Análisis de la tipificación del artículo 153 bis del Código Penal Argentino

Gastón A. Bruno

Universidad de Palermo

Author Note

Email Address: gaston@gastonbruno.com.ar

Abstract

El artículo 153 bis del Código Penal Argentino tipifica el acceso indebido dentro del campo de la tecnología informática, en donde este verbo puede tomar varias interpretaciones en este sentido. Como consecuencia de esto, ciertos actos podrían ser penados indebidamente. *Este trabajo analiza la acción en la que se basa la ley dentro del contexto de la tecnología informática, planteando la problemática y proponiendo una redacción distinta para subsanar la situación desarrollada.*

Índice de contenidos

Alcance

Este trabajo se enfoca particularmente en analizar el verbo interviniente en la tipificación del artículo 153 bis del Código Penal Argentino. Si bien emplea definiciones actuales de *delito informático*, no pretende evaluarlas; simplemente emplear ese marco de significados literales actuales con el objetivo de demarcar un contexto en el cual se desarrolle la exposición de este análisis. Asimismo, no se cuestionan las diversas opiniones que conforman el marco teórico.

Tampoco se analizan las distintas partes que componen el artículo 153 bis, que resultan interesantes bajo otro análisis en cuanto a si son aplicables y/o tienen razón de ser. Estas partes contemplan los aspectos de tomar acciones *a sabiendas* (como menciona textualmente), la cuestión del dolo o la culpa, el *sistema o el dato informático* (como menciona textualmente), el alcance de *cualquier* medio (como menciona textualmente), etc.

En cuanto a los terrenos del derecho y de la informática, se evita desarrollar sus explicaciones elementales, empleando de manera sucinta los fundamentos relevantes que conforman el sustento de la exposición.

La ley 26.388 de delitos informáticos se ha sancionado el 4 de junio de 2008 con todos los 172 votos a su favor (Users Staff, 2011). Esta ley contempla modificaciones del Código Penal Argentino con el objetivo de incluir los delitos informáticos y sus respectivas penas. No solo incorpora artículos, sino que también modifica y deroga otros (InfoLEG, 2013).

En particular, este trabajo se enfocará en el artículo 5° de esta ley, que incorpora como artículo 153 bis, el siguiente:

> *"Artículo 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."*

Delito informático

La temática central de la ley 26.388 se desarrolla en base a los delitos dentro del área informática. Esto produce que se encuentre la necesidad de convergencia entre dos mundos distintos en cuanto al ámbito legal y el tecnológico. Las características intrínsecas de estos dos terrenos que los caracterizan de forma tan lejana hacen bastante difícil llegar a un establecimiento claro en cuanto a la definición, e incluso la existencia o razón de ser, de un delito informático.

Antes de adentrarse en las distintas posiciones que puedan haber, se exponen las definiciones de ambas palabras en su significado genuino para el lenguaje español, de modo de establecer un marco contextual, al menos lingüístico. Para la Real Academia Española, un delito tiene los siguientes significados:

> *"1. m. Culpa, quebrantamiento de la ley.*
>
> *2. m. Acción o cosa reprobable.*
>
> *3. m. Der. Acción u omisión voluntaria o imprudente penada por la ley." (Real Academia Española, 2013)*

Mientras que la palabra "informático" se refiere a lo relativo a la informática, cuya definición es:

> *"1. f. Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras." (Real Academia Española, 2013)*

Por lo tanto, una interpretación basada en el diccionario de un "delito informático" consiste en: "*Acción u omisión voluntaria o imprudente penada por la ley, perteneciente o relativa al conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras"*.

Más allá del significado literal, Juan Domingo González resalta la existencia de distintas acepciones en este sentido de personas relacionadas al derecho y de organizaciones internacionales (Gonzalez, 2011).

