Crítica y Derecho
Revista Jurídica

e-ISSN 2737-6281 / p-ISSN 2737-629X
https://revistadigital.uce.edu.ec/index.php/criticayderecho/issue/view/297

Desafíos contemporáneos del derecho y la democracia

La funcionalidad informática como objeto de tutela penal: bases dogmáticas para la comprensión del bien jurídico en los delitos informáticos

The Functionality of Information Systems as an Object of Criminal-Law Protection: Dogmatic Foundations for Understanding the Legally Protected Interest in Computer Offences

Jonathan Marcelo Ramos Mera
Asociación Académica Ecuatoriana de Derecho e Informática. Ecuador.
marcefer1@live.com.ar
https://orcid.org/0009-0004-0787-5720

https://doi.org/10.29166/cyd.v7i13.10451
Recibido: 2026-03-02 / Aceptado: 2026-05-15 / Publicado: 2026-07-15

RESUMEN

El bien jurídico en este tipo de infracciones penales encuentra su fundamento en la norma constitucional, en cuanto constituye un criterio de legitimación y, al mismo tiempo, un límite del ius puniendi. A partir de esta premisa, el trabajo examina críticamente la tesis según la cual la ley penal no protege de manera inmediata bienes jurídicos, sino que reacciona frente a su lesión o puesta en peligro. Sobre esa base, se revisan las principales posturas doctrinales que sitúan el bien jurídico, ya sea en la confianza en el funcionamiento de los sistemas, ya sea en la información considerada en abstracto, concluyéndose que ambas formulaciones resultan insuficientes para explicar con precisión la estructura de estas figuras penales. Frente a ello, se propone identificar como objeto de tutela penal la funcionalidad de los sistemas de información y comunicación, entendida como el conjunto de condiciones que permiten su operatividad segura, íntegra, disponible y reservada. Esta propuesta se contrasta con diversos tipos penales del catálogo punitivo ecuatoriano y permite ofrecer una base dogmática unitaria para la comprensión de estos delitos.

Palabras Claves: bien jurídico, funcionalidad de los sistemas, delitos informáticos, derecho penal informático, tutela penal.

ABSTRACT

The legally protected interest in this category of criminal offences finds its basis in the constitutional norm, insofar as it constitutes both a criterion for legitimising and a limit upon the ius puniendi. On that premise, the article critically examines the thesis according to which criminal law does not provide immediate protection to legally protected interests, but rather reacts to their injury or endangerment. Against that background, it reviews the principal doctrinal positions that locate the legally protected interest either in trust in the functioning of systems or in information considered in the abstract, concluding that both formulations are insufficient to explain with precision the structure of these criminal offences. It therefore proposes identifying as the object of criminal-law protection the functionality of information and communication systems, understood as the set of conditions that allow for their secure, integral, available, and access-restricted operation. This proposal is tested against various offences within the Ecuadorian penal framework and makes it possible to offer a unitary dogmatic basis for understanding these offences**.**

Keywords: legally protected interest, system functionality, computer offences, computer criminal law, criminal-law protection.

INTRODUCCIÓN

La expansión del ecosistema digital ha transformado de manera profunda las formas de interacción social, económica, institucional y comunicacional, pero también ha complejizado los presupuestos clásicos de imputación jurídica. En este contexto, uno de los problemas dogmáticos más relevantes consiste en determinar cuál es el bien jurídico comprometido en los delitos informáticos, particularmente cuando las conductas típicas no se proyectan exclusivamente sobre intereses tradicionales, como el patrimonio, la intimidad o la fe pública, sino también sobre condiciones estructurales de funcionamiento del entorno tecnológico. La cuestión no es menor, pues de su adecuada delimitación dependen tanto la legitimidad material de la incriminación como la correcta interpretación de los tipos penales, la fijación de sus contornos lesivos y la preservación del carácter fragmentario del derecho penal. Desde esta perspectiva, el problema que aborda este trabajo se sitúa en la ausencia de una construcción dogmática suficientemente unitaria y precisa acerca del bien jurídico en los delitos contra la seguridad de los activos de los sistemas de información y comunicación.

El bien jurídico constituye una categoría central de la dogmática penal, en la medida en que permite identificar el interés o valor socialmente relevante que justifica la intervención del derecho penal frente a determinadas conductas. No se trata únicamente de un concepto descriptivo, sino de un criterio material de legitimación del poder punitivo, pues delimita

aquello que el Estado puede proteger mediante la amenaza de una pena. Desde esta perspectiva, el bien jurídico cumple una función de garantía: impide que la criminalización se fundamente en meras razones morales, simbólicas, administrativas o de conveniencia política, y exige que toda figura penal se vincule con la protección de intereses constitucionalmente relevantes.

El estudio parte de una premisa básica: el bien jurídico penal no puede desvincularse del mandato constitucional, en tanto constituye un criterio de legitimación y, al mismo tiempo, un límite del ius puniendi. Ello obliga a examinar críticamente la conocida afirmación según la cual la ley penal no protege bienes jurídicos de manera inmediata, sino que reacciona frente a su lesión o puesta en peligro. Sobre esa base, el objetivo central de este artículo es determinar, desde una perspectiva dogmática, constitucional y sistemática, cuál es el objeto de tutela penal que permite dotar de coherencia material a los delitos informáticos. El artículo busca establecer si dicho referente debe situarse en la confianza en el funcionamiento de los sistemas, en la información considerada en abstracto o, más precisamente, en la funcionalidad de los sistemas de información y comunicación como presupuesto de su desenvolvimiento regular, seguro e íntegro.

La importancia del tema radica en que la expansión de la criminalidad informática ha puesto en evidencia la insuficiencia de ciertas categorías tradicionales cuando se trasladan sin matices al entorno digital. La utilidad de este artículo de revisión dogmática es, por ello, doble. En el plano teórico, contribuye a precisar el fundamento material de la intervención penal en un ámbito caracterizado por la concurrencia de bienes jurídicos y por una frecuente confusión entre delitos cometidos mediante tecnologías y delitos que recaen directamente sobre sistemas, datos o procesos digitales. En el plano práctico, ofrece un criterio de interpretación relevante para la lectura sistemática de los tipos penales del catálogo punitivo ecuatoriano, evitando construcciones excesivamente amplias o difusas que podrían debilitar las exigencias de taxatividad, lesividad y proporcionalidad. Su relevancia actual se explica, además, porque la creciente dependencia social e institucional respecto de infraestructuras digitales exige categorías dogmáticas capaces de comprender con mayor precisión el desvalor específico de las conductas que comprometen su operatividad.

