Fecha de presentación: enero, 2022
Fecha de aceptación: marzo, 2022
Fecha de publicación: abril, 2022

44

LA INFRACCIÓN

AL DEBER OBJETIVO DE CUIDADO EN EL PROCESO DE HARDENING

THE INFRINGEMENT OF THE OBJECTIVE DUTY OF CARE IN THE HARDENING PROCESS

Alberto Leonel Santillán Molina[1]
E-mail: us.albertosantillan@uniandes.edu.ec
ORCID: https://orcid.org/0000-0001-8517-8980
Nelly Valeria Vinueza Ochoa[1]
E-mail: ub.nellyvinueza@uniandes.edu.ec
ORCID: https://orcid.org/0000-0002-8935-7545
Cristian Fernando Benavides Salazar[1]
E-mail: us.cristianbenavides@uniandes.edu.ec
ORCID: https://orcid.org/0000-0002-4326-2137
[1] Universidad Regional Autónoma de Los Andes. Ecuador.

Cita sugerida (APA, séptima edición)

Santillán Molina, A. L., Vinueza Ochoa, N., & Benavides Salazar, C. F. (2022). La infracción al deber objetivo de cuidado en el proceso de Hardening. *Revista Universidad y Sociedad*, 14(S2), 364-372.

RESUMEN

El problema de investigación radica en determinar si cabe la conducta imprudente en los ciberdelitos cuando el técnico de seguridad informática responsable del proceso de hardening, por imprudencia, impericia, negligencia o inobservancia de sus lex artis, infracciona el deber de cuidado, lo que da como resultado una intromisión al sistema informático bajo su responsabilidad, por lo que el objetivo de este trabajo es establecer los parámetros teóricos en los que se sustenta la imputación al tipo objetivo en los delitos informáticos, por infracción al deber objetivo de cuidado del responsable de la seguridad del sistema de tratamiento de información. La presente investigación fue cualitativa, en la que se utilizó los métodos histórico-lógico que identificó las líneas de investigación que permitieron establecer cómo se encuentra descrito el delito informático en el derecho penal moderno, el método analítico-sintético relativa a las definiciones sobre el delito informático, imputación objetiva y el proceso de hardening, y finalmente el método de análisis jurídico relativo a las disposiciones legales aplicables; y como técnica de investigación se utilizó el análisis de contenido. En los resultados se desarrolló la importancia del hardening, las pericias informáticas en materia penal que sustentan el principio de objetividad de Fiscalía en la Investigación penal, llegando a concluir que el delito informático en nuestra legislación es doloso, pero se ha demostrado académicamente que existe la posibilidad de una conducta culposa abordada desde la previsibilidad, advertibilidad y evitabilidad del resultado como presupuesto de la conducta imprudente.

Palabras clave: Hardening, seguridad informática, Imputación objetiva, ciberdelito, pericia informática.

ABSTRACT

The research problem lies in determining whether there is reckless conduct in cybercrimes when the computer security technician responsible for the hardening process, due to recklessness, inexperience, negligence or non-observance of its lex artis, infringes the duty of care, which gives as The result was an interference with the computer system under his responsibility, so the objective of this work is to establish the theoretical parameters on which the imputation of the objective type in computer crimes is based, for infringement of the objective duty of care of the person in charge of security of the information processing system. The present investigation was qualitative, in which the historical-logical methods were used that identified the lines of investigation that allowed to establish how the computer crime is described in modern criminal law, the analytical-synthetic method relative to the definitions of the crime computer science, objective imputation and the hardening process, and finally the method of legal analysis related to the applicable legal provisions; and content analysis was used as a research technique. In the results, the importance of hardening was developed, the computer skills in criminal matters that support the principle of objectivity of the Prosecutor's Office in the criminal investigation, concluding that the computer crime in our legislation is malicious, but it has been academically demonstrated that there is the possibility of a culpable conduct approached from the predictability, predictability and avoidability of the result as a presupposition of the reckless conduct.

Keywords: Hardening, Informatic security, objective imputation, cybercrime, computer expertise.

