

ABG. JOSÉ GREGORIO PUMAREJO. APROXIMACIÓN AL ESTUDIO DEL DELITO DE ACCESO INDEBIDO EN LA LEGISLACIÓN PENAL VENEZOLANA. 37-58. REVISTA CENIPEC. 38. 2026. ENERO - DICIEMBRE. ISSN: 0798-9202.

ABG. JOSÉ GREGORIO PUMAREJO

**APROXIMACIÓN AL ESTUDIO DEL DELITO DE ACCESO INDEBIDO
EN LA LEGISLACIÓN PENAL VENEZOLANA**

Recepción: 06/02/2026.

Aceptación: 28/04/2026.

Abg. José Gregorio Pumarejo
luchon78@gmail.com
<https://orcid.org/0009-0008-3111-7144>
Universidad Central de Venezuela
CARACAS-VENEZUELA

Resumen

Esta investigación analiza el delito de acceso indebido (Art. 6, Ley Especial Contra los Delitos Informáticos) mediante la dogmática penal. Define la conducta como un delito de mera actividad y tipo cerrado, diferenciando entre el acceso no autorizado (*outsider*) y el exceso de funciones (*insider*). El estudio busca precisar la calificación jurídica para garantizar el principio de legalidad en el proceso penal.

Palabras clave: tecnologías de información, delitos informáticos, acceso indebido.

An approach to the study of the offense of unauthorized access in venezuelan criminal legislation

Abstract

This research analyzes the crime of unauthorized access (Art. 6, Special Law Against Computer Crimes) through criminal dogmatics. It defines the conduct as a formal offense (mera actividad) and a closed type, distinguishing between unauthorized access (*outsider*) and exceeding authority (*insider*). The study aims to clarify legal qualification to ensure the principle of legality in criminal proceedings.

Key words: information technologies, cybercrimes, unauthorized accesslegal.

Approche de l'étude du délit d'accès indu dans la législation pénale vénézuélienne

Résumé

Cette recherche analyse le délit d'accès non autorisé (art. 6 de la Loi spéciale contre les délits informatiques) au moyen de la dogmatique pénale. Elle définit la conduite comme un délit de simple activité et de type fermé, distinguant entre l'accès non autorisé (*outsider*) et le dépassement de fonctions (*insider*). L'étude vise à préciser la qualification juridique afin de garantir le principe de légalité dans la procédure pénale.

Mots clés: technologies de l'information, délits informatiques, accès non autorisé.

Abordagem do estudo do crime de acesso indevido na legislação penal venezuelana

Resumo

Esta pesquisa analisa o crime de acesso indevido (Art. 6º da Lei Especial contra Crimes Informáticos) sob a ótica da dogmática penal. Define a conduta como um crime de mera atividade e de tipo fechado, diferenciando o acesso não autorizado (*outsider*) do excesso no exercício de funções (*insider*). O estudo procura precisar a qualificação jurídica para garantir o princípio da legalidade no processo penal.

Palavras chave: tecnologias da informação, crimes informáticos, acesso indevido.

1.- Introducción

En el contexto de la sociedad de la información, el ordenamiento jurídico venezolano ha respondido a los desafíos tecnológicos mediante la promulgación de la Ley Especial Contra los Delitos Informáticos (2001). Dentro de este marco legal, el acceso indebido, tipificado en el artículo 6, se erige como la piedra angular y delito matriz de la legislación penal tecnológica en el país. Su relevancia reside en que constituye la conducta base, la entrada no autorizada o el exceso en el uso de un sistema, que suele preceder o facilitar la ejecución de tipos penales más complejos.

La presente investigación se fundamenta en un análisis exhaustivo de los elementos de este tipo penal, empleando como herramienta metodológica la Teoría General del Delito. Para comprender el fenómeno del acceso indebido, es imperativo iniciar con el estudio de la acción como comportamiento humano que encaja en una descripción legal. En este sentido, se adopta un concepto de acción finalista, el cual permite diferenciar la conducta voluntaria de aquellas situaciones donde existe ausencia de acción, tales como movimientos reflejos o estados de inconsciencia.

A través de este abordaje dogmático, el estudio desglosa los componentes esenciales del delito:

Tipo Objetivo: Se identifican las conductas rectoras de acceder, interceptar, interferir o usar sistemas tecnológicos. **Sujetos:** Se determina que el sujeto activo es indeterminado ("toda persona"), mientras que el pasivo es el titular del sistema o bien jurídico tutelado. **Tipo Subjetivo:** Se establece que la modalidad de comisión es eminentemente dolosa, analizada desde las teorías de la voluntad y la representación, lo que excluye cualquier forma de responsabilidad objetiva en respeto al principio de culpabilidad. **Elementos Normativos:** Se profundiza en el concepto de "debida autorización", cuya valoración es el criterio diferenciador entre terceros ajenos (*outsiders*) y usuarios legítimos que exceden sus facultades (*insiders*). Finalmente, esta delimitación técnica permite concluir que el acceso indebido es un delito de mera actividad y de tipo cerrado.