Para la doctora Silvina Laura Rinaldi se puede prescindir de la existencia particular del delito informático, pudiendo englobar cualquier actividad en este sentido bajos los tipos penales tradicionales, que emplean como medio las herramientas informáticas (Rinaldi, 2001):

> *"Estamos en presencia de delitos clásicos en los que su naturaleza no varía en gran medida por el hecho de que para su perpetración se haga uso de moderna tecnología relacionada con la computación. Por lo tanto no puede hablarse de delito informático sino más bien de una categoría criminológica como delincuencia o criminalidad informática dentro de la cual se agruparán los problemas del procesamiento de datos, relevantes para el derecho penal sin modificar los tipos penales y las conductas a ellos vinculadas. La gran mayoría de los ilícitos informáticos pueden encuadrarse en los tipos penales tradicionales, en la medida en que sistemas computarizados sean utilizados como medio, instrumento, herramienta u objeto de aquellos."*

Carlos Sueiro está más cerca a compartir la posición de Rinaldi en cuanto a que sostiene en su análisis de la ley 26.388 lo siguiente:

> "con la instrumentación de una ley de reforma integral, armónica y concordada con el Código Penal de la Nación, no se crearon nuevas figuras delictivas o tipos penales, sino que se modificaron ciertos aspectos de los tipos penales ya contemplados por nuestro ordenamiento jurídico, con el objeto de receptar y captar las nuevas tecnologías como medios comisivos para su ejecución. De esta manera,

> se afirma que la tecnología de la informática y de las comunicaciones sólo constituyen nuevos medios comisivos para realizar las acciones o conductas ya descriptas por los tipos penales previstos por nuestro Código Penal de la Nación, sin dar lugar por el momento a nuevas ontologías o conductas que deban ser receptadas por nuestro ordenamiento jurídico.” *(Sueiro, 2011)*

En esta misma línea, Marcelo Riquert resalta el hecho de no conformar un nuevo tipo penal como una ventaja, recordando la intervención del diputado Nemirovsci en el debate parlamentario de la ley, destacando que no se estaba *“sancionando una ley de delitos informáticos que crea nuevas figuras penales. Simplemente estamos adaptando los tipos penales a nuevas modalidades delictivas, que encuentran a la informática como medio de acción típica.”* (Riquert, 2009)

Sin embargo, existen diversas opiniones que contrariamente, sustentan la justificación de la existencia del delito informático. En línea con esto, el doctor Julio Télles Valdez conceptualiza al delito informático en forma típica y atípica, entendiendo a la primera como a *"las conductas típicas, antijurídicas y culpables, en las que se tienen a las computadoras como instrumento o fin"* y a las segundas *"actitudes ilícitas en que se tienen a las computadoras como instrumento o fin"* (Télles Valdez, 2000). Asimismo, Télles Valdez también sostiene lo siguiente:

> “no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no han sido objeto de tipificación aún." *(Télles Valdez, 1996)*

Para el Doctor Gabriel A. Cámpoli, los delitos informáticos representan acciones no triviales, en el sentido de que requieren de un conocimiento específico para llevarlos a cabo:

> *"El campo de los delitos informáticos aparece hoy ante el legislador como un mundo que puede decirse no al alcance de la mayoría, y más aún si nos adentramos específicamente en el punto de los delitos electrónicos ya que su aprehensión implica un mayor grado de compromiso con conocimientos tecnológicos que a la postre resultan sólo para algunos elegidos." (Cámpoli, 2001)*

La abogada especializada en derecho penal Hemilce Fissore sostiene que *"el delito informático implica cualquier actividad ilícita que encuadra en figuras tradicionales ya conocidas como: robo, hurto, fraude, estafa, sabotaje, etc.; pero siempre involucrando a la informática como medio para cometer el ilícito"*, sin embargo basándose en que:

> *"Las tecnologías de la información y las comunicaciones están cambiando las sociedades en todo el mundo al mejorar la productividad en las industrias tradicionales, revolucionar los procesos laborales y modificar la velocidad y el flujo de capitales. Sin embargo, este crecimiento rápido también ha desencadenado nuevas formas de delincuencia informática", concluye en que "ante nuevas conductas socialmente reprochables, se requiere indefectiblemente nuevos tipos penales que anticipen su sanción. Tanto en el ámbito internacional como nacional la actualización de las normas en la materia ya hace varios años se ha puesto en marcha, el gran desafío será entonces igualar o al menos aproximarse a los tiempos de evolución y desarrollo con qué vorazmente se nos presenta en nuestros días la tecnología." (Fissore)*

Por otro lado, Gustavo A. Arocena define al delito informático de la siguiente manera:

> *"El delito informático o ciberdelito es el injusto determinado en sus elementos por el tipo de la ley penal, conminado con pena y por el que el autor merece un reproche de culpabilidad, que, utilizando a los sistemas informáticos como medio comisivo o teniendo a aquéllos, en parte o en todo, como su objeto, se vinculan en el tratamiento automático de datos." (Arocena)*

En cuanto a La Organización de Naciones Unidas, se reconocen los siguientes tipos de delitos informáticos (Seguinfo, 2013):

Fraudes cometidos mediante manipulación de computadoras

- Manipulación de los datos de entrada: este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir.
- La manipulación de programas: consiste en modificar los programas existentes en el sistema o en insertar nuevos programas o rutinas. Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente tiene conocimientos técnicos concretos de informática y programación.
- Manipulación de los datos de salida: se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude del que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos.
- Fraude efectuado por manipulación informática: aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una

cuenta y se transfieren a otra. Se basa en el principio de que 10,66 es igual a 10,65 pasando 0,01 centavos a la cuenta del ladrón n veces.