Para desarrollar esta propuesta, el trabajo se apoya en una revisión bibliográfica centrada en la doctrina penal que ha discutido el bien jurídico en los delitos informáticos, tanto en sus formulaciones más amplias como en aquellas orientadas a identificar un interés específicamente informático. Esa revisión incluye, de una parte, las posturas que sitúan el bien jurídico en la confianza en el funcionamiento de los sistemas informatizados y, de otra, aquellas que lo identifican con la información como nuevo objeto de tutela. Del mismo modo, se incorpora el examen de aportes doctrinales que han propuesto la funcionalidad informática como categoría capaz de explicar el injusto propio de estas infracciones. Esta revisión teórica se articula con el análisis de la sistemática del Código Orgánico Integral Penal, con la referencia a la estructura del Convenio de Budapest y con la consideración del marco constitucional ecuatoriano, así como con pronunciamientos jurisprudenciales relevantes sobre la función legitimadora del bien jurídico en el derecho penal.

En este punto, resulta necesario precisar que el Convenio de Budapest, formalmente denominado Convenio sobre la Ciberdelincuencia, tiene su origen en el Consejo de Europa y fue abierto a la firma en Budapest el 23 de noviembre de 2001. En el caso ecuatoriano, el Estado depositó su instrumento de adhesión el 12 de diciembre de 2024, fecha en la que el Consejo de Europa registró la incorporación de Ecuador como Estado Parte; sin perjuicio de que su entrada en vigor para el país se produjo el 1 de abril de 2025. Este instrumento internacional regula, principalmente, la tipificación de conductas que afectan la confidencialidad, integridad y disponibilidad de los sistemas, redes y datos informáticos; establece herramientas procesales para la obtención, preservación y tratamiento de evidencia digital; y prevé mecanismos de cooperación internacional para la investigación y persecución penal de delitos cometidos mediante o contra sistemas informáticos.

En ese horizonte, y a partir de la articulación entre la doctrina penal, la sistemática del Código Orgánico Integral Penal y los estándares internacionales derivados del Convenio de

Budapest, particularmente aquellos referidos a la confidencialidad, integridad y disponibilidad de los sistemas y datos informáticos, la tesis que se sostiene es que ni la confianza en el funcionamiento de los sistemas ni la información considerada en abstracto permiten, por sí solas, explicar con suficiente precisión dogmática la estructura de estas figuras penales. Frente a ello, se propone reconocer como objeto de tutela penal la funcionalidad de los sistemas de información y comunicación, entendida como el conjunto de condiciones que hacen posible su operatividad regular, segura, íntegra, disponible y jurídicamente controlada. Esta construcción permite dotar de coherencia material a los delitos informáticos, armonizar su interpretación con los compromisos internacionales asumidos por el Estado ecuatoriano y, al mismo tiempo, preservar las exigencias constitucionales de lesividad, proporcionalidad y mínima intervención penal, sin desconocer su eventual carácter pluriofensivo ni la concurrencia de otros bienes jurídicos tradicionales afectados en cada caso

Bien jurídico y mandato constitucional en el ecosistema digital

El bien jurídico constante en los diferentes tipos penales del catálogo punitivo parte de la derivación de la Constitución de la República del Ecuador, esto sucede porque el concepto de: "(…) bien jurídico vinculante político criminalmente sólo se puede derivar de los cometidos, plasmados en la Ley Fundamental, basado en la libertad del individuo, a través de los cuales se le marcan sus límites a la potestad punitiva del Estado". [1]

La doctrina sobre los bienes jurídicos establece:

> (…) los bienes jurídicos son circunstancias dadas o finalidades que son útiles para el individuo y su libre desarrollo en el marco de un sistema social global estructurado sobre la base de esa concepción de los fines o para el funcionamiento del propio sistema. [2]

La Corte Nacional de Justicia ha señalado en su sentencia de 01 de septiembre de 2022, dentro del Juicio No. 19303-2019-00328, al respecto, lo siguiente:

> "(…) el bien jurídico es un reflejo de la realidad materia e inmaterial que se vive, por lo que se define en función de cada ilícito considerado como tal en el catálogo de normas dispositivas del ordenamiento jurídico penal." [3]

La Corte Constitucional del Ecuador sobre este concepto de bien jurídico, ha manifestado:

> "35.- (…) se entienda como tal un derecho o un principio de rango constitucional. En este sentido, el bien jurídico es un dique más para limitar el poder punitivo estatal. Permitir que la justicia penal opere, o sea que el mecanismo más violento permitido del Estado entre en funcionamiento, tendría legitimidad si se lo hace cuando se han vulnerado derechos y principios reconocidos constitucionalmente. 36.- La Función Legislativa no tendría legitimidad para crear cualquier tipo penal si es que no hay un bien jurídico reconocido constitucionalmente."[4]

[1] Claus Roxin, Derecho penal. Parte general. Tomo I: Fundamentos. La estructura de la teoría del delito, trad. Diego-Manuel Luzón Peña, Miguel Díaz y García Conlledo y Javier de Vicente Remesal, 1.ª ed. (Madrid: Civitas, 1997), 55

[2] Claus Roxin, Derecho penal. Parte general. Tomo I: Fundamentos. La estructura de la teoría del delito, trad. Diego-Manuel Luzón Peña, Miguel Díaz y García Conlledo y Javier de Vicente Remesal, 1.ª ed. (Madrid: Civitas, 1997),56

[3] Corte Nacional de Justicia del Ecuador, Sala Especializada de lo Penal, Penal Militar, Penal Policial, Tránsito, Corrupción y Crimen Organizado, Juicio No. 19303-2019-00328, sentencia de 1 de septiembre de 2022, jueza ponente Daniella Camacho Herold.

[4] Corte Constitucional del Ecuador, Sentencia No. 34-19-IN/21 y acumulados, 28 de abril de 2021, pp. 35-36. Voto Concurrente Juez Constitucional Ramiro Ávila Santamaria.

En esta sentencia es importante rescatar entre los párrafos 33 y 34, la siguiente frase en relación al bien jurídico: *"La ley penal no protege bienes jurídicos".* [5]

La afirmación según la cual *"la ley penal no protege bienes jurídicos"* puede resultar, en una primera aproximación, provocadora; sin embargo, contiene una precisión dogmática relevante. En efecto, si se parte de que el derecho penal no actúa de manera originaria como mecanismo general de prevención, sino como una forma de reacción institucional frente a conductas que ya han lesionado o puesto en peligro un interés jurídicamente relevante, entonces no es técnicamente exacto atribuirle, en sentido estricto, una función de protección inmediata del bien jurídico. La intervención penal presupone, más bien, la constatación de un ataque relevante contra ese bien, de modo que su actuación no se agota en "proteger", sino en reaccionar sancionatoriamente frente a la lesión o puesta en peligro jurídicamente intolerable.