INTRODUCCIÓN

Doctrinariamente el delito se define como la acción típicamente antijurídica y culpable, la cual es atribuible desde la imputación, a quien cometió el injusto penal, y por tanto debe de ser sometido a una pena. (Gaviria, 2005).

Dentro de su clasificación existe una que aborda la intencionalidad del agente que se traduce en el dolo y la culpa como elementos subjetivos del tipo penal, es así como el delito se clasifica desde la intención en doloso y culposo. El delito doloso a su vez se clasifica en intencional, cuando el acontecimiento dañoso o peligroso que la ley penal ha descrito como tal, proviene de la propia acción u omisión del agente, es decir, su conducta es dolosa, cuando conociendo los elementos objetivos del tipo penal, los ejecuta esperando un resultado o una lesión al derecho ajeno, actuando con voluntad y conciencia; y culposa cuando el acontecimiento no previsto ni querido por el agente, se verifica por imprudencia, impericia o inobservancia de leyes, reglamentos o lex artis que infraccionan el deber objetivo de cuidado, rebasando de esta manera el riesgo permitido, por lo que no existiría intención positiva de irrogar daño sino falta de previsión.

En el delito imprudente no entra en juego el dolo con actos anteriores o simultáneos, sino que se presentan ciertos elementos de la imprudencia que sobrepasan el riesgo aceptable, tales como la "previsibilidad, advertibilidad y evitabilidad del resultado como presupuesto de la conducta imprudente" (Roxin, 2013, pág. 999).

Es aquí donde encaja la teoría de la imputación al tipo objetivo cuyo autor es el maestro alemán Claus Roxin, quien bosqueja en "1970 en su libro Homenaje a Honig, la vinculación con el criterio de creación de un riesgo jurídicamente relevante y de una lesión del bien jurídico. (Roxin & Vásquez, 2007).

El planteamiento que el Maestro de la Universidad de Múnich sostiene, es que "es objetivamente imputable un resultado causado por una conducta humana, cuando dicha acción ha creado un peligro jurídicamente desaprobado, que se ha realizado en el resultado típico y que pertenezca al ámbito de protección de la norma infringida" (Roxin, 2013, pág. 377), por lo tanto, se debe entender que la aplicación de esta teoría, abarca con precisión a los delitos imprudentes donde el dolo se excluye mas no la culpa como presupuesto vital del tipo.

El ciberdelito es aquel acto que en su descripción típica exige la presencia del uso de la informática como medio para la comisión de la infracción, y la alteración, manipulación o modificación de los datos informáticos, como elementos de su antijuridicidad que lo hacen un acto de reproche merecedor de una sanción penal.

La doctrina mayoritaria considera al delito informático como una conducta eminentemente dolosa, cuando el agente a sabiendas vulnera las medidas de seguridad que han sido impuestas para impedir el acceso no autorizado a los sistemas automatizados de información, tales como: "lector del iris del ojo, reconocimiento de patrones de voz, así como también el reconocimiento biométrico facial, la huella dactilar, y finalmente el usuario y contraseña que da el acceso a la operatividad del sistema" (Suarez, 2016, pág. 344), y de esta manera beneficiarse de la intromisión para cometer otras conductas como el espionaje o sabotaje informático.

No obstante también se encuentran en esta parte de la teoría del delito informático impropio, el hecho de que no protegen bienes jurídicos específicos a la informática, sino otros bienes jurídicos como la intimidad, la privacidad, la propiedad, la fe pública, la indemnidad sexual, es decir se usan los medios electrónicos como las redes sociales u otro medio de comunicación masiva por internet para cometer el delito, pero lo cierto es, que una vez analizada la forma en la que se ejecuta las medidas impuestas que impiden el acceso no consentido, se verificaría la imprudencia al deber objetivo de cuidado en el agente de seguridad informática responsable del proceso del hardening.

El "hardening" (Gómez, 2014, pág. 52) es un procedimiento de seguridad informática que tiene como finalidad "asegurar un sistema mediante la reducción de sus vulnerabilidades, eliminando software que no prestan ninguna funcionalidad, o servicios, o usuarios, o accesos innecesarios, o cerrando puertos en desuso, y así evitar que el sistema sea vulnerado por la falta de previsibilidad, advertibilidad y evitabilidad del acceso no consentido por impericia, imprudencia, o inobservancia de las reglas de cuidado del agente de seguridad.

