruana de Ciencias Penales,* (11).

Elías Puelles, R. (2017). Luces y sombras en la lucha contra la delincuencia informática en Perú. En D. Dupuy & M. Kiefer (coords.). *Cibercrimen. Aspectos de Derecho penal y procesal penal. Cooperación Internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de Internet*. Editorial B de F.

Equipo Editorial del diario El Comercio. (13 de mayo de 2020). EE.UU. acusa a hackers chinos de intentar robar investigación de vacuna contra el COVID-19. *El Comercio.* https://elco-

mercio.pe/tecnologia/actualidad/coronavirus-covid-19-hackers-china-eeuu-acusa-a-hackers-chinos-de-intentar-robar-investigacion-de-vacuna-contra-el-covid-19-noticia/

Equipo Editorial del diario El Comercio. (07 de julio de 2020). Del príncipe nigeriano al hacker más buscado: la tenebrosa historia de Hushpuppi. *El Comercio.* https://elcomercio.pe/mundo/actualidad/instagram-del-principe-nigeriano-al-hacker-mas-buscado-la-historia-de-hushpuppi-phishing-ciberdelincuentes-noticia/

Equipo Editorial del diario El Comercio. (10 de setiembre del 2020). Bitcoin | La billetera con US$690 millones que se disputan hackers de todo el mundo. *El Comercio.* https://elcomercio.pe/tecnologia/tecnologia/bitcoin-la-billetera-con-us690-millones-que-se-disputan-hackers-de-todo-el-mundo-noticia/

Equipo Editorial del diario El Comercio. (18 de setiembre del 2020). COVID-19 | Acusan a hackers chinos de robar información sobre potencial vacuna de España. *El Comercio.* https://elcomercio.pe/tecnologia/ciencias/covid-19-acusan-a-hackers-chinos-de-robar-informacion-sobre-potencial-vacuna-en-espana-noticia/

Equipo Editorial del diario El Comercio. (07 de noviembre del 2020). Cuidado: descubren una vulnerabilidad de Windows que permite a los hackers tener control total de tu PC. *El Comercio.* https://elcomercio.pe/tecnologia/ciencias/cuidado-descubren-una-vulnerabilidad-en-windows-que-permite-a-los-hackers-tener-control-total-de-tu-pc-noticia/

Equipo Editorial del diario El Comercio. (09 de enero del 2021). Cuidado: hackers prometen ayudar a vacunarse contra el COVID-19 y roban datos personales. *El Comercio.* https://elcomercio.pe/tecnologia/actualidad/cuidado-hackers-prometen-ayudar-a-vacunarse-contra-el-covid-19-y-roban-datos-personales-noticia/

Equipo Editorial del diario El Comercio. (10 de marzo del 2021). Cuidado: hackers comienzan a estafar con la venta de vacunas falsas contra el COVID 19. *El Comercio.* https://elcomercio.pe/tecnologia/actualidad/cuidado-hackers-prometen-ayudar-a-vacunarse-contra-el-covid-19-y-roban-datos-personales-noticia/

Equipo Editorial del diario El Comercio. (02 de abril del 2021). Los tramposos de Call of Duty: Warzone son el nuevo objetivo de los hackers para distribuir malware de forma sencilla. *El Comercio.* https://elcomercio.pe/tecnologia/e-sports/los-tramposos-de-call-of-duty-warzone-son-el-nuevo-objetivo-de-los-hackers-para-distribuir-malware-de-forma-sencilla-noticia/

Equipo Editorial del diario El Comercio. (05 de abril del 2021). Hackers publican datos de usuarios de más de 500 millones de cuentas de Facebook. *El Comercio.* https://elcomercio.pe/mundo/actualidad/facebook-hackers-publican-datos-de-usuarios-de-mas-de-500-millones-de-cuentas-una-red-social-business-insider-noticia/