Desde esa perspectiva, la expresión "protección de bienes jurídicos" debe ser entendida con cautela. En sentido dogmático estricto, el derecho penal no protege bienes jurídicos de la misma manera en que lo hacen otros sectores del ordenamiento mediante mecanismos de organización, prevención o control. Su función específica consiste en tipificar y sancionar aquellas conductas que lesionan o amenazan de forma relevante determinados intereses valorados por el ordenamiento. Por ello, resulta más preciso afirmar que el bien jurídico cumple en derecho penal una función de referente material de la incriminación y de criterio de legitimación del ius puniendi, antes que una función de protección directa en sentido preventivo.

En consecuencia, la tesis aquí acogida coincide con la idea de que el derecho penal se activa una vez que el bien jurídico ha sido lesionado o puesto en peligro de forma jurídicamente relevante, de modo que su lógica estructural es predominantemente reactiva y no preventiva.

Precisado lo anterior, corresponde identificar el fundamento constitucional de los bienes jurídicos involucrados en los delitos contra la seguridad de los activos de los sistemas de información y comunicación.

La Constitución de la República del Ecuador, determina el derecho de todas las personas al acceso universal a las tecnologías de información y comunicación (TIC)6. En ese sentido, es deber estatal el garantizar una seguridad integral que haga posible un acceso efectivo y seguro. Este derecho está reconocido expresamente por la Constitución al consagrar el acceso universal a las (TIC) como una manifestación del derecho a la comunicación, lo que coloca a la conectividad y a la inclusión digital en la esfera de protección constitucional directa.

Ahora bien, el mandato de acceso no puede leerse aislado del mandato de seguridad. La carta fundamental impone al Estado el deber de garantizar a sus habitantes una cultura de paz y "seguridad integral", lo cual, aplicado al entorno digital, se traduce en evitar que el mismo elemento que habilita derechos (las TIC) se convierta en un medio de lesión a bienes jurídicos personales y colectivos (patrimonio, intimidad, seguridad pública, información, seguridad y funcionalidad de los sistemas, etc.).

A partir de este punto, el análisis se torna particularmente complejo, pues en materia de delitos informáticos no existe uniformidad dogmática al momento de identificar un único bien jurídico común a todas las figuras que integran este ámbito. Aunque el fundamento constitucional previamente señalado remite de manera directa al acceso a las tecnologías de la información y comunicación y a la exigencia de un entorno digital seguro, ello no resuelve por sí solo la cuestión relativa al interés jurídicamente relevante que, en términos penales, justifica la incriminación de estas conductas.

La dificultad se explica, en buena medida, porque en esta clase de infracciones convergen y pueden verse comprometidos diversos intereses individuales y colectivos. Según

[5] Corte Constitucional del Ecuador, Sentencia No. 34-19-IN/21 y acumulados, 28 de abril de 2021, pp. 33-34. Voto Concurrente Juez Constitucional Ramiro Ávila Santamaria.
[6] Ecuador, Constitución de la República del Ecuador, Registro Oficial 44, 20 de octubre de 2008. Artículo 16.

el caso, la conducta puede proyectarse sobre el patrimonio, la información, la intimidad, la privacidad, la integridad personal en determinadas manifestaciones, la seguridad pública o incluso sobre condiciones básicas de funcionamiento de la infraestructura tecnológica. De ahí que no resulte extraño advertir en muchos supuestos una estructura pluriofensiva, en la que la conducta lesiona o pone en peligro, de manera simultánea, más de un bien jurídico.

Sin embargo, el problema dogmático central no radica únicamente en constatar esa eventual pluriofensividad, sino en determinar si, más allá de los bienes jurídicos tradicionales que puedan verse concurrentemente afectados, existe un bien jurídico propio o preponderante que permita dotar de unidad sistemática a los delitos informáticos. En este punto surge precisamente la discusión acerca de si ese referente material debe ubicarse en la seguridad de los sistemas, en la información como objeto de tutela, o en atributos funcionales más específicos, como la confidencialidad, integridad, disponibilidad o accesibilidad de los sistemas y de los datos.

Por ello, el presente artículo no parte de afirmaciones categóricas ni de una identificación apriorística del bien jurídico, sino de aproximaciones sucesivas dirigidas a delimitar con mayor precisión este problema. El objetivo es establecer en qué medida las infracciones analizadas responden a la tutela de un interés tecnológico-funcional propio y en qué medida, al mismo tiempo, coexisten con bienes jurídicos tradicionales cuya lesión o puesta en peligro también se hace presente en el caso concreto.

Un primer paso metodológico indispensable consiste en precisar a qué llamamos “delitos informáticos”. La expresión suele emplearse en sentido amplio para abarcar cualquier conducta delictiva cometida mediante tecnologías digitales o que recaiga sobre ellas; sin embargo, una construcción dogmática más rigurosa exige restringir inicialmente el análisis a aquellas infracciones en las que el componente informático no es un mero medio accidental, sino el núcleo del injusto. Desde esa perspectiva, interesa distinguir entre los delitos comunes cometidos por medio de sistemas informáticos y aquellos en los que la afectación recae precisamente sobre la esfera de seguridad, funcionamiento o fiabilidad del entorno digital.

Esta precisión resulta especialmente relevante en el caso ecuatoriano, porque el Código Orgánico Integral Penal, contiene un capítulo específico denominado: “Delitos contra la seguridad de los activos de los sistemas de información y comunicación”, lo que revela una opción legislativa por agrupar determinadas conductas bajo una lógica material propia. Esa técnica de sistematización responde, al menos en parte, a la estructura del Convenio de Budapest, cuyo capítulo II, sección 1, diferencia, por un lado, los delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos y, por otro, los llamados delitos informáticos, entre los que figuran la falsificación y el fraude informáticos[7].

Bajo esa referencia, cabe sostener que, para los fines de este artículo, el punto de partida no debe situarse en cualquier infracción con componente tecnológico, sino en aquellas figuras del catálogo ecuatoriano que conservan una vinculación directa con ese núcleo informático delineado por el Convenio de Budapest. En otras palabras, el análisis del bien jurídico ha de concentrarse, ante todo, en los delitos que recaen sobre datos, sistemas, comunicaciones o procesos digitales y que, por ello, parecen expresar de manera más nítida un interés de tutela específicamente informático, aun cuando todavía no se haya precisado con exactitud su contenido dogmático.

La propia sistemática del Código Orgánico Integral Penal ofrece un primer punto de partida para la delimitación del bien jurídico en esta materia. En efecto, el legislador ha ubicado estas figuras bajo la denominación de “delitos contra la seguridad de los activos de los sistemas de información y comunicación”[8], lo que permite advertir, al menos en una primera aproximación, que la unidad de sentido no se construye de manera directa a bienes

[7] Budapest, Convenio sobre la Ciberdelincuencia, Consejo de Europa, 23 de noviembre del 2001. Art. 2, 3, 4, 5, 6, 7 y 8.