2.- La Constitución como marco de protección del bien jurídico

La Constitución de la República Bolivariana de Venezuela establece el marco normativo que declara la ciencia, la tecnología y el conocimiento como áreas de interés público. En este contexto, el Estado asume la responsabilidad de asegurar que dichas actividades se desarrollen bajo estrictos principios éticos y legales. Dicha protección constitucional se extiende al ámbito digital, donde el ordenamiento jurídico tutela los bienes jurídicos frente a ilícitos informáticos, tipificando y sancionando específicamente el acceso indebido a sistemas y datos, como una manifestación concreta de la garantía estatal en el resguardo de la integridad tecnológica y la seguridad de la información:

Artículo 110. El Estado reconocerá el interés público de la ciencia, la tecnología, el conocimiento, la innovación y sus aplicaciones y los servicios de información necesarios por ser instrumentos fundamentales para el desarrollo económico, social y político del país, así como para la seguridad y soberanía nacional. Para el fomento y desarrollo de esas actividades, el Estado destinará recursos suficientes y creará el sistema nacional de ciencia y tecnología de acuerdo con la ley. El sector privado deberá aportar recursos para los mismos. El Estado garantizará el cumplimiento de los principios éticos y legales que deben regir las actividades de investigación científica, humanística y tecnológica. La ley determinará los modos y medios para dar cumplimiento a esta garantía.

De esta disposición constitucional se desprende la tutela de las tecnologías y los servicios de información como bienes de interés público, al ser reconocidos como instrumentos esenciales para el desarrollo económico, social y político de la Nación. En el contexto del auge de la sociedad de la información, cobran especial relevancia tanto el desarrollo tecnológico como la protección de los datos y la información que estos sistemas albergan. Si bien el artículo no constituye un mandato de incriminación penal en sí mismo, sí representa un fundamento constitucional que legitima la intervención del derecho penal para sancionar aquellas conductas que lesionen o pongan en peligro dichos bienes jurídicos, o que los utilicen

como medio de comisión. En este sentido, la tipificación del delito de acceso indebido a sistemas o datos informáticos encuentra su justificación última en la necesidad de salvaguardar la integridad y seguridad de estas tecnologías declaradas de interés público por la Carta Magna.

3.- Bien jurídico tutelado en el delito de acceso indebido

En cuanto al objeto jurídico o bien jurídico tutelado, la Ley Especial Contra los Delitos Informáticos (2001) establece como objeto de protección los sistemas que utilizan tecnologías de información. No obstante, parte de la doctrina ha ampliado esta noción. Al respecto, Hernández (2009) señala que:

Como ya se ha mencionado en relación a las propuestas que aluden a la idea de la seguridad informática, los delitos vinculados con la informática no sólo dañan en su comisión bienes jurídicos individuales y concretos; su comisión también pone en peligro la confianza de la sociedad en el buen funcionamiento de los sistemas informáticos y de las redes de transmisión de datos (p. 239).

Bajo esta perspectiva, el delito de acceso indebido, previsto en el citado texto legal, no solo vulnera la seguridad de sistemas y datos en sentido estricto, sino que además lesiona un interés supraindividual: la confianza colectiva en la integridad y confiabilidad de las infraestructuras tecnológicas. Dicha confianza, erigida sobre el interés público que la Constitución reconoce a la ciencia y la tecnología, se ve afectada cuando se quebrantan los mecanismos de acceso y se transgreden los principios éticos y legales que deben regir el uso de estos instrumentos fundamentales para el desarrollo social y económico del país.

La conducta típica de acceso indebido afecta la disponibilidad y confidencialidad de los datos e información contenidos en los sistemas que utilizan tecnologías de información, generando un perjuicio a la persona cuyos datos fueron objeto de acceso, el cual variará según la finalidad perseguida por el sujeto activo en la comisión del hecho.

En este sentido, Mayer (2017) sostiene que estas conductas no solo producen afectaciones individuales a las personas mediante el acceso indebido, sino

que también comprometen el correcto funcionamiento de las tecnologías de información, así como las características de confidencialidad que estas cumplen, considerando el carácter instrumental y colectivo que despliegan en la sociedad:

La funcionalidad informática constituye, por una parte, un interés cuyo sentido y alcance debe precisarse dinámicamente, así como en atención a la forma en que opera el uso de redes computacionales, en tanto sistemas de interconexión (remota y masiva) entre los individuos. Ella constituye, por otra parte, un bien jurídico instrumental de carácter colectivo, cuya tutela penal debe verificarse en términos particularmente acotados (p. 255).

Por consiguiente, los delitos informáticos, y específicamente el acceso indebido previsto en la Ley Especial Contra los Delitos Informáticos, revisten un carácter *pluriofensivo*, en tanto no afectan un único bien jurídico, sino que lesionan o ponen en peligro diversos intereses tutelados por el derecho penal. Esta pluriofensividad se manifiesta tanto en la dimensión individual (patrimonio, privacidad, intimidad) como en la colectiva, al quebrantar la confianza social en la integridad y seguridad de las infraestructuras tecnológicas que, por mandato constitucional, constituyen instrumentos fundamentales para el desarrollo del país.

