

El hacking como comportamiento típico en las nuevas formas de delincuencia organizada¹

Hacking as a typical behavior in new forms of organized crime

Santos Montenegro, Manuel Agustín²

Barrios Miranda, Ángel Silverio³

González de Vincés, Petrick Jeanny⁴

RECIBIDO – SEPTIEMBRE 2018 – ACEPTADO FEBRERO 2019 – PUBLICADO MARZO 2019

¹ Artículo original derivado de investigación en el área penal, Facultad de Jurisprudencia, Ciencias Sociales y Políticas de la Universidad de Guayaquil. Inicio 2017-2018

² Abogado de los Juzgados y Tribunales del Ecuador, Criminólogo, docente de la Facultad de Jurisprudencia de la Universidad de Guayaquil Correo electrónico: manuel.santos@ug.edu.ec, manuelsantos3@hotmail.es, ORCID <https://orcid.org/0000-0002-3340-8083>.

³ Abogado de los Juzgados y Tribunales del Ecuador, Criminólogo, docente de la Facultad de Jurisprudencia de la Universidad de Guayaquil Correo electrónico: angel.barriosm@ug.edu.ec, anbami@hotmail.com, ORCID <https://orcid.org/0000-0003-3056-4416>

⁴ Licenciada en Administración de la Universidad del Zulia. Egresada en Derecho de la Facultad de Jurisprudencia de la Universidad de Guayaquil. correo electrónico: petrick.gonzalezd@ug.edu.ec, petrickgonzalez@gmail.com, ORCID <https://orcid.org/0000-0001-6873-4666>.

Resumen

Introducción. La palabra “hacking” es un anglicismo que tomó su acepción del verbo “to hack” que significa “hachar” que se refiere a la acción ejercida con fuerza sobre los postes telefónicos de aquellos técnicos en la década de los sesenta en los Estados Unidos que golpeaban para poder enderezar las líneas y reparar alguna falla en la comunicación. **Objetivo** Determinar si es el hacking un comportamiento típico, antijurídico y penalmente ajustado a lo estipulado por el Código Orgánico Integral Penal. **Materiales y métodos** el tipo de investigación es documental y el método hipotético deductivo. **Resultados** El delito que más se ajusta al comportamiento del hacker en Ecuador es el ataque cibernético y a su vez la delincuencia organizada se contempla en el Código Orgánico Integral Penal como un comportamiento penalmente relevante y sancionable. **Conclusiones** sería lo ideal poder especificar a través de otro tipo penal que considere la sola irrupción no autorizada a cualquier tipo de sistema informático ajeno a quien lo ejecuta.

Palabras Clave: ataque cibernético, delincuencia organizada, tipo penal.

Abstract

Introduction. The word "hacking" is an Anglicism that took its meaning from the verb "to hack" which means "hachar" which refers to the action exercised with force on the telephone poles of those technicians in the sixties in the United States who beat to be able to straighten the lines and repair some communication failure. **Objective** Determine if hacking is a typical behavior, unlawful and criminally adjusted to the provisions of the Organic Comprehensive Criminal Code. **Materials and methods** the type of research is documentary and the hypothetical deductive method. **Results** The crime that best suits the behavior of the hacker in Ecuador is the cyber attack and organized crime in turn is considered in the Organic Comprehensive Criminal Code as a criminally relevant and punishable behavior. **Conclusions** would be the ideal to be able to specify through another type of crime that considers the unauthorized irruption alone to any type of computer system outside the person who executes it.

Keywords: cyber attack, organized crime, criminal type.