[8] Ecuador, Código Orgánico Integral Penal, Registro Oficial 180, Suplemento, 10 de febrero del 2014, Art. 229 a 234.4.

jurídicos clásicos como el patrimonio, la intimidad, la fe pública, sino alrededor de un interés de naturaleza más amplia vinculado a la seguridad de los activos informáticos. [9]

Desde esa perspectiva, cabría sostener preliminarmente que el legislador ha querido reconocer en este ámbito un bien jurídico de carácter supraindividual, en tanto presupuesto necesario para el desenvolvimiento confiable, seguro y regular de las tecnologías de la información y comunicación.

La referencia legislativa a la "seguridad de los activos" constituye una pauta interpretativa relevante, pero todavía requiere ser precisada en su contenido material. En efecto, resta determinar si esa seguridad debe entenderse como tutela de los datos en sí mismos, de los sistemas como estructuras funcionales, de sus atributos de confidencialidad, integridad y disponibilidad, o de un concepto más amplio vinculado al funcionamiento mismo del ecosistema digital.

En conexión con lo anterior, una parte de la doctrina ha sostenido que el bien jurídico comprometido en esta clase de infracciones no radica exclusivamente en la seguridad de los sistemas, sino en la confianza que la sociedad deposita en su funcionamiento. Desde esta perspectiva, la relevancia penal de estas conductas surgiría de su aptitud para afectar la credibilidad, fiabilidad y previsibilidad de los sistemas de información y comunicación como soportes de interacción social, económica e institucional. Así, la seguridad no aparecería como un valor aislado, sino como el presupuesto técnico que hace posible esa confianza colectiva en el entorno digital, de modo que la lesión a los activos informáticos comprometería, al mismo tiempo, la expectativa social de que tales sistemas operen de forma estable, íntegra y segura.

La doctrina reconoce a este bien jurídico en este tipo de delitos bajo los siguientes términos:

> "(…) la confianza en el funcionamiento de los sistemas informatizados", como interés de carácter supraindividual –colectivo–. Se parte de que el buen funcionamiento de los sistemas es condición indispensable para el normal desarrollo de las relaciones económicas y personales de nuestros días, porque de ello depende que no se colapsen las actividades del mundo bancario, bursátil, de seguros, transportes, gestión tributaria, Seguridad Social, sanitario (…)[10]

Sin perjuicio de aquello la propia doctrina hace una crítica a este aspecto señalando que:

> Por una parte, el Derecho penal solo puede proteger algo que (ya) existe, lo que excluiría la confianza que se verifica porque así lo dispone una norma jurídica. Por otra parte, la confianza en la conducta de otras personas sería una mera suposición acerca de cómo se espera que ellas se comporten, lo que llevado a los delitos informáticos equivaldría a decir que su bien jurídico es la expectativa de operatividad de los sistemas informáticos. A ello se agrega que la confianza en el sistema en este caso informático no se ve afectada por la comisión de un delito; por el contrario, su afectación se produciría por la ausencia de sanciones tras la realización de comportamientos delictivos. [11]

La tesis que ubica el bien jurídico de estas infracciones en la confianza en el funcionamiento de los sistemas informáticos presenta, sin duda, una intuición relevante: pone de manifiesto que la criminalidad informática no incide únicamente sobre intereses individuales aislados,

[9] Ecuador, Estrategia para el fomento del desarrollo y uso ético y responsable de la inteligencia artificial en el Ecuador, Registro Oficial Suplemento 206, 19 de enero del 2026. Seguridad de la información: Conjunto de medidas preventivas y reactivas de las instituciones y de los sistemas tecnológicos que permiten la preservación de la confidencialidad, integridad y disponibilidad de la información.

[10] Mirentxu Corcoy Bidasolo, "Problemática de la persecución penal de los denominados delitos informáticos: particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos", *Eguzkilore*, n.º 21, 2007, 10

[11] Laura Mayer Lux, "El bien jurídico protegido en los delitos informáticos", *Revista Chilena de Derecho*, vol. 44, n.º 1, 2017, 243.

sino también sobre condiciones generales de desenvolvimiento social en entornos digitales. En ese sentido, resulta comprensible que parte de la doctrina haya querido destacar la dimensión supraindividual de estos delitos, especialmente en contextos en los que la operatividad de sistemas bancarios, bursátiles, sanitarios, tributarios o de comunicaciones se ha vuelto indispensable para el desarrollo ordinario de la vida contemporánea.

Sin embargo, la confianza en el funcionamiento de los sistemas no constituye, en sentido estricto, el bien jurídico más adecuado para explicar estas infracciones. Se trata de una expectativa social de regularidad y previsibilidad, pero no de una realidad directamente lesionable por la conducta típica. Por ello, su utilización como objeto de tutela puede generar un nivel excesivo de abstracción y debilitar las funciones de delimitación, interpretación y legitimación propias del bien jurídico penal. La confianza puede verse afectada como consecuencia del delito, pero no representa necesariamente el interés inmediato protegido. En consecuencia, el referente dogmático más preciso no es la confianza, sino la funcionalidad regular, segura, íntegra y disponible de los sistemas de información y comunicación.

Adicional a las concepciones expuestas, existen otros autores que señalan que el bien jurídico en este tipo de delitos, es la información, y al respecto han dicho:

> En nuestra opinión, consideramos que debe ser la información un nuevo bien jurídico protegido, como un bien intangible, pero de claro valor en nuestra "sociedad de la información". Sin embargo, debemos puntualizar qué tipo de información deberemos proteger. ¿Es cualquier tipo de información susceptible de recibir el resguardo del arma más dura que tiene el derecho, el sistema penal? Opinamos que no, que no cualquier información debería ser protegida, o para ser más preciso, no cualquier aspecto de la información debería ser protegido[12].

Desde esta perspectiva, la doctrina citada erige a la información como nuevo bien jurídico protegido en este tipo de delitos. Esta percepción es válida para describir de manera amplia el fenómeno de la criminalidad informática o para explicar elementos normativos centrados en la confidencialidad, integridad y disponibilidad de datos; sin embargo, no ofrece por sí sola una respuesta satisfactoria para delitos que, como el previsto en el artículo 232 de la norma penal, están estructurados sobre la interferencia del sistema y no sobre el dato como objeto autónomo de lesión. De ahí que la formulación dogmáticamente más precisa no deba centrarse en la "información" sin más, sino en la seguridad del activo informático y en la integridad funcional del sistema que hace posible el tratamiento, transmisión y recepción de esa información.

En ese sentido, la información puede ocupar en estos supuestos un lugar jurídicamente relevante, pero no necesariamente como bien jurídico principal del tipo. En el ataque a la integridad de sistemas informáticos, el dato o el contenido digital aparecen más bien como componentes funcionalmente vinculados al sistema: pueden ser el medio a través del cual se produce la afectación, o uno de los intereses que resultan ulteriormente comprometidos cuando el sistema es degradado o paralizado.