Equipo Editorial del diario El Comercio. (31 de julio del 2021). Hackers rusos se infiltraron en emails de fiscales de EE.UU. *El Comercio.* https://elcomercio.pe/mundo/eeuu/estados-unidos-hackers-rusos-se-infiltraron-en-emails-de-fiscales-de-eeuu-rusia-solarwinds-noticia/

Equipo Editorial del diario El Comercio. (13 de agosto del 2021). Poly Network | Los hackers que devolvieron casi la mitad de la millonaria suma que habían robado. *El Comercio.* https://elcomercio.pe/tecnologia/tecnologia/poly-network-los-hackers-que-devolvieron-casi-la-mitad-de-la-millonaria-suma-que-habian-robado-noticia/

Equipo Editorial del diario El Comercio. (10 de septiembre del 2021). Los hackers rusos y el creciente peligro de que interfieran en las elecciones alemanas. *El Comercio.* https://elcomercio.pe/tecnologia/tecnologia/poly-network-los-hackers-que-devolvieron-casi-la-mitad-de-la-millonaria-suma-que-habian-robado-noticia/

Equipo Editorial del diario El Comercio. (27 de septiembre del 2021). Compras online: estos son los tipos de fraude más utilizados por hackers. *El Comercio.* https://elcomercio.pe/casa-y-mas/mantenimiento/ciberdelincuencia-compras-online-estos-son-los-tipos-de-fraude-mas-utilizados-por-hackers-nndc-noticia/

Equipo Editorial del diario El Comercio. (04 de noviembre del 2021). EE.UU. ofrece recompensa de 10 millones de dólares por los hackers de DarkSide. *El Comercio.* https://elcomercio.pe/mundo/eeuu/estados-unidos-ofrece-recompensa-de-usd-10-millones-por-los-hackers-de-darkside-noticia/?ref=ecr

Equipo Editorial del diario El Comercio. (08 de marzo del 2022). El grupo de hackers LAPSUS$ roba credenciales de firmas de código de Nvidia para descargar 'malware'. *El Comercio.* https://elcomercio.pe/tecnologia/actualidad/nvidia-

el-grupo-de-hackers-lapsus-roba-credenciales-de-firmas-de-codigo-de-nvidia-para-descargar-malware-rmmn-noticia/?ref=ecr,

Espinoza Calderón, V. (2022). *Delitos informáticos y nuevas modalidades delictivas*. Instituto Pacífico.

Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (R.D. 2010, 3) (España).

Gómez Vieites, A. (2014). *Enciclopedia de la Seguridad Informática*.

Hernández Díaz, L. (2019). *Los accesos ilícitos a sistemas informáticos. Normativa internacional y regulación en el ordenamiento penal español*. Thomson Reuters Aranzadi.

Malkin, G. (1983). *Internet User's Glossary*. https://www.rfc-editor.org/rfc/rfc1983

Mazzoni, G. (2010). *¿Se puede creer a un testigo? El testimonio y las trampas de la memoria*. Editorial Trotta.

Ministerio de Justicia y Derechos Humanos (2022). *Ciberdelincuencia. Reporte de información estadística y recomendaciones para la prevención*. https://cdn.www.gob.pe/uploads/document/file/3562747/Reporte%20de%20Ciberdelincuencia.pdf.pdf

Miró Llinares, F. (2012). *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio*. Marcial Pons.

Nieva Fenoll, J. (2010). *La valoración de la prueba*. Marcial Pons.

Oré Sosa, E. (2022). *Delictum. Apuntes de Derecho Penal*. Editores del Centro.

Palomino Ramírez, W. (2014). El intrusismo y los otros delitos informáticos regulados en la Ley Nº 30096. *Gaceta Penal & Procesal Penal,* (56).

Peña Cabrera Freyre, A. (2015). Los delitos informáticos: el uso de instrumentos digitales en las redes informáticas y en el ciberespacio. *Gaceta Penal & Procesal Penal*, (76).

Pérez López, J. (2019). *Delitos regulados en leyes penales especiales*. Gaceta Jurídica.

Resolución Legislativa 30913 del Congreso de la República, Resolución Legislativa que aprueba el Convenio sobre la Ciberdelincuencia, Diario Oficial El Peruano, 13 de febrero de 2019.