1. Introducción.

Desde que se iniciaron las primeras experimentaciones con los procesadores de datos, nacen las actividades humanas conducentes a tener acceso y disponibilidad de los mismos, como parte de un patrimonio intelectual intangible pero que sin duda existe, la diferenciación de un software computacional y el hardware es fácil de determinar en la práctica, sin embargo, para efectos de la ley existen aún muchas deficiencias con respecto a la regulación de los primeros, debido a su carácter voluble y a veces inmedible. (Carpio, 2013)

En este sentido, resulta necesario indicar que la ley penal por su misma naturaleza requiere de una determinación exacta de la conducta penalmente reprochable que en efecto, se denomina comportamiento típico, ya que se enmarca en una forma específica de exteriorizar el comportamiento humano, para evitar divagaciones en la ley o tipos penales que pueden ajustarse a varios comportamientos, la doctrina penal indica que es necesario que esa conducta esté claramente descrita en la ley penal. (Albán, 2016)

El software está compuesto por los programas, sistemas, datos, que se encuentran entrelazados por funciones o algoritmos que le dan sentido, por tanto, tal como indica (Cisneros, 2009) el bien jurídico protegido en este caso sería el software, lo que no excluye al hardware en casos que un ataque intencionado a través de virus pueda ocasionar daños en el disco duro y otras partes físicas de la computadora.

En lo cotidiano, la palabra “hacker” se ha popularizado debido a medios de comunicación y las mismas redes sociales que lo han promocionado como una persona que se dedica a intervenir sin permiso los sistemas electrónicos, así como los datos que contienen que pertenecen a una persona en específico, sin embargo, este experto en sistemas no necesariamente lo haría ilegítimamente, pues existe también el hacking ético, que no es más que el peritaje y servicio de seguridad informática tan necesario en estos días. (Vizueta, 2011)

Se denomina hacking al conjunto de técnicas que se utilizan para tener acceso a un sistema que no pertenece al mismo ejecutor, para esta incursión por lo regular cada quien configura su propio conjunto de claves de accesibilidad y es la actividad de descifrar estas claves o interferir en los computadores que se conoce como la actividad de “hackeo”. (Vallejo, 2010)

En 1983, como indica (Carpio, 2013) se da a conocer uno de los primeros conceptos de delitos informáticos de la OCDE (Organización de Cooperación y Desarrollo Económico), que indicó que un delito informático es un comportamiento antijurídico, no ético, no autorizado, relacionado con el procesamiento automático de datos y transmisión de datos. Del mismo modo, (Sarzana, 2010) indicó que delito informático es un comportamiento criminal que involucra a una computadora como material, objeto y medio para ejecutar una conducta penalmente reprochable. De igual forma, (Vizueta, 2011) los delitos informáticos serían los que se realicen contra los bienes ligados al tratamiento automático de datos, según lo analizado, los delitos informáticos son aquellas conductas antijurídicas, típicas y penalmente reprochables que utilizan como medios de perpetración el procesamiento de datos de forma

electrónica o digital, lo que incluye no sólo ordenadores o computadoras sino también aparatos móviles de procesamiento de información.

En Ecuador la ley penal sólo contempla seis tipos penales con respecto al manejo de información que puede estar ajustado a la conducta del hacking, haciendo la salvedad de aquellos casos en los que la intervención o “explotación” de sistemas está amparado por la ley y autorizado para peritos expertos así como investigadores en el área de criminología. (Albán, 2016)

Sin duda, la magnitud de estas variables de estudio que se pretenden analizar en el presente artículo, son extensas, por lo tanto, es el objetivo ajustar el comportamiento del hacker en las nuevas formas de delincuencia organizada, lo que específicamente no se declara en el Código Orgánico Integral Penal, sin embargo, puede tomarse como un concurso de infracciones, lo que sí está claro en la conducta penalmente reprochable y los verbos rectores que la determinan, con respecto a delitos ligados a la información y la asociación para delinquir.

En este sentido la hipótesis de investigación estaría declarada como un interrogante: ¿Es el hacking un delito en el Ecuador? Lo que deriva otros interrogantes como: ¿Cuál sería el tipo penal cuando existe no sólo un hackeo sino también la participación de una organización delictiva?