La información, en cuanto objeto de protección jurídica, ya tiene cabida en delitos tradicionales o en figuras de contenido diverso, como aquellos relativos a la revelación de secretos, la afectación de datos personales o la divulgación de información reservada. En cambio, por ejemplo, en el artículo 232 del Código Penal, el problema no radica en la mera existencia de información valiosa ni en su sola alteración, sino en la afectación grave del entorno sistémico que sostiene su circulación y procesamiento. Por eso, cuando el Convenio de Budapest distingue entre ataque a los datos y ataque al sistema, ofrece una clave dogmática decisiva, sin embargo, recordemos que el artículo 232 ecuatoriano se alinea principalmente con la segunda lógica. En consecuencia, el bien jurídico no debe formularse

[12] Marcelo Temperini, "Delitos informáticos y cibercrimen: alcances, conceptos y características", en la obra: *Cibercrimen y delitos informáticos: Los nuevos tipos penales en la era de internet*, comp. Ricardo Antonio Parada y José Daniel Errecaborde, 1.ª ed. (Ciudad Autónoma de Buenos Aires: Erreius, 2018), 60.

como la información en abstracto, sino como la seguridad e integridad funcional del sistema informático como activo tecnológico.

Por lo argumentado hasta este momento, se puede sostener, sin más, que: anclar a "la información" como bien jurídico propio de estos delitos, termina por diluir la especificidad del injusto informático y por oscurecer la frontera entre figuras que protegen el dato y figuras que protegen el sistema.

En el marco del tipo penal de ataque a la integridad de sistemas informáticos, por ejemplo, la información podrá ser un interés concurrente, mediato o incluso ulteriormente afectado, pero el núcleo de tutela permanece anclado en la funcionalidad segura del sistema.

Dentro del conjunto de delitos contra la seguridad de los activos de los sistemas de información y comunicación tipificados en el Código Orgánico Integral Penal, no solo el artículo 232 permite afirmar que el sistema ocupa el lugar central de tutela penal. También podemos referirnos al artículo 234, relativo al acceso no consentido a sistemas informáticos, telemáticos o de telecomunicaciones, con una construcción semejante, aunque desde una lógica distinta. Mientras el artículo 232 protege la integridad funcional del sistema frente a su obstaculización grave, el artículo 234 protege el sistema en su dimensión de reserva, control de acceso y exclusión frente a terceros no autorizados. En ambos casos, la información puede resultar comprometida, expuesta o ulteriormente lesionada, pero no constituye el eje inmediato del injusto, pues la lesión primaria recae sobre el sistema como ámbito tecnológico jurídicamente delimitado.

En una primera dimensión, el artículo 234 del Código Orgánico Integral Penal, puede vincularse con la característica de confidencialidad, en cuanto protege la reserva del sistema frente al acceso de terceros no autorizados.[13]

Desde esta perspectiva, el injusto típico se configura cuando se quiebra la expectativa legítima de que el entorno informático permanezca cerrado o restringido para quienes carecen de autorización de ingreso. No obstante, la tutela no se agota en la confidencialidad entendida como secreto de la información, pues el precepto protege además el control de acceso al sistema mismo, esto es, la facultad del titular de excluir a terceros y mantener bajo su dominio el ingreso, permanencia e interacción dentro de ese espacio tecnológico.

El delito de acceso no consentido, no debe interpretarse como una figura centrada en el dato o en el contenido alojado en el sistema, sino como un tipo cuyo núcleo se agota, en lo esencial, en la ruptura ilegítima de la barrera de acceso. Su consumación no exige daño, sustracción, alteración o difusión de información; basta el ingreso o la permanencia sin autorización para que el desvalor típico se perfeccione. Precisamente por ello, la información aparece aquí en un plano consecuencial: puede ser el objeto ulterior de otros comportamientos, pero la razón inmediata de tutela penal es la preservación del sistema como espacio de acceso reservado bajo control de su titular legítimo.

Es por ello, que en esta clase de infracciones puede afirmarse la coexistencia de un bien jurídico propiamente informático, junto con la eventual afectación de otros bienes jurídicos que se proyectan de manera concurrente o ulterior. La estructura de estos delitos revela, en tal sentido, un marcado carácter pluriofensivo, pues la intrusión o el ataque al sistema no agotan necesariamente su desvalor en la sola lesión del activo informático, sino que pueden extender sus efectos a intereses adicionales, como la información allí alojada o tratada, el patrimonio, la propiedad, la intimidad, la confidencialidad de las comunicaciones e incluso la continuidad de actividades económicas o institucionales que dependen de la operatividad del entorno digital.

[13] Ecuador, Asamblea Nacional, *Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad*, texto aprobado en segundo debate, 10 de febrero de 2026, art. 20-B, lit. a); Presidencia de la República del Ecuador, *Objeción parcial por inconveniencia al referido proyecto*, Oficio No. T.368-SGJ-26-0061, 12 de marzo de 2026; Asamblea Nacional, allanamiento a la objeción parcial y remisión al Registro Oficial para publicación, 31 de marzo de 2026. Reforma agregada a la Ley Orgánica de Transformación Digital y Audiovisual, Registro Oficial 689, Tercer Suplemento, 7 de febrero del 2023. Confidencialidad. - Garantizar que los datos, sistemas y activos digitales sean accesibles únicamente por personas, entidades o sistemas autorizados, evitando divulgaciones, accesos o exposiciones indebidas.

La propia doctrina al respecto en estos delitos reconoce que:

> "(…) el bien jurídico protegido en el delito informático será aquél protegido en el delito que presuntamente se ha realizado: patrimonio, Hacienda Pública…"[14]

Frente a la tesis doctrinal conforme a la cual el delito informático no constituye una categoría autónoma, sino una mera modalidad de realización de delitos tradicionales, cabe sostener críticamente que dicha concepción conduce, en términos lógicos, a negar la existencia de un bien jurídico propiamente informático.

Actualmente determinadas legislaciones han optado por ampliar el concepto de ciberdelincuencia más allá de los ataques estrictamente dirigidos contra sistemas o datos, para incluir también delitos tradicionales cuando son cometidos por, a través de o con el uso de tecnologías de la información y comunicación. El caso de Filipinas resulta especialmente ilustrativo:

> En Filipinas, la Ley de Prevención contra la Ciberdelincuencia de 2012, Ley de la República Nro. 10175 (RA10175) tiene una disposición específica que clasifica los delitos definidos en el Código Penal Revisado (una ley de 1930) y leyes especiales que, si se cometen con el uso de las TIC, se consideran delitos cibernéticos y se castigan con penas un grado más altas que las penas definidas en el Código Penal Revisado.[15]

Una opción legislativa de esta naturaleza no está exenta de objeciones dogmáticas. Si se lleva hasta sus últimas consecuencias, corre el riesgo de disolver la especificidad del bien jurídico propiamente informático, pues la tecnología deja de operar como ámbito material autónomo de tutela y pasa a funcionar, casi exclusivamente, como un factor de agravación o de extensión del injusto de delitos ya conocidos.