Manipulación de los datos de entrada

- Como objeto: cuando se alteran datos de los documentos almacenados en forma computarizada.
- Como instrumento: las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial.

Daños o modificaciones de programas o datos computarizados

- Sabotaje informático: es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.
- Acceso no autorizado a servicios y sistemas informáticos: estos accesos se pueden realizar por diversos motivos, desde la simple curiosidad hasta el sabotaje o espionaje informático.
- Reproducción no autorizada de programas informáticos de protección legal: ésta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, se considera, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

Adicionalmente a estos tipos de delitos reconocidos, el XV Congreso Internacional de Derecho ha propuesto todas las formas de conductas lesivas de la que puede ser objeto la información. Ellas son:

- Fraude en el campo de la informática.
- Falsificación en materia informática.
- Sabotaje informático y daños a datos computarizados o programas informáticos.
- Acceso no autorizado.
- Intercepción sin autorización.
- Reproducción no autorizada de un programa informático protegido.
- Espionaje informático.
- Uso no autorizado de una computadora.
- Tráfico de claves informáticas obtenidas por medio ilícito.
- Distribución de virus o programas delictivos.

En cuanto a la Organización para la Cooperación y el Desarrollo Económicos, un delito informático es

> *"cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos. Los delitos informáticos se realizan necesariamente con la ayuda de los sistemas informáticos, pero tienen como objeto del injusto la información en sí misma".*

Por último se expresa la definición más divulgada en el ámbito de varios trabajos realizados en este sentido, que afirman la existencia del delito informático y lo definen como "*Cualquier actividad ilegal que encuadra en figuras tradicionales ya conocidas como robo, hurto, fraude,*

falsificación, perjuicio, estafa y sabotaje, pero siempre que involucre la informática de por medio para cometer la ilegalidad”.

La importancia del verbo acceder en el artículo 153 bis

Si bien y como se ha desarrollado anteriormente, el delito informático puede contemplar diversas actividades bajo ciertas condiciones; en su forma más elemental, comprende una acción determinada. Dicha acción debe presentar una interpretación clara y unívoca bajo una norma penal, para que ésta comprenda un acto delictivo.

Tipificación del “acceso a un sistema o dato informático”

Una ley puede contemplar una determinada acción con el objeto de determinar si dicho acto va contra ella o no. Adicionalmente, para que ésta pueda ser castigada en el caso de que esa acción sea efectivamente ilícita, la ley debe además establecer una pena para dicho actuar. En esto consiste la tipificación de un determinado accionar dentro del marco de la doctrina penal (Gonzalez, 2011).

En particular, para el artículo 153 bis dentro del marco de la ley 23.388, la acción contemplada consiste en el *acceso* a sabiendas por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido. En cuanto a la pena, se contemplan dos distintas. Por un lado, si dicho 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, la pena es de un (1) mes a un (1) año de prisión. En caso contrario, la pena se reduce a prisión de quince (15) días a seis (6) meses. Cabe destacar, que para ambos casos la pena, cualquiera sea, queda sujeta a si esta acción no resultare un delito más severamente penado.

Definidos estos dos aspectos, queda tipificado en un sentido amplio, el acto de acceder a un sistema o dato informático, mientras que se cumplan las condiciones de que este acto sea a sabiendas, por cualquier medio y sin la debida autorización o excediendo la que se posea.

Problemática en la interpretación del verbo tipificado

Bajo la redacción actual del artículo 153 bis del Código Penal Argentino, la acción basada en el verbo acceder, resulta poco conveniente en términos de poder definir claramente cuándo una acción queda comprendida dentro de un ilícito que debe ser penado y cuándo no. Esto representa un grave problema en cuanto a que permite que esta falta de definición concreta, de lugar a distintas posturas en relación a posibles hechos concretos. Además, una acción tipificada que no contemple claridad y exactitud en su interpretación no se condice con los fundamentos de un artículo penal, que debe comprender una determinada acción de forma específica. Todo esto resulta de gran importancia, siendo que una mala interpretación en este sentido, no solamente conlleva a definir la legitimidad de un accionar, sino que además; al estar penado puede resultar en consecuencias de privación de la libertad.