4.- Elementos del tipo penal de acceso indebido en la Ley Especial Contra los Delitos Informáticos

4.1.- Análisis de la conducta típica

El tipo penal se compone de una faz objetiva y una faz subjetiva. La primera remite al aspecto externo de la conducta realizada por el autor y se corresponde con la descripción contenida en la ley penal. En palabras de Puig (2006), "los elementos estructurales del tipo penal son tres (03): la conducta típica, sus sujetos y sus objetos" (p. 218).

El análisis del tipo penal de acceso indebido requiere precisar su ubicación y contenido normativo. Dicho tipo se encuentra tipificado en el artículo 6 de la Ley Especial Contra los Delitos Informáticos (2001), publicada en la Gaceta Oficial N.º 37.313 del 29 de octubre de 2001, la cual forma parte

del Título II, Capítulo I, denominado "De los Delitos Contra los Sistemas que Utilizan Tecnologías de Información". El texto del artículo es el siguiente:

Artículo 6. Acceso Indebido Toda persona que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.

Del análisis del artículo 6 de la Ley Especial Contra los Delitos Informáticos (2001) es posible identificar los tres elementos estructurales del tipo penal señalados por Puig (2006): la conducta típica, los sujetos y los objetos. Dentro de la conducta típica se distinguen, a su vez, dos componentes necesarios para su examen: el aspecto objetivo, que corresponde al elemento externo o material del comportamiento y el subjetivo.

4.2.- Conducta típica

La conducta típica del acceso indebido, prevista en el artículo 6 de la Ley Especial Contra los Delitos Informáticos (2001), consiste en:

De esta disposición se desprenden cuatro verbos rectores que describen las acciones punibles: acceder, interceptar e usar -siendo necesario aclarar que la conjunción "o" presenta estas conductas como alternativas-. Para precisar su sentido jurídico-penal, resulta útil acudir a las definiciones del Diccionario de la lengua española:

Acceder (del latín *accedere*): 'entrar en un lugar o pasar a él' (Real Academia Española [RAE], s.f., definición 2).

Interceptar (del latín *interceptus*, participio de *intercipere*): 'apoderarse de algo antes de que llegue a su destino' (RAE, s.f., definición 1).

Usar: 'hacer servir una cosa para algo' (RAE, s.f., definición 1).

Estas acepciones contribuyen a delimitar el alcance objetivo de cada modalidad de conducta, en tantos elementos del tipo objetivo. Las acepciones del Diccionario de la lengua española (Real Academia Española,

s.f.) contribuyen a delimitar el alcance objetivo de cada modalidad de conducta, en tanto, elementos del tipo objetivo. Los verbos acceder, interceptar y usar -junto con interferir, previsto en la norma- constituyen las conductas típicas del acceso indebido en la Ley Especial Contra los Delitos Informáticos (2001). Estas acciones describen los comportamientos externos que deben examinarse para la comprobación del tipo penal. Cabe precisar que tales verbos no son concurrentes, es decir, basta con que se realice uno de ellos para que la conducta se adecue al tipo penal.

El tipo penal de acceso indebido, previsto en el artículo 6 de la Ley Especial Contra los Delitos Informáticos (2001), no exige que la acción de acceder, interceptar, interferir o usar recaiga necesariamente sobre datos o información contenidos en un sistema automatizado. La redacción de la norma permite entender que el objeto material puede estar constituido tanto por los componentes físicos (*hardware*) como por el sistema en sí mismo considerado.

En este contexto, la interceptación o interferencia implica siempre una relación directa con el sistema; tales conductas pueden presentarse como consecuencia de un acceso previo o de manera autónoma. Por su parte, acceder -entendido como entrar en un sistema o componente- constituye la conducta típica basal, cuyo resultado inmediato es la penetración en el ámbito del sistema. Esta acción puede o no ir seguida de la obtención efectiva de datos, pues el tipo no condiciona la consumación del acceso a dicho resultado adicional. Así, mientras acceder supone el ingreso, obtener -aunque no constituya un verbo rector autónomo en este tipo penal- representa un posible paso ulterior que podría implicar el conocimiento efectivo de la información contenida.

Las conductas típicas descritas en el artículo 6 de la Ley Especial Contra los Delitos Informáticos (2001) -acceder, interceptar, interferir o usar sistemas que utilicen tecnologías de información- requieren, para su configuración, que se realicen sin la debida autorización. Ello implica que el titular o propietario del sistema no ha otorgado el permiso correspondiente o que, en caso de haberlo hecho, la conducta excede los límites de la autorización conferida.

El medio empleado para ejecutar la conducta típica es indistinto; puede tratarse de una conexión a través de internet o del acceso directo a un computador

personal. En este sentido, Azuaje y Leal (2011) señalan que "el acceso puede ser hecho con cualquier medio, sea a través de Internet, sea situándose frente a la computadora y tecleando el *login* y el *password*" (p. 35).