Sin embargo, esta crítica no exige desconocer que una agravación de este tipo pueda resultar proporcional en determinados supuestos. En efecto, hay delitos en los que el uso de TIC incrementa objetivamente el desvalor de acción y de resultado, ya sea por la escala masiva de afectación, la velocidad de ejecución, el anonimato, la automatización, la capacidad de replicación o la ampliación exponencial del universo de víctimas. En tales casos, el recurso a la tecnología sí puede justificar una respuesta penal más intensa. Pero una cosa es reconocer ese plus de desvalor en ciertos tipos y otra, muy distinta, es convertir toda utilización tecnológica en razón suficiente para absorber el fenómeno dentro de una categoría indiferenciada de ciberdelincuencia. La primera opción responde a exigencias de proporcionalidad; la segunda, en cambio, amenaza con borrar la frontera entre los delitos en que la tecnología es solo medio y aquellos en los que el sistema mismo constituye el centro del injusto y, por tanto, del bien jurídico tutelado

La funcionalidad informática como objeto de tutela en este tipo de infracciones penales

A partir de lo analizado se advierte, que la confianza no constituye un referente dogmáticamente suficiente para erigirse en bien jurídico inmediato de estas infracciones, pues remite más bien a una expectativa social acerca del comportamiento regular del sistema que a una realidad material susceptible de lesión directa. En segundo lugar, tampoco la información, considerada en abstracto, permite ofrecer una formulación satisfactoria y unitaria del bien jurídico, ya que en numerosos supuestos su afectación aparece de modo concurrente, mediato o ulterior, sin coincidir necesariamente con el núcleo del injusto típico.

[14] Mirentxu Corcoy Bidasolo, "Problemática de la persecución penal de los denominados delitos informáticos: particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos", *Eguzkilore*, n.º 21, 2007, 10

[15] Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), *Ciberdelito I: Guía práctica para un abordaje integral del fenómeno. Tipos generales. Marco jurídico y derechos humanos. El ABC de la investigación*, 1.ª ed., revisión y adaptación de la Oficina de Análisis Estratégico contra la Criminalidad (OFAEC), marzo de 2022, 40.

Por ello, la delimitación del bien jurídico en los delitos contra la seguridad de los activos de los sistemas de información y comunicación exige desplazar el análisis hacia aquello que resulta inmediatamente comprometido por la conducta: la funcionalidad propia del sistema como presupuesto de su desenvolvimiento regular en el entorno digital.

Desde esta perspectiva, la seguridad del sistema no debe entenderse como un bien jurídico autónomo y aislado, sino como la condición general que preserva esa funcionalidad. A su vez, la confidencialidad, integridad y disponibilidad, destacadas por el Convenio de Budapest, no operan necesariamente como bienes jurídicos independientes entre sí, sino como manifestaciones concretas o aristas funcionales de esa seguridad, en cuanto hacen posible el desarrollo correcto, estable y confiable del sistema y de los datos que en él se procesan. En consecuencia, el bien jurídico puede formularse, como la funcionalidad propia de los sistemas de información y comunicación, entendida como el conjunto de condiciones que garantizan su operatividad segura, íntegra y disponible.

En ese sentido, la formulación del bien jurídico en esta materia exige partir de una constatación básica: no toda afectación producida en el entorno digital recae inmediata y directamente sobre la información considerada en abstracto, ni sobre la confianza social depositada en los sistemas. En numerosos supuestos, aquello que resulta primariamente comprometido es la capacidad del sistema para operar conforme a su diseño, finalidad y reglas de acceso, tratamiento y circulación. Desde esta perspectiva, el eje de tutela no debe situarse en expectativas sociales o en el dato aislado, sino en la funcionalidad informática del sistema, entendida como la aptitud de este para desenvolverse de forma regular, segura y conforme a los parámetros que hacen posible su utilización legítima.

La funcionalidad informática, así entendida, no equivale a una mera operatividad mecánica o técnica del sistema. Se trata de una categoría dogmática integrada por las condiciones que permiten que los sistemas de información y comunicación procesen, almacenen, transmitan y resguarden datos de manera regular, segura, íntegra, disponible y jurídicamente controlada. Su afectación adquiere relevancia penal cuando la conducta compromete de forma no autorizada alguno de esos atributos esenciales, ya sea mediante la alteración, interrupción, degradación, acceso indebido, manipulación o supresión de datos, procesos o estructuras tecnológicas. En esa medida, la tutela penal no se dirige únicamente al contenido que circula dentro del sistema, sino al sistema mismo como infraestructura funcional que soporta relaciones sociales, económicas, institucionales y comunicacionales.

Ello no impide reconocer que, en muchos casos, estas infracciones tengan carácter pluriofensivo, pues junto a la funcionalidad informática pueden verse afectados otros bienes jurídicos como el patrimonio, la intimidad, la protección de datos personales o la fe pública. Precisamente por ello, la funcionalidad permite distinguir los delitos cometidos simplemente mediante tecnologías de la información y comunicación, en los que la tecnología opera como medio de ejecución, de los delitos propiamente dirigidos contra sistemas, datos o procesos digitales, en los que el desvalor específico recae sobre la estructura funcional del entorno informático.

Esta construcción permite explicar con mayor precisión la sistemática del capítulo del Código Orgánico Integral Penal relativo a los delitos contra la seguridad de los activos de los sistemas de información y comunicación. En efecto, lo que esas figuras revelan es una preocupación legislativa por preservar las condiciones de funcionamiento del entorno digital frente a accesos indebidos, ataques, interferencias, alteraciones o manipulaciones que comprometen su normal desarrollo.

Así, la seguridad no aparece como un bien jurídico separado de la funcionalidad, sino como la condición general que la preserva; y la confidencialidad, integridad y disponibilidad, como manifestaciones específicas de esa seguridad, en cuanto concurren en el mantenimiento del sistema como espacio funcionalmente apto y jurídicamente resguardado.[16]

[16]Ecuador, Asamblea Nacional, Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad, texto aprobado en segundo debate, 10 de febrero de 2026, art. 20-B, lit. a); Presidencia de la República del Ecuador, Objeción parcial por inconveniencia al referido proyecto,

Esta comprensión de este interés supraindividual tutelado, se verifica con particular nitidez en el delito de ataque a la integridad de sistemas informáticos. En esta infracción penal el legislador no castiga cualquier alteración del dato en sí mismo, sino la intervención dirigida a obstaculizar gravemente el funcionamiento del sistema.

Por ello, aun cuando la conducta típica incluya verbos como borrar, alterar, suprimir o deteriorar contenido digital, tales acciones solo adquieren relevancia penal en la medida en que se conectan con la afectación funcional del activo tecnológico.