Determinar si es el hacking un comportamiento típico, antijurídico y penalmente ajustado a lo estipulado por el Código Orgánico Integral Penal.

2. Materiales y métodos

El tipo de investigación es documental y el método hipotético deductivo, además empleando las técnicas de revisión y procesamiento de información para poder ajustar el comportamiento penalmente relevante a la conducta del hacker, en este sentido, se puede decir que también se emplea un método analítico-descriptivo con el objeto de dar un aporte científico con respecto a las nuevas formas de crimen organizado que se evidencian en estos tiempos modernos. (Balestrini, 2010)

3. Resultados

La teoría del Delito en cuanto al comportamiento criminal

Según (Carpio, 2013) es en el inicio del siglo XX cuando Listz (citado por Carpio, 2013) determina una definición de delito que aún es aceptada en la legislación penal vigente: “acto culpable, contrario al derecho y sancionado con una pena”; una idea bastante simple pero a la vez que aún define lo que se conoce como delito, Beling (citado por Carpio, 2013) a su vez agrega que el proceso del cometimiento del acto penalmente relevante debe contener un proceso material causal, además del contenido objetivo de la voluntad situacional con el ánimo de causar un perjuicio; lo que termina completando las ideas y genera una serie de escuelas, como la finalista, la matemática y la neoclásica.

A efectos del presente artículo, se tomará como punto de partida estos conceptos básicos, la acción es la causa del resultado, el comportamiento debe ser visible, es decir debe ejecutarse una acción o inacción evidente por parte del sujeto activo del delito, que lleve a deducir que tenía una intención de generar un resultado. Todo esto, debe tomarse en cuenta para poder ajustar un tipo penal a la acción de “hacking”, y es el objetivo de esta investigación poder describirlo en cuanto a los tipos penales vigentes en el Código Orgánico Integral Penal (2014).

Como ya se ha indicado al inicio, el hacking es el proceso de acceder a información cifrada que a todo el público en general está oculta, por esto, regularmente es ilegal, salvo en caso de hacking ético, que no es más que un peritaje a sistemas informáticos que se encuentran inmersos en cualquier proceso judicial, es por esto, que al analizar los tipos penales en el Ecuador, en cuanto a la legislación vigente, se puede señalar la descripción que a continuación se detalla:

Tabla 1. Análisis de los Tipos Penales en el Código Orgánico Integral Penal y la Conducta del Hacker

Tipo Penal	Verbo rector	Conducta del Hacker
Revelación ilegal de base de datos	Revelar información	Efectivamente un hacking puede intervenir sistemas informáticos y su revelarlo al público en general a través de la red. Sin embargo, el hacking no se ajusta necesariamente a este tipo penal porque no siempre la información se revela, lo que ocurre siempre es la interferencia en el sistema electrónico.
Interceptación ilegal de datos	Interceptar, escuchar, desviar, grabar, observar... (datos informáticos)	Es un tipo penal que sí se ajusta al hacking, pues la labor de un hacker efectivamente puede interceptar, escuchar, desviar, grabar, observar,
Número 1	Diseñar, desarrollar, vender, ejecutar, programar, enviar... mensajes de seguridad, páginas electrónicas, enlaces, ventanas, sistemas de resolución de nombres de dominio, pago electrónico.	diseñar, desarrollar, vender, ejecutar, programar, enviar, información. También puede inducir a ingresar a sitios falsos, además copiar, clonar y comercializar información contenida en los sistemas informáticos. Lo que no siempre es el objetivo del hacking.
Número 2	Inducir a un persona a ingresar a una dirección	