El decir que el *acceder* no denota claridad en cuanto a su ámbito de acción, se fundamenta bajo las características del verbo empleado y la tecnología informática. Bajo este contexto, *acceder* a un sistema o dato informático puede ser interpretado de formas distintas, ya que en definitiva; la definición el verbo acceder ha tenido origen bajo un contexto físico, mientras que en el campo de la informática se requiere contemplar un ámbito virtual. Desde la concepción de estos dos mundos, existe una diferencia fundamental entre lo que respecta a lo físico y a lo virtual. Éste es un ejemplo más de situaciones que resaltan las dificultades del derecho al emplear los recursos formales de la ley para aplicarlos a ciertos ámbitos que requieren de una forma totalmente nueva y distinta de pensar las cosas; resultando en incompatibilidades, ambigüedades y consecuencias distintas a lo que se esperaba al momento de desarrollar un marco legal para una determinada situación.

Resulta importante aclarar que la importancia en cuanto a la diferencia entre lo físico y lo virtual que aquí se plantea, no tiene como objeto entrar en la discusión de la vigencia o no de un

acto; en cuanto a si éste debe ser regulado bajo el criterio territorial de la ley penal, siendo que las acciones informáticas se dan en el ciberespacio quedan por fuera de la jurisdicción de cualquier Estado.

Bajo la premisa de que la informática propone *nuevas formas de hacer las cosas*, se requiere entonces además *nuevas formas de definir dichas cosas*. Sin embargo, hasta ahora la definición contempla palabras que no son nuevas. Bajo un análisis formal y taxativo, el verbo "acceder" contiene cuatro distintas definiciones:

> *"1. intr. Consentir en lo que alguien solicita o quiere.*
>
> *2. intr. Ceder en el propio parecer, conviniendo con un dictamen o una idea de otro, o asociándose a un acuerdo.*
>
> *3. intr. Entrar en un lugar o pasar a él.*
>
> *4. intr. Tener acceso a una situación, condición o grado superiores, llegar a alcanzarlos." (Real Academia Española, 2013)*

A los efectos de lo que concierne al ámbito que se está desarrollando, se establece como definición formal de la palabra "acceder" a la acción de *entrar en un lugar o pasar a él*. Ésta sustenta una interpretación dentro de un contexto físico, distinto al de la tecnología informática.

Se sostiene que el ámbito informático se da dentro de un contexto virtual, siendo que si bien los elementos que permiten su funcionamiento son físicos, los resultados que el usuario busca; están representados dentro un contexto que solamente existe bajo la interpretación que el usuario y las máquinas le brindan, no consistiendo en una cosa tangible.

Marcelo Temperini también expone este problema en su análisis del artículo 153 bis., planteando un ejemplo en el cual una persona realiza un escaneo de puertos en una red, consiguiendo variada información de los sistemas interconectados. Para Temperini no existe

acceso allí, ya que sostiene que *"para que exista acceso a los fines de este tipo penal, el sujeto debería tener la posibilidad real de poder disponer de la información accedida indebidamente."* (Temperini)

Conclusiones

En primer lugar, se quiere dejar en claro que este trabajo no critica el objetivo de la ley 26.388; ya que si bien aquí se plantea una problemática puntual, se valoran las iniciativas que llevan a la incorporación de la tecnología informática dentro de las actividades cotidianas. En ese sentido, se considera un gran hito en lo que respecta al ámbito del derecho penal; el hecho de tomar esta primera aproximación con un concepto tan abstracto y distinto en esencia al derecho, como lo es el de la informática y todas las acciones que devengan de esta área.

El esfuerzo en cuanto a los trabajos en el contexto de esta ley se considera de vital importancia, siendo que la sociedad contemporánea ha incorporado de manera natural la tecnología informática permitiendo que así como ésta se utilice para acciones positivas, sea el medio también para cometer acciones indebidas. En este sentido, se destaca la iniciativa en cuanto a la actualización del Código Penal sancionado el 29 de octubre de 1921 durante la primera presidencia de Hipólito Yrigoyen, que lo acerca a la realidad de otra sociedad diferenciada por más de 90 años de evolución.