En estas infracciones penales el desvalor típico no gira en torno al contenido informativo, sino a la quiebra del control de acceso y, con ello, a una dimensión esencial de la funcionalidad del sistema: su capacidad de operar como espacio reservado, bajo dominio del titular legítimo. En este punto, la confidencialidad aparece como una manifestación específica de la seguridad del sistema, en cuanto presupone que el entorno informático permanezca cerrado o restringido frente a terceros no autorizados. La barrera de acceso forma parte, por tanto, de la arquitectura funcional del sistema; si esta se rompe, el sistema deja de desenvolverse bajo las condiciones de seguridad, reserva y exclusión que le son propias.

El artículo 230 referente al delito de interceptación ilegal de datos, confirma igualmente esta tesis, aunque desde una técnica legislativa más heterogénea. En su numeral primero, la interceptación de contenido digital en tránsito compromete la funcionalidad del sistema de comunicación en su dimensión de confidencialidad: el canal deja de operar bajo las condiciones de reserva que lo hacen funcionalmente seguro para emisor y receptor. En los numerales segundo y tercero, cuando se diseñan o diseminan contenidos, enlaces, páginas o mecanismos destinados a inducir al usuario a ingresar a un sitio distinto del que pretende acceder, la afectación recae sobre la autenticidad funcional del acceso digital, sobre la fiabilidad de las rutas de navegación y de los mecanismos de autenticación.

En los numerales cuarto y quinto del referido delito, relativos a la clonación y facilitación de instrumentos para la clonación de tarjetas o medios de pago, la afectación a la funcionalidad del sistema no se presenta con la misma inmediatez que en los supuestos de ataque o acceso no consentido. En estos casos, el problema se ubica, de forma más directa, en la vulneración de la seguridad y autenticidad de los instrumentos electrónicos de pago y de los mecanismos de validación transaccional. La relevancia informática de la conducta radica en que la clonación permite introducir en el circuito operaciones aparentemente legítimas, alterando los procesos de identificación y autorización sobre los que descansa el sistema. Por ello, más que una lesión primaria a la operatividad general del sistema, lo que aquí se compromete de manera inmediata es la fiabilidad del entorno transaccional digital, sin perjuicio de que de ello puedan derivarse, ulteriormente, afectaciones patrimoniales y perturbaciones funcionales en el ecosistema de pagos.

En ese sentido, en todos estos casos pueden coexistir otros bienes jurídicos lesionados o puestos en peligro; sin embargo, lo que otorga unidad sistemática a estos delitos es que la conducta recae, de manera inmediata, sobre las condiciones que hacen posible el desenvolvimiento regular del sistema.

La doctrina respecto a este bien jurídico ha señalado que:

> La funcionalidad informática es un presupuesto para la realización de diversas actividades de gran relevancia para las personas y las instituciones que están a su

Oficio No. T.368-SGJ-26-0061, 12 de marzo de 2026; Asamblea Nacional, allanamiento a la objeción parcial y remisión al Registro Oficial para publicación, 31 de marzo de 2026, Artículo 20-B. Reforma agregada a la Ley Orgánica de Transformación Digital y Audiovisual, Registro Oficial 689, Tercer Suplemento, 7 de febrero del 2023. Confidencialidad. - Garantizar que los datos, sistemas y activos digitales sean accesibles únicamente por personas, entidades o sistemas autorizados, evitando divulgaciones, accesos o exposiciones indebidas. Integridad. - Asegurar que la información, los sistemas y los procesos digitales se mantengan completos, coherentes y sin alteraciones no autorizadas o accidentales, preservando su exactitud y fiabilidad. Disponibilidad. - Garantizar que los servicios, plataformas, sistemas y datos digitales estén accesibles y operativos cuando sean requeridos por usuarios autorizados, incluso en situaciones de contingencia o ataque.

> servicio en un Estado democrático de derecho. Esta, se identifica con aquel conjunto de condiciones que posibilitan que los sistemas informáticos realicen adecuadamente las operaciones de almacenamiento, tratamiento y transferencia de datos, dentro de un marco tolerable de riesgo. El reconocimiento de la funcionalidad informática como bien jurídico específico, propiamente informático, se justifica si los delitos informáticos, junto con incidir en el soporte lógico de un sistema informático, implican el uso de redes computacionales. En ese contexto, 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.[17]

Esta orientación doctrinal importante en la materia reconoce en la funcionalidad informática un bien jurídico específicamente propio de este ámbito, en cuanto presupuesto indispensable para el adecuado desenvolvimiento de las operaciones de almacenamiento, tratamiento, transferencia y control de datos en los sistemas de información y comunicación.

Esta formulación no solo permite captar con mayor precisión la especificidad del injusto informático, sino que además se ajusta a la sistemática del Código Orgánico Integral Penal, cuyo capítulo sobre delitos contra la seguridad de los activos de los sistemas de información y comunicación evidencia una opción legislativa dirigida a tutelar, de manera inmediata, las condiciones de operatividad del entorno digital. Bajo esta comprensión, la seguridad no constituye un bien jurídico autónomo separado de la funcionalidad, sino la condición general que la preserva; y, a su vez, la confidencialidad, integridad y disponibilidad deben entenderse como manifestaciones específicas de esa seguridad, en cuanto hacen posible el desenvolvimiento regular, reservado, íntegro y disponible del sistema y de los datos que en él se procesan.

Solo a partir de esta construcción resulta posible mantener la coherencia entre la estructura típica de estas infracciones, la ubicación sistemática que les ha dado el legislador ecuatoriano y la distinción dogmática entre la lesión inmediata al sistema y la eventual afectación concurrente o ulterior de otros bienes jurídicos tradicionales.

CONCLUSIONES

El bien jurídico en los delitos informáticos no puede construirse al margen del marco constitucional. En el contexto ecuatoriano, la Constitución no solo reconoce el acceso universal a las tecnologías de la información y comunicación, sino que exige que dicho acceso se desarrolle en condiciones de seguridad integral. De ello se desprende que el bien jurídico cumple una doble función: por un lado, actúa como criterio de legitimación material de la intervención penal; por otro, opera como límite del *ius puniendi*, al impedir la expansión de la criminalización hacia ámbitos carentes de un referente constitucionalmente relevante.

En este artículo se evidencia, asimismo, que la afirmación según la cual la ley penal no protege bienes jurídicos en sentido inmediato no debilita la teoría del bien jurídico, sino que la depura. El derecho penal no constituye el mecanismo originario de organización o aseguramiento de los intereses sociales, sino una forma de reacción institucional frente a lesiones o puestas en peligro jurídicamente intolerables. En esa medida, el bien jurídico no debe entenderse como objeto de una protección preventiva directa, sino como referente material de la incriminación y como criterio de legitimidad de la respuesta punitiva.