4.3.- Sujetos

El sujeto activo del tipo penal es quien realiza la conducta descrita en la norma, mientras que el sujeto pasivo es el titular del bien jurídico protegido. Al respecto, Puig (2006) señala que "el sujeto pasivo no coincide necesariamente con el sujeto sobre el que recae físicamente la acción, ni con el "perjudicado"" (p. 220). De allí que resulte necesario distinguir entre el sujeto pasivo y la persona sobre la cual recae materialmente la acción típica.

En el ámbito de los delitos informáticos, particularmente en el acceso indebido, esta distinción adquiere especial relevancia. La acción típica puede ejecutarse, por ejemplo, a través de internet sobre una cuenta de correo electrónico o una aplicación, sin que ello implique que el titular del software o sistema afectado sea necesariamente la persona que sufre la lesión al bien jurídico. En consecuencia, resulta pertinente realizar esta diferenciación para una adecuada comprensión del tipo penal.

En el tipo penal de acceso indebido previsto en la Ley Especial Contra los Delitos Informáticos (2001), no se exige una cualidad o circunstancia especial en el sujeto activo para la realización de las conductas típicas; por consiguiente, cualquier persona que lleve a cabo las acciones descritas puede ser considerada sujeto activo. En cuanto al sujeto pasivo, este viene constituido por el titular o propietario del sistema que utilice tecnologías de información, titular del bien jurídico protegido. En este contexto, resulta pertinente la distinción entre las distintas clases de hackers, tal como la presenta Campos (2016):

Black hat hackers: Hackers de sombrero negro, son los que se dedican a romper la seguridad de un medio electrónico o crean algún virus para que los servidores sufran daños y posteriormente la pérdida de información.

White hat hackers: Hackers de sombrero blanco, son los hackers que respetan y cumplen su ética. Regularmente son los que trabajan para empresas dedicándose exclusivamente a encontrar

vulnerabilidades en el sistema de seguridad de los ordenadores y a proteger la información de los *Black Hat Hackers* (p.33).

Esta clasificación resulta relevante para el análisis del tipo penal de acceso indebido, pues si bien la norma no exige una característica especial en el sujeto activo, permite reconocer los perfiles que comúnmente ejecutan tales conductas: los white hat hackers (sombros blancos), quienes normalmente actúan sin fines maliciosos, y los black hat hackers o crackers (sombros negros), cuyo propósito es vulnerar la seguridad de los sistemas informáticos.

4.4.- Objetos

En el análisis del tipo penal resulta necesario distinguir entre el objeto material y el objeto jurídico. El primero -también denominado objeto de la acción- está constituido por la persona o cosa sobre la cual recae físicamente la conducta típica. El segundo -conocido como bien jurídico tutelado- es el objeto de protección de la ley. En el caso del acceso indebido, el objeto material no coincide con el sujeto pasivo, pues aquel recae sobre los sistemas que utilizan tecnologías de información o sus componentes, mientras que el sujeto pasivo es el titular del bien jurídico.

5.- Tipo subjetivo

En cuanto al tipo subjetivo, este comprende las circunstancias internas o elementos psíquicos que determinan la realización de la conducta típica por parte del sujeto activo. Al respecto, Bacigalupo (1999) señala:

Es claro que en la acción se dan elementos exteriores (objetivos) y elementos interiores (subjetivos). Este aspecto subjetivo constituye el "tipo subjetivo". Sin embargo, los elementos subjetivos no son cognoscibles directamente, sino a través de los elementos externos que objetivan un contenido psíquico del comportamiento (p.314).

El tipo subjetivo comprende los elementos internos que concurren en el sujeto activo para la realización de la conducta típica, los cuales se manifiestan fundamentalmente a través del dolo, la culpa y la preterintención como formas

de imputación subjetiva. Esta concepción, que sitúa al dolo como elemento integrante del tipo subjetivo, encuentra su fundamento en la teoría finalista de la acción desarrollada por Welzel (1956).

En el caso específico del acceso indebido, tipificado en el artículo 6 de la Ley Especial Contra los Delitos Informáticos (2001), la modalidad subjetiva es exclusivamente dolosa. Ello obedece a que el tipo penal en cuestión no contiene una cláusula expresa de incriminación culposa, es decir, no emplea términos como "por negligencia", "imprudencia" o "inobservancia de reglamentos" que permitan atribuir la conducta a título de culpa. En consecuencia, al carecer de dicha previsión legal, no es posible imputar subjetivamente el acceso indebido en su modalidad culposa.