	diferente a la quiere acceder.	
Número 3	Copiar, clonar, comercializar, informar... bandas magnéticas chips o dispositivos electrónicos en tarjetas de crédito, débito, pago o similares.	
Número 4	Producir, fabricar, distribuir, poseer, facilitar, materiales o dispositivos electrónicos o sistemas informáticos destinados a cometer un delito.	
Transferencia electrónica de activo patrimonial	Alterar, manipular, modificar... el funcionamiento de un programa o sistema informático (para apropiación no consentida de un activo patrimonial de otra persona)	El hacking puede realizar transferencia electrónica pero no necesariamente este tipo penal es cometido en el acto de hackeo.
Ataque a la integridad de Sistemas informáticos	Destruir, dañar, borrar, deteriorar, alterar, suspender, trabar, causar mal funcionamiento, suprimir datos.	Es tal vez el tipo penal más ajustado a la conducta del hacker, quien puede interferir casi siempre con el ánimo de destruir, deteriorar, alterar, suspender, trabajar o causar mal funcionamiento de los sistemas.
Número 1	Diseñar, desarrollar, programar, adquirir, enviar, introducir, ejecutar, vender o distribuir (dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos del delito.	Además el hacking puede incluir la alteración con el ánimo de causar otro delito como la estafa, la extorsión, entro otros tipos penales relevantes.
Número 2	Destruir, alterar sin autorización del titular, la infraestructura tecnológica necesaria	

	para la transmisión, recepción o procesamiento de información general.	
Delitos contra la información pública reservada legalmente	Destruir, inutilizar información clasificada.	Se interfiere en un sistema del Estado, o se realiza hacking en sitios, bases de datos, sistemas de información que pertenecen al Estado y que se consideran legalmente reservadas. Esta interferencia efectivamente es un hackeo, pero no todo hackeo tiene como objetivo los sistemas públicos.
Acceso no consentido a un sistema informático telemático o de telecomunicaciones.	Acceder (en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones).	Se constituye igual que el delito anterior, y el verbo rector sólo acceder, se considera en sí un hacking.

Fuente: Santos, Barrios y González (2019)

Los delitos informáticos, tal como se evidencia anteriormente tiene una serie de cualidades que dificultan la adecuación de la conducta al tipo penal, a continuación se hará una descripción del tipo penal: ataque a la integridad de sistemas informáticos que también podemos compararlo con el hacking. Al finalizar se dan una serie de conclusiones para la configuración de nuevos tipos penales que se refieran específicamente al hacking. (Albán, 2016)

Sujeto de la Acción

El sujeto de la acción penal en este caso es cualquier persona, indeterminada, sin embargo, se puede especificar que este sujeto debe poseer los conocimientos necesarios para la irrupción no autorizada en el sistema. Lo que también puede configurarse en un autor intelectual, en caso de ser el que comete el delito contratado por alguien más a quien le interese la información, en cuyo caso sería un autor material. (Carpio, 2013)

Ausencia de la Acción

En este caso no se considera ausencia de acción u omisión, pues para que el delito se consuma es necesario realizar un comportamiento visible. (San-Martín, 2006)

Fases de la Acción

Existe una premeditación que puede constituirse en una serie de acciones previas al cometimiento de la acción penalmente relevante, en tal sentido, todo acto de preparación, como adquisición de ordenadores, programas y demás elementos necesarios para la acción.

Luego, la ejecución del ataque a la integridad de los sistemas informáticos puede considerarse el cometimiento efectivo de la acción además finalmente una disposición de la información posterior a la irrupción en el sistema sin ningún tipo de autorización legítima por parte del propietario de esa información, lo que puede ser: almacenar, borrar, distorsionar o disponer de esos datos de cualquier manera. Lo que se puede resumir de la siguiente forma:

1. **Inter Criminis:** lo que se conoce como los actos previos a la consumación del delito, en este caso, la adecuación del espacio o adquisición de equipos telemáticos o informáticos de cualquier tipo así como los softwares o programas que se requieran para la consumación del delito.
2. **Acción Penal:** es el momento el que efectivamente se ejecuta el acceso no autorizado en el sistema con el fin de poder atacar la integridad del sistema.
3. **Fin de la acción:** se finaliza disponiendo de la información adquirida, lo que también incluye borrarla, eliminarla o destruirla si así fuera la intención del experto que realiza el ataque, pero también se puede conservar y almacenar o devolverla al mismo lugar pero modificada.