Desde esa base, el trabajo demuestra que las fórmulas que sitúan el bien jurídico, ya sea en la confianza en el funcionamiento de los sistemas, ya sea en la información considerada en abstracto, resultan insuficientes para explicar con precisión dogmática la estructura de estas infracciones. La confianza remite a una expectativa social demasiado abstracta y mediata para constituirse en objeto inmediato de tutela penal; la información, por

[17] Laura Mayer Lux, "El bien jurídico protegido en los delitos informáticos", *Revista Chilena de Derecho*, vol. 44, n.º 1, 2017, 255.

su parte, aunque jurídicamente relevante en múltiples supuestos, no permite diferenciar adecuadamente los delitos que recaen sobre datos de aquellos cuyo núcleo de injusto se proyecta directamente sobre el sistema, su operatividad y sus condiciones de funcionamiento.

En consecuencia, la categoría que ofrece mayor coherencia sistemática es la funcionalidad de los sistemas de información y comunicación. Esta debe entenderse como el conjunto de condiciones que hacen posible su desenvolvimiento regular, seguro, íntegro, disponible y jurídicamente controlado. Desde esta perspectiva, la seguridad no constituye un bien jurídico autónomo separado de la funcionalidad, sino la condición general que la preserva; a su vez, la confidencialidad, la integridad y la disponibilidad no actúan necesariamente como bienes independientes, sino como manifestaciones funcionales de esa misma tutela.

Esta formulación permite explicar con mayor precisión la sistemática del Código Orgánico Integral Penal y su conexión con la lógica del Convenio de Budapest. En efecto, los tipos relativos a interceptación ilegal de datos, ataque a la integridad de sistemas, acceso no consentido, transferencia electrónica de activo patrimonial y falsificación informática revelan, con diferentes intensidades y matices, que la lesión penalmente relevante recae de manera inmediata sobre condiciones estructurales del entorno digital. Incluso cuando concurren otros bienes jurídicos, como el patrimonio, la intimidad, la fe pública o la confidencialidad de las comunicaciones, la unidad se mantiene porque el núcleo del injusto continúa anclado en la afectación funcional del sistema o de las condiciones que hacen posible su operatividad confiable.

El análisis realizado permite afirmar, además, que la funcionalidad informática no excluye la pluriofensividad. Por el contrario, ofrece una concepción dogmática que permite reconocer la coexistencia de un bien jurídico propiamente informático con otros bienes jurídicos concurrentes o ulteriormente afectados. Esta constatación resulta especialmente importante para evitar dos errores frecuentes: de una parte, diluir la especificidad del injusto informático en categorías tradicionales; de otra, expandir de manera indiscriminada la noción de ciberdelincuencia hasta convertir toda utilización de tecnologías en fundamento suficiente para una tutela penal diferenciada.

El principal aporte del presente trabajo consiste en proponer una base dogmática unitaria para la comprensión de los delitos informáticos en el ordenamiento ecuatoriano. La funcionalidad de los sistemas de información y comunicación permite articular la exigencia constitucional de legitimidad, la estructura típica de las figuras del catálogo punitivo ecuatoriano y la necesidad de preservar un concepto restrictivo y material del bien jurídico en el ámbito digital. Solo a partir de esta construcción es posible interpretar estas infracciones con mayor rigor, mantener la coherencia entre lesividad y tipicidad, y evitar que la expansión de la criminalidad informática conduzca a soluciones conceptualmente imprecisas o dogmáticamente débiles.

Con todo, debe precisarse que el alcance de esta propuesta es principalmente dogmático y sistemático. Su contribución se concentra en ofrecer una categoría interpretativa capaz de dotar de coherencia material a los tipos penales analizados y de orientar su aplicación conforme a los principios de lesividad, proporcionalidad y mínima intervención. En esa línea, futuras investigaciones podrían profundizar en la incidencia de esta concepción del bien jurídico en la política criminal del Estado, en la priorización de investigaciones, en la valoración del riesgo tecnológico y, especialmente, en la proporcionalidad de las penas previstas para los delitos informáticos, a fin de verificar si la respuesta punitiva guarda correspondencia con el grado real de afectación a la funcionalidad de los sistemas de información y comunicación.

BIBLIOGRAFÍA

CLAUS, Roxin. Derecho penal. Parte general. Tomo I: Fundamentos. La estructura de la teoría del delito. Traducción de Diego-Manuel Luzón Peña, Miguel Díaz y García Conlledo y Javier de Vicente Remesal. 1.ª ed. Madrid: Civitas, 1997

Corte Nacional de Justicia del Ecuador. Sala Especializada de lo Penal, Penal Militar, Penal Policial, Tránsito, Corrupción y Crimen Organizado, Juicio No. 19303-2019-00328. Sentencia, 1 de septiembre de 2022.

Corte Constitucional del Ecuador. Sentencia No. 34-19-IN/21 y acumulados, 28 de abril de 2021.

Ecuador, Constitución de la República del Ecuador, Registro Oficial 449, Suplemento, 20 de octubre del 2008.

Ecuador, Código Orgánico Integral Penal, Registro Oficial 180, Suplemento, 10 de febrero del 2014.

Hungría - Budapest, Convenio sobre la Ciberdelincuencia, Serie de Tratados Europeos – Nro. 185. 23 de noviembre del 2001

Ecuador. Asamblea Nacional del Ecuador. Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad: texto aprobado en segundo debate el 10 de febrero de 2026; objeción parcial por inconveniencia contenida en el Oficio No. T.368-SGJ-26-0061, de 12 de marzo de 2026; y allanamiento de la Asamblea Nacional con remisión al Registro Oficial para publicación, 31 de marzo de 2026.

Ecuador, Estrategia para el fomento del desarrollo y uso ético y responsable de la inteligencia artificial en el Ecuador, Registro Oficial Suplemento 206, 19 de enero del 2026.

CORCOY BIDASOLO, Mirentxu. “Problemática de la persecución penal de los denominados delitos informáticos: particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos”. Eguzkilore, n.º 21, 2007.

MAYER LUX, Laura, “El bien jurídico protegido en los delitos informáticos”, Revista Chilena de Derecho, vol. 44, N.º 1, 2017.

Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), Ciberdelito I: Guía práctica para un abordaje integral del fenómeno. Tipos generales. Marco jurídico y derechos humanos. El ABC de la investigación, 1.ª ed., revisión y adaptación de la Oficina de Análisis Estratégico contra la Criminalidad (OFAEC), marzo de 2022.

TEMPERINI, Marcelo. “Delitos informáticos y cibercrimen: alcances, conceptos y características”. En la obra: Cibercrimen y delitos informáticos: Los nuevos tipos penales en la era de internet, compilado por Ricardo Antonio Parada y José Daniel Errecaborde. 1.ª ed. Ciudad Autónoma de Buenos Aires: Erreius, 2018.