Al tratarse de un tipo penal que únicamente admite la modalidad dolosa, corresponde precisar qué se entiende por dolo y cómo se imputa esta forma subjetiva en el delito de acceso indebido. En este sentido, debe señalarse que ni la Ley Especial Contra los Delitos Informáticos (2001) ni el Código Penal venezolano (2005) ofrecen una definición expresa del dolo. Este último, en su artículo 61, se limita a establecer las bases de la imputación subjetiva al disponer que "nadie puede ser castigado como reo de delito no habiendo tenido la intención de realizar el hecho que lo constituye, excepto cuando la ley se lo atribuya como consecuencia de su acción u omisión". De esta manera, la determinación del concepto y alcance del dolo -así como la distinción entre sus diversas clases- queda deferida a la elaboración doctrinal y jurisprudencial. El texto de dicha norma es el siguiente:

Artículo 61. Nadie puede ser castigado como reo de delito no habiendo tenido la intención de realizar el hecho que lo constituye, excepto cuando la ley se lo atribuye como consecuencia de su acción u omisión.

El que incurra en faltas, responde de su propia acción u omisión, aunque no se demuestre que haya querido cometer una infracción de la ley.

La acción u omisión penada por la ley se presumirá voluntaria, a no ser que conste lo contrario.

En esta norma se consagra la responsabilidad a título subjetivo, excluyéndose la responsabilidad penal objetiva en tanto que la misma resulta incompatible con los principios que rigen el derecho penal en un Estado Democrático Social de Derecho y de Justicia, particularmente con el principio de culpabilidad y el principio del hecho.

Prosiguiendo con lo antedicho, ante la ausencia de una definición legal del dolo, es necesario acudir a la dogmática penal -esto es, a la doctrina especializada- así como a la jurisprudencia nacional, a fin de precisar su concepto y alcance. Dicha tarea resulta tanto más relevante cuanto que la imputación a título de dolo conlleva la aplicación de las penas más severas previstas en el ordenamiento jurídico.

En este orden de ideas, Roxin (1997) define el dolo típico de la siguiente manera: "Por dolo típico se entiende, según una usual fórmula abreviada, el conocimiento (saber) y voluntad (querer) de los elementos del tipo objetivo" (p. 308). De esta definición se desprende que el dolo implica, por un lado, el conocimiento de los elementos objetivos del tipo y, por otro, la voluntad de realizar la conducta o de alcanzar el resultado previsto por la norma. Esta doble exigencia -cognoscitiva y volitiva- explica que la sanción prevista para las conductas dolosas sea la más severa dentro del ordenamiento jurídico-penal.

Esta concepción del dolo corresponde a lo que la doctrina ha denominado atribución psicológico-descriptiva, esto es, la identificación de estados mentales en casos genéricos que el derecho penal cataloga como dolosos. A partir de esta base, se han desarrollado diversas teorías explicativas, entre las que destacan la teoría de la voluntad y la teoría de la representación. Al respecto, Bacigalupo (1999) ha realizado importantes precisiones:

Tradicionalmente las explicaciones referentes al dolo se han polarizado en las llamadas teoría de la voluntad y teoría de la representación. La discusión afecta en primer lugar a la esencia del dolo y en segundo lugar a la cuestión práctica de la distinción entre el dolo y la culpa (p.323).

Las teorías de la voluntad y de la representación han intentado explicar el dolo desde una perspectiva psicológica, esto es, a partir de los procesos internos del sujeto, permitiendo además diferenciarlo de la culpa consciente y la culpa inconsciente. Dado que el presente trabajo no tiene por objeto realizar un estudio exhaustivo del dolo, sino únicamente precisar su concepto y determinar la clase de dolo que resulta admisible en el tipo penal de acceso indebido, resulta suficiente con señalar las distinciones fundamentales.

En función de la teoría que se acoja -voluntad o representación-, es posible distinguir tres clases de dolo: directo, de consecuencias necesarias y eventual. En el dolo directo, el sujeto tiene la intención de realizar los elementos del tipo objetivo. En cambio, en el dolo de consecuencias necesarias y en el dolo eventual, aunque no existe propiamente una intención dirigida a la realización del tipo, el sujeto se representa la producción del resultado como segura o probablemente, respectivamente.

Desde la perspectiva del dolo psicológico-descriptivo -esto es, aquel que concibe el dolo como un proceso anímico del sujeto-, el tipo penal de acceso indebido previsto y sancionado en el artículo 6 de la Ley Especial Contra los Delitos Informáticos (2001) admite las tres modalidades tradicionales: dolo directo, dolo de consecuencias necesarias y dolo eventual. En el primer caso, el sujeto activo realiza la conducta de acceder, interceptar, interferir o usar un sistema con la intención de llevar a cabo los elementos del tipo objetivo. En las dos restantes, si bien no existe una intención dirigida directamente a la realización del tipo, el sujeto se representa la producción del resultado como segura (dolo de consecuencias necesarias) o como probable (dolo eventual), y aun así ejecuta la acción.

En relación con el tipo subjetivo, resulta pertinente mencionar que las corrientes funcionalistas-normativistas -cuyo principal exponente es Günther Jakobs (1997)- han impulsado, a través de desarrollos dogmáticos posteriores como los de Pérez Barberá (2011) y Greco (2017), una concepción alternativa del dolo. Esta perspectiva, conocida como dolo normativo o, en contraposición, atributivo-normativo, desplaza el eje de la imputación subjetiva desde la constatación empírica de procesos anímicos hacia una valoración normativa del comportamiento, modificando sustancialmente la forma de imputar el dolo.