Sin embargo, como respuesta a la problemática planteada, se propone una modificación a la redacción del artículo 153 bis, de modo de especificar el ámbito de acción del verbo tipificado. En definitiva, se propone cambiar el verbo *acceder* por el de *interactuar* considerando además que dicha acción *resulte en un flujo de información*. De este modo, el artículo se propone de la siguiente manera: "*Será reprimido con…, el que a sabiendas interactúe por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema informático de acceso restringido, resultando en un flujo de información en el que ingresen o egresen datos desde una fuente de información…*"

De esta manera, si bien el verbo *interactuar* pudiera contemplar más actividades que las del verbo *acceder,* se reducen aquellas a las que se comprendan bajo el dolo resultante en cuanto a manejar datos relacionados al sistema en cuestión. Esto deja por fuera aquellas situaciones en las cuales se pudiera *acceder* a un dato o sistema informático concebidas sin ningún tipo de dolo ni consecuencia negativa. Por otro lado, refuerza las acciones en las cuales su origen sea específicamente generar este tipo de consecuencias negativas premeditadas.

Trabajo futuro

En primera instancia y bajo lo planteado al inicio de este análisis, se cree conveniente estudiar la posibilidad de incorporar un nuevo léxico, que desde su concepción se base en la tecnología informática; de manera de evitar las ambigüedades que resultan del empleo de palabras que simplemente se adaptan a un nuevo paradigma.

En este sentido, se espera que como consecuencia, se vuelva a trabajar en la definición de los tipos penales involucrados en las actividades relacionadas a la tecnología informática.

Por último y a raíz de esto mismo, resultará conveniente revisar también las penas asociadas a estos nuevos tipos penales.

Referencias

Arocena, G. A. (s.f.). *La regulación de los delitos informáticos en el código penal argentino. Introducción a la ley nacional núm. 23.388.*

Cámpoli, G. A. (2001). *El Elemento Subjetivo En Los Delitos Electrónicos – ¿El Dolo O La Culpa?* Quito, Ecuador: Primer Congreso Mundial de Derecho Informático.

Fissore, H. M. (s.f.). *Delitos Informáticos.*

Gonzalez, J. D. (2011). *Ley de Delitos Informáticos (26.388).*

InfoLEG. (25 de 6 de 2013). *Información legislativa y documental*. Obtenido de InfoLEG: http://www.infoleg.gov.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

Real Academia Española. (25 de 6 de 2013). *DICCIONARIO DE LA LENGUA ESPAÑOLA - Vigésima segunda edición*. Obtenido de Real Academia Española: http://buscon.rae.es/drae/?val=delito

Real Academia Española. (25 de 6 de 2013). *DICCIONARIO DE LA LENGUA ESPAÑOLA - Vigésima segunda edición*. Obtenido de Real Academia Española: http://buscon.rae.es/drae/?val=acceder

Real Academia Española. (25 de 6 de 2013). *Real Academia Española*. Obtenido de DICCIONARIO DE LA LENGUA ESPAÑOLA - Vigésima segunda edición: http://buscon.rae.es/drae/?val=inform%C3%A1tica

Rinaldi, S. L. (2001). *Delitos informáticos, perfil criminológico del hacker, especial referencia a los delitos de contenido económico y normativa aplicable.* Mar del Plata: Primeras Jornadas Latinoamericanas de Derecho Informático.

Riquert, M. A. (2009). *Delincuencia Informática en Argentina y el MERCOSUR, Prólogo de David Baigún.* Buenos Aires: Editorial Ediar.

Seguinfo. (25 de 6 de 2013). *Legislación y Delitos Informáticos - Tipos de Delitos Informáticos*. Obtenido de Seguinfo: http://www.segu-info.com.ar/delitos/tiposdelito.htm

Sueiro, C. C. (2011). *La eficiencia de la ley 26.388 de reforma en materia de criminalidad informática al código penal de la nación.*

Télles Valdez, J. (1996). *Derecho Informático. 2° Edición.* México: Mc Graw Hill.

Télles Valdez, J. (2000). *VIII Congreso Iberoamericano de Derecho e Informática.* Cancún y Distrito Federal, México.

Temperini, M. G. (s.f.). *Delitos Informáticos: La punibilidad del Hacking y sus consecuencias.*

Users Staff. (2011). *Hacking desde cero.*