Riquert, M. (2017). El acceso ilegítimo a sistema o dato informático (art. 153 bis del Código Penal). En D. Dupuy & M. Kiefer (coords.). *Cibercrimen. Aspectos de Derecho penal y procesal penal. Cooperación Internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de Internet*. Editorial B de F.

Rueda Martín, M. (2009). Cuestiones político-criminales sobre las conductas de hacking. *Revista Internacional Derecho Penal Contemporáneo*, (28).

Sáenz Delgado, E. (2021). Delincuencia cibernética y descubrimiento y revelación de secretos. En E. Sáenz Delgado, & D. Fernández Bermejo (coords.). *Tratado de Delincuencia Cibernética*. Thomson Reuteres Arazandi.

Velasco San Martín, C., & Sanchís, C. (2019). *Delincuencia informática. Tipos delictivos e investigación. Con jurisprudencia tras la reforma procesal y penal del 2015*. Tirant Lo Blanch.

Villavicencio Terrero, F. (2014). Delitos informáticos. *Ius et Veritas,* (49).

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

Código Penal [CP], Decreto Legislativo 635, Diario Oficial *El Peruano*, 08 de abril de 1991 (Perú).

Decreto Ley 2848/40 [C. P.] de 7 de dezembro de 1940, Diário Oficial da União [D.O.U.] (Brasil).

Código Penal, Ley 14, Gaceta Oficial Digital, 18 de mayo de 2007 (Panamá).

Ley 599 [C. Pen.], 24 de julio de 2000, Diario Oficial [D.O.] (Colombia).

Código Penal, Ley 1160, Gaceta Oficial, 26 de noviembre de 1997 (Paraguay).

Código Penal, Ley 4573, La Gaceta, 15 de noviembre de 1970 (Costa Rica).

Ley 11179 [Cód. Pen.], 03 de noviembre de 1921, Boletín Nacional (Argentina).

Ley Orgánica 10/1995 [CP], BOE 281, 24 de noviembre de 1995 (España).

Convenio sobre la Ciberdelincuencia, 23 de noviembre de 2001.

Decreto Supremo 010-2019-RE, Ratifican el Convenio sobre la Ciberdelincuencia, Diario Oficial *El Peruano*, 10 de marzo de 2019 (Perú).

Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología, 09 de mayo de 2007 (República Dominicana).

Ley 30096, Ley de Delitos Informáticos, Diario Oficial *El Peruano*, 22 de octubre de 2013 (Perú).

Ley 21459, Ley que establece normas sobre delitos informáticos, deroga la Ley 19223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest, 09 de junio de 2022 (Chile).

Proyecto de Ley 5071/99-CR, Proyecto de Ley de Delitos Informáticos, presentado el 18 de agosto de 1999 (Perú).

Proyecto de Ley 5132/99-CR, Propone establecer como figura típica penal los delitos informáticos, presentado el 31 de agosto de 1999 (Perú).

Proyecto de Ley 34/2011-CR, Proyecto de Ley que regula los Delitos Informáticos, presentado el 11 de agosto de 2011 (Perú).

Proyecto de Ley 2520/2012-PE, Proyecto de Ley de Represión de la Cibercriminalidad, presentado el 26 de julio de 2013 (Perú).

Proyecto de Ley 2991/2013-CR, Proyecto de Ley que modifica la Ley 30096, Ley de Delitos Informáticos, presentado el 25 de noviembre de 2013 (Perú).

Proyecto de Ley 2999/2013-CR. Proyecto de Ley que modifica, incorpora y deroga diversos artículos a la Ley 30096, Ley de Delitos Informáticos, presentado el 27 de noviembre de 2013 (Perú).

Resolución de la Fiscalía de la Nación 1503-2020-MP-FN, Crean la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público con competencia nacional y designan y nombran Fiscales en el Distrito Fiscal de Lima, Diario Oficial *El Peruano*, 30 de diciembre del 2020.