La conducta visible radica en la utilización efectiva de herramientas telemáticas para la intervención no autorizada de datos. (Espinosa, 2015)

Nexo entre la Conducta y el Resultado

Por tratarse de un delito de resultado el nexo causal es evidente, existe una conexión objetiva entre la causa y el resultado del delito, para (Cabanelas, 2012) la causalidad representa un requisito peculiar de una especie de infracciones, al consumarse existiría una manifestación volitiva, aunque para otros autores no constituye un requisito indispensable, en el caso estudiado se evidencia que quien irrumpe en un sistema con el ánimo de disponer de datos sin estar autorizado está efectivamente ligado a una causa evidente y una intención de causar perjuicio.

Estructura del Tipo Penal

1. **Sujeto Activo:** el sujeto activo es cualquier persona.
2. **Sujeto Pasivo:** el sujeto pasivo o víctima es el propietario de los datos.
3. **Conducta:** la conducta es la irrupción en el sistema telemático o datos.
4. **Bien Jurídico Protegido:** son los datos, programas, información, software y demás que constituyen el objeto del ataque.

Imputación Subjetiva

- **Culpa:** La culpabilidad recae sobre aquella persona que destruya o altere sistemas informáticos, lo que necesariamente involucra una irrupción en el mismo para poder efectivamente dañarlo, borrarlo, modificarlo o extraerlo. El delito hace culpable a quien efectivamente ejecuta la acción, lo que no excluye que no pueda tener conciencia de la gravedad del acto que está cometiendo, sobre todo si el ejecutor es una persona joven o menor de edad inclusive.
- **El Dolo:** el dolo consiste en el ánimo de causar daño, que se encuentra implícito, sin embargo, para la defensa de quien se encuentra imputado por este delito, se

puede evidenciar en un hacking ético que evidencia que efectivamente se realizó una acción con toda la intención de causarle daño al sistema, modificarlo, borrarlo o extraer datos.

- **Error de Tipo:** Esto es muy común, ya que los tipos penales que considera el Código Orgánico Integral Penal son limitados, y cada día surgen diferentes formas de causar daño a los sistemas telemáticos, que pudieran involucrar otros elementos distintos a los considerados por la norma.

La Delincuencia Organizada como Agravante

En el Artículo 369 el Código Orgánico Integral Penal indica que la delincuencia organizada implica la intervención de dos o más personas que de forma permanente o reiterada financien cualquier forma de actividad delictiva, además en delitos informáticos como es el caso del hacking o el transgresión de ataque cibernético, es casi inevitable traspasar fronteras, lo que con las conexiones globales se da con frecuencia, de acuerdo a (Carpio, 2013) la investigación judicial debe iniciar con el hecho local pero se extiende hasta diligencias que trascienden las fronteras del país, debido a que los domicilios electrónicos pueden variar, incluso, el autor del delito puede estar físicamente en cualquier parte del mundo, lo que puede generar dificultades para los investigadores de la Fiscalía del Ecuador y en cuyo caso los convenios y tratados internacionales pasan a cubrir los vacíos legales a considerar.

El Comportamiento Típico

El hacking, como tal, no se encuentra tipificado como una conducta penalmente relevante, sin embargo, tal como se analizó anteriormente, el ataque cibernético vendría siendo el tipo penal o comportamiento típico que más se ajusta a este tipo de actividad de aquellas personas que tienen las habilidades para el manejo de sistemas informáticos. Ahora bien, la delincuencia organizada sí se encuentra contemplada como un tipo penal en el Código Orgánico Integral Penal, por ende, es el hacking una forma de crimen organizado cuando para su perpetración se requiere la intervención de más de una persona, y además se puede traspasar las fronteras físicas del país, lo que también dificulta ejecutar el proceso penal y la sanción correspondiente al delito. (Holguín, 2011)