En línea con lo expuesto, resulta pertinente esta alusión, pues la concepción normativista del dolo -impulsada por Jakobs (1997) y desarrollada por autores como Pérez Barberá (2011) y Greco (2017) - modifica sustancialmente la forma de imputar y probar esta categoría dogmática. Desde esta perspectiva, el tipo subjetivo tendería a desaparecer, quedando únicamente el tipo objetivo como referente de la imputación. En este esquema, el dolo se inferiría a partir de circunstancias objetivas externas que permitirían presumir su concurrencia, lo que evitaría la dificultad probatoria inherente a la constatación de procesos anímicos internos. Bajo este enfoque, además, el dolo se concibe como una categoría unitaria que, en última instancia, se identificaría con el dolo eventual.

6.- Elementos normativos

Los elementos normativos del tipo objetivo se caracterizan por requerir, para su comprensión, algo más que una mera percepción sensorial; su significado debe ser complementado mediante una valoración cultural o jurídica. En este sentido, Puig (2006) precisa:

Son elementos normativos los que aluden a una realidad determinada por una norma jurídica o social. Según esta definición, cabe distinguir entre elementos normativos jurídicos y elementos normativos sociales. Ambos pueden a su vez, subdividirse en elementos referidos a una valoración (o valorativos) y elementos referidos a un sentido (p.232).

De lo anterior se desprende que, para constatar la concurrencia de un elemento normativo en el caso concreto, resulta indispensable realizar una valoración - cultural o jurídica- que trasciende la simple apreciación sensorial. Dicha operación es determinante, pues la ausencia de esta valoración podría conducir a una incorrecta subsanación del tipo penal por falta de un elemento normativo. Cabe añadir que los elementos normativos no se encuentran presentes en la totalidad de los tipos penales, sino únicamente en aquellos cuyo legislador ha incorporado cláusulas valorativas de esta naturaleza.

Desde otra perspectiva, Bacigalupo (1999) precisa que los "elementos normativos son aquellos en los que predomina una valoración y que, por lo

tanto, no pueden ser percibidos sólo mediante los sentidos" (p. 226). Dado que estos elementos integran la descripción típica, resulta oportuno examinar su concurrencia en el tipo penal de acceso indebido.

En la lectura del artículo 6 de la Ley Especial Contra los Delitos Informáticos (2001) es posible identificar un elemento normativo: la expresión "debida autorización". Para determinar si concurre este elemento, se requiere una valoración -fundamentalmente cultural- acerca del origen y alcance de dicha autorización. En tal sentido, Azuaje y Leal (2011), citando a Kerr, señalan que "las normas que otorgan autorización son de tres tipos: código, contractuales y sociales" (p. 35). Importa precisar que el elemento normativo no debe confundirse con la antijuricidad, pues aquel forma parte de la descripción típica, mientras que esta constituye una categoría distinta dentro de la teoría del delito.

En relación con los elementos normativos del tipo penal, Bascur y Peña (2022) analizan específicamente la autorización en los siguientes términos:

Ahora bien, con relación a iii) los elementos normativos de carácter alternativo "sin autorización del titular" y "excediendo la autorización que se posea", estos reflejan con nitidez que los datos o el sistema informático no se encuentra destinado al autor de la intromisión (p.11).

De esta distinción se desprende una diferenciación fundamental entre dos situaciones: la ausencia total de autorización y el exceso en la autorización concedida. En el primer supuesto, nos encontramos ante un extraneus u outsider, esto es, alguien que no ha recibido autorización alguna y, no obstante, accede, obtiene, intercepta o interfiere con el sistema de tecnologías de información, sin que dichos datos o información le estén destinados. En el segundo supuesto, se trata de un intraneus o insider, es decir, una persona que sí ha recibido autorización, pero cuyas conductas exceden los límites de la misma.

7.- Elementos descriptivos

En cuanto a los elementos descriptivos, estos se encuentran presentes en todo tipo penal y se caracterizan porque su comprensión requiere únicamente

una correcta percepción sensorial. Sobre esta categoría, Bacigalupo (1999) señala: "Elementos descriptivos son aquellos que el autor puede conocer y comprender predominantemente a través de sus sentidos; puede verlos, tocarlos, oírlos, etcétera" (p. 226). De ello se sigue que, para constatar la concurrencia de un elemento descriptivo, basta con la apreciación sensorial del mismo.

Para finalizar, resulta oportuno mencionar que la dogmática penal contemporánea ha desarrollado la teoría de la imputación objetiva como un elemento adicional que debe evaluarse en el análisis del tipo penal. Sin embargo, dado que el presente trabajo no pretende un examen exhaustivo de esta teoría -lo que excedería sus objetivos-, únicamente se deja constancia de que, en un análisis completo de la tipicidad, deberían considerarse los principios que rigen la imputación de la conducta, tales como el riesgo permitido, el principio de confianza, el principio de prohibición de regreso y el principio de imputación a la víctima.

En caso de concurrir alguno de estos principios -riesgo permitido, principio de confianza, prohibición de regreso o imputación a la víctima-, no habría lugar a la imputación del tipo objetivo, pues tales principios operan como causales de exclusión de la imputación objetiva.

Procede precisar, adicionalmente, que el tipo penal de acceso indebido es un delito de mera actividad, ya que las conductas descritas -acceder, interceptar, interferir o usar- se consuman con la sola realización de la acción, sin que se requiera la producción de un resultado separable y perceptible sensorialmente como modificación del mundo exterior. Se distingue así de los delitos de resultado, en los cuales la consumación exige un efecto o consecuencia distinta de la propia conducta.

Por otra parte, se trata de un tipo penal cerrado, en contraposición a los denominados tipos penales abiertos. Esta teoría fue desarrollada inicialmente por Welzel (1956) y posteriormente ampliada por Roxin (1997). Sobre los tipos penales abiertos, Jescheck y Weigend (2014) han señalado lo siguiente:

La teoría de los tipos "abiertos" sostiene que en Derecho penal existen tipos de los que no pueden deducirse completamente, sino tan sólo en parte, los elementos del injusto del delito

correspondiente. La integración de los que se encuentran ausentes debe ser llevado a cabo por medio de componentes positivos de la antijuricidad que se encuentran fuera del tipo. Los tipos abiertos son definidos como aquellas disposiciones penales "en las que falta una imagen rectora de carácter objetivo para completar el tipo", de modo que en la práctica no puede tener lugar de la mano del texto legal una diferenciación entre el comportamiento prohibido y el permitido (p.364).

El artículo 6 de la Ley Especial Contra los Delitos Informáticos (2001), que tipifica el acceso indebido, describe de manera completa la conducta típica, los sujetos y los objetos de tutela penal, sin que sea necesario acudir a otras disposiciones para integrar tales elementos. Importa precisar que no debe confundirse la categoría de tipo penal abierto con la presencia de elementos normativos en la descripción típica. En tal sentido, el tipo penal de acceso indebido corresponde a la categoría de tipo cerrado.

8.- Conclusiones

La investigación permitió constatar que el acceso indebido, tipificado en el artículo 6 de la Ley Especial Contra los Delitos Informáticos (2001), constituye la piedra angular de la legislación penal tecnológica en Venezuela. Ello obedece a su naturaleza de delito matriz, en tanto conducta base -esto es, la entrada no autorizada al sistema- que precede o facilita la comisión de otros tipos penales más complejos contenidos en la misma ley. Conforme a los postulados de la Teoría General del Delito, el análisis del tipo penal de acceso indebido se desglosa en los siguientes aspectos técnicos:

Es un delito de mera actividad, en tanto el tipo penal se consuma con la simple ejecución de la conducta descrita -acceder, interceptar, interferir o usar-, sin que se requiera la producción de un daño material o resultado externo posterior para su configuración;

Se trata de un tipo penal cerrado, dado que la ley describe de manera exhaustiva y precisa la conducta prohibida, los sujetos intervinientes y los objetos de tutela penal, sin necesidad de acudir a otras disposiciones normativas para complementar su significado jurídico;

Es de sujeto activo indiferenciado o común, pues la norma emplea la expresión "toda persona", lo que implica que no se exige una cualidad técnica o profesional especial para ser autor del delito;

El sujeto pasivo del delito es el titular o propietario del sistema de tecnologías de información, quien ve vulnerado su bien jurídico de seguridad informática como objeto de tutela penal;

En orden al elemento normativo, un hallazgo relevante del análisis lo constituye el papel de la "debida autorización" como elemento normativo del tipo. La tipicidad de la conducta no se configura únicamente por el ingreso de un tercero ajeno (*outsider*) al sistema, sino también por el abuso de confianza del usuario legítimo (*insider*) que, teniendo acceso autorizado, excede los límites de las facultades que le fueron otorgadas;

La conducta típica recae directamente sobre sistemas que utilizan tecnologías de información o sus componentes, protegiendo no solo el soporte físico (*hardware*), sino primordialmente la confidencialidad y disponibilidad de los datos contenidos en ellos.

Cabe concluir señalando que la identificación detallada de estos elementos permite distinguir claramente el acceso indebido de otras figuras delictivas afines, evitando confusiones en la calificación jurídica y asegurando que la persecución penal se ajuste estrictamente al principio de legalidad.