Existe un impedimento propio del delito informático que es la identificación del sujeto activo, pues los autores materiales saben cómo protegerse en el ámbito virtual donde efectivamente se ejecuta la acción delictiva, esto genera que progresivamente sea más complejo el descifrar las actividades del hacker, y se requiere de tecnología de punta por parte de los agentes investigadores, que casi siempre no poseen las mismas herramientas telemáticas que quien ejecuta la acción penal, es por esto que se justifica la propuesta y sanción de un tipo penal que se ajuste mucho más a las conductas como el hacking.

4. Conclusiones

1. El “hacking” proviene del verbo inglés to hack que significa “hachar”, lo que asemeja a las hachas que utilizaban los técnicos de comunicación en los inicios de las telecomunicaciones, el acto de hackeo o hackear es la irrupción no autorizada en sistemas informáticos o electrónicos que no pertenecen al sujeto que la ejecuta.

2. Según la teoría clásica del delito, el hecho de irrumpir de forma no autorizada a sistemas informáticos, programas, base de datos, computadores personales, móviles, etc. Es un delito de resultado que requiere la prueba material de una evidencia de haber efectivamente realizado la intervención en algún momento, lo que queda grabado en los sistemas, y puede constituir en la demostración del hecho.
3. El hacking no está contemplado como delito específico en la legislación ecuatoriana, sin embargo, los cuatro tipos penales que existen: revelación ilegal de base de datos, interceptación ilegal de datos, transferencia electrónica de activo patrimonial y ataque a la integridad de sistemas informáticos, así como los que se ejecutan contra el patrimonio público como: delito contra la información pública y acceso no consentido a un sistema informático de telecomunicaciones; constituyen en sí una modalidad de hacking; de estos delitos mencionados se analizó el ataque cibernético como el más ajustado a la conducta del hacker.
4. Si bien se puede constituir en un acto preparatorio o condición indispensable para la ejecución del delito informático, el hacking no está contemplado como tipo penal en sí, lo que sería recomendable para poder ajustar la norma específicamente al ámbito práctico o la realidad que regula la ley penal.

Referencias bibliográficas

- Albán, E. (2016). *Manual de Derecho Penal Ecuatoriano*. Quito: Ediciones Legales.
- Asamblea Constituyente. (2008). *Constitución de la República del Ecuador*. Montecristi: Asamblea Constituyente del Ecuador.
- Asamblea Nacional. (2014). *Código Orgánico Integral Penal*. Quito: Registro oficial.
- Burneo, R. (2010). *Derechos y Garantías Constitucionales en el Ecuador*. Quito: Corporación de Estudios y Publicaciones.
- Cabanellas, G. (2012). *Diccionario Jurídico Elemental*. Buenos Aires: Eliasta.
- Carpio, D. (2013). *El Delito Informático. Prueba Pericial Informática*. Quito: Jurídica del Ecuador.
- Cisneros, E. (2009). *Los Delitos Informáticos*. Quito: Universidad Simón Bolívar-Ecuador.
- Espinosa, G. (2015). *Enciclopedia Jurídica. Volumen I*. Barcelona: Iuris.
- Holguín, J. (2011). *Derecho Constitucional Ecuatoriano*. Loja: Universidad Técnica Particular de Loja.
- Reyes, A. (2008). *Dogmática y Criminología*. Quito: Legis.
- San-Martín, C. (2006). *Derecho Penal*. Lima, Perú: Grijiley.
- Sarzana, C. (2010). *Criminalité e Tecnologia*. Roma: S.E.
- Vallejo, V. (2010). *El Delito Informático en la Legislación Ecuatoriana*. Quito: Corporación de Estudios y Publicaciones.
- Vizueta, J. (2011). *Delitos Informáticos en el Ecuador*. Guayaquil: Endino.