Referencias bibliográficas

- Azuaje, M y Leal, S. (2011). Tres tipos penales informáticos. Revista de Ciencias Jurídicas de la Universidad Rafael Urdaneta Vol. V N° 1 (enero - junio 2011), consultado el 27 de diciembre de 2023, URL: <https://www.redalyc.org/pdf/1275/127521341003.pdf>
- Bascur, G. y Peña, R. (2022). Los delitos informáticos en Chile: Tipos delictivos, sanciones y reglas procesales de la Ley 21.459, primera parte. Revista de Estudios de la Justicia, <https://doi.org/10.5354/0718-4735.2022.67885>, consultado el 03 de noviembre de 2023, URL: <https://revistas.uchile.cl/index.php/RECEJ/article/view/67885>

- Barbagalo, F. (2022). Cibercrimen y delitos informáticos: una aproximación entre Legislación italiana y brasileña. Migalhas, Brasil, consultado el 30 de octubre de 2023, URL: <https://www.migalhas.com.br/depeso/374734/cibercriminalidade-e-crimes-informaticos>
- Betancur, N. (2002). *Curso de Derecho Penal (Esquemas del delito)*. 3ra edición. Bogotá, Colombia. Editorial Temis.
- Campos, P. (2016). Delitos informáticos en México y sus formas de prevención. Sección Tópicos Latinoamérica, México, consultado el 01 de noviembre de 2023, URL: http://revista.cleu.edu.mx/new/descargas/1604/articulos/Articulo09_Delitos_informaticos_en_Mexico_y_sus_formas_de_prevenicion.pdf
- Llamas, J. y Llamas, I. (2018). Internet, ¿Arma o Herramienta? Universidad de Guadalajara, México, consultado el 02 de noviembre de 2023, URL: http://www.publicaciones.cucsh.udg.mx/kiosko/2018/internet_arma_o_herramienta_Ebook.pdf
- Greco, Luis. (2017). Dolo sin Voluntad. Revista Nuevo foro penal N° 88. Consultado el 28 de diciembre de 2023, URL: <https://publicaciones.eafit.edu.co/index.php/nuevo-foro-penal/article/view/4749>
- Herzberg, R. (2008). Reflexiones sobre la teoría final de la acción. Revista Electrónica de Ciencia Penal y Criminología, consultado el 26 de diciembre de 2023, URL: <http://criminnet.ugr.es/recpc/10/recpc10-01.pdf>
- Hernández, L. (2009). El Delito Informático. Eguzkilore Numero 23, San Sebastián. Consultado el 27 de diciembre de 2023, URL: <https://www.ehu.eus/documents/1736829/2176697/18-Hernandez.indd.pdf>
- Jakobs, G. (1997). *Derecho Penal. Parte General Fundamentos y Teoría de la Imputación*. 2da. Edición corregida. Madrid, España: Marcial Pons, Ediciones Jurídicas.
- Jescheck, H, y Weigend, T. (2014). *Tratado de Derecho Penal. Parte General, Volumen 1*. (trad. Miguel Olmedo Cardenete) Traducción de la quinta edición alemana, Biblioteca Nacional del Perú: Pacíficos Editores S.A.C.
- Ley Especial Contra los Delitos Informáticos. Gaceta Oficial N.º 37.313. Del 17 de octubre de 2001.
- Mayer, L. (2017). El bien jurídico protegido en los delitos informáticos. Revista Chilena de Derecho, Vol. 44, N.º 1, Chile. Consultado el 27 de diciembre de 2023, URL: <https://www.scielo.cl/pdf/rchilder/v44n1/art11.pdf>
- Medina, J., Cárdenas, C., y Mejía, M. (2021). Análisis del phishing y la ley de delitos informáticos en Colombia. Cuaderno de Investigaciones: Semilleros

- Andina, (14). <https://doi.org/10.33132/26196301.1948>, consultado el 02 de noviembre de 2023, URL: <https://revia.areandina.edu.co/index.php/vbn/article/view/1948>
- Pérez Barberá, G., (2011), El concepto de dolo en el derecho penal. Hacia un abandono definitivo de la idea de dolo como estado mental [Versión electrónica] Cuaderno de Derecho Penal Nº 6, consultado el 28 de diciembre de 2023, URL: https://revistas.usergioarboleda.edu.co/index.php/cuadernos_de_derecho_penal/article/view/392
- Puig, S. (2006). *Derecho Penal. Parte General*. (8 a. ed.). Barcelona: España. Editorial Reppertor.
- Real Academia Española. (2023). Obtener. Versión Electrónica de la 23ª edición del Diccionario de la lengua española. Consultado el 27 de diciembre de 2023, URL: <https://dle.rae.es/obtener>
- _____ (2023). Acceder. Versión Electrónica de la 23ª edición del Diccionario de la lengua española. Consultado el 27 de diciembre de 2023, URL: <https://dle.rae.es/acceder>
- _____ (2023). Interceptar. Versión Electrónica de la 23ª edición del Diccionario de la lengua española. Consultado el 27 de diciembre de 2023, URL: <https://dle.rae.es/interceptar>
- _____ (2023). Usar. Versión Electrónica de la 23ª edición del Diccionario de la lengua española. Consultado el 27 de diciembre de 2023, URL: <https://dle.rae.es/usar>
- Roxin, C. (1997). *Derecho Penal. Parte General Tomo I, Fundamentos de la Estructura de la Teoría del Delito*. 2da. Edición corregida. Madrid, España: Civitas, S.A.
- Welzel, H. (1956). *Derecho Penal. Parte General*. Buenos Aires: Argentina: Roque Delpama Editor.