Los actos preparatorios de aseguramiento que generalmente realiza el técnico sobre el sistema informático al "endurecer las medidas de seguridad son: 1. Cambiar periódicamente todas las claves de acceso, la cual funciona como una medida preventiva cuando la clave ha sido obtenida legítima o ilegítimamente de manos del titular de la cuenta; 2. Desinstalación de software que puedan presentar bondades para una penetración no autorizada; 3. Deshabilitar usuarios que estén sin uso en el sistema, y así evitar un acceso de una persona que se haya revocado su permiso de acceder, pero que no haya sido deshabilitado en el mismo y presente una puerta que permita la intromisión y que esta se verifique por falta de cuidado

del agente de seguridad; 4. Deshabilitar servicios en desuso, cambiando la configuración de los puertos lógicos y así evitar su uso no autorizado; 5. Instalación de antivirus; 6. Actualización del software; y, 7. Obtener copias de seguridad y respaldo de la información.

Como podemos observar de lo explicado, es posible que en el ciberdelito se pueda presentar una conducta imprudente por infracción al deber objetivo de cuidado por rebasamiento del riesgo permitido, y por ende que el delito informático se encuadre en la categoría del delito culposo.

Por lo expuesto, el problema de investigación radica en determinar si cabe la conducta imprudente en los delitos informáticos por infracción al deber objetivo de cuidado, como elemento en la teoría de la imputación objetiva, por lo que el objetivo de esta investigación es establecer los parámetros teóricos en los que se sustenta la imputación al tipo objetivo en los delitos informáticos, por infracción al deber objetivo de cuidado, del responsable de la seguridad del sistema automatizado de información en el proceso de hardening.

La imputación al tipo objetivo

Como ya hemos explicado en la fórmula de la imputación al tipo objetivo, es que esta depende de la participación del autor activamente y de una relación causal para poder imputar de manera directa la conducta en los elementos descriptivos del tipo objetivo, lo que requiere como presupuesto de la realización del tipo "es que el autor haya causado el resultado" (Roxin, 2013, pág. 346).

Por tanto, para poder llegar a realizar este análisis en cuanto a la conducta imprudente, se debe abordar las posiciones teóricas del maestro alemán Claus Roxín cuando sostiene que:

a) Un resultado causado por el agente sólo se puede imputar al tipo objetivo, si la conducta del autor ha creado un peligro no cubierto por el riesgo permitido y que el mismo se encuentre en el resultado concreto; y, b) Si el resultado se presenta como una ejecución del peligro creado por el agente, por regla general va a ser imputado cuando se cumple el tipo objetivo (Roxin, 2013, pág. 346).

En tal virtud, esta teoría de imputación presupone necesariamente la realización de un peligro que ha sido creado por el autor y que definitivamente no es cubierta por el riesgo permitido, cuando ésta se encuentra debidamente tipificada en el ordenamiento jurídico penal.

Entre las teorías que sustentan la imputación objetiva tenemos la de la causalidad, que se define como el conjunto de hechos ejecutados por una persona, los cuales se encuentran interrelacionados para el cumplimiento de un fin específico, es decir, causa y efecto; y la teoría del nexo causal que exige la existencia de un vínculo que una la infracción con el responsable, y de ahí partir para determinar si el agente ha causado el resultado final que ha sido descrito en los elementos del tipo objetivo, y que sea relevante para la producción de un resultado típico, cuando sea rebasado el riesgo permitido a través de la creación de un peligro jurídicamente desaprobado.

Bajo esta misma lógica, se puede definir al riesgo permitido como aquel conjunto de hechos que crean un peligro relevante pero que jurídicamente se encuentra permitido, y que se debe cumplir para evitar la comisión de una infracción, ya que el rebasamiento del mismo obligaría al juzgador analizar su conducta descrita en el tipo.

Son estas normas de cuidado en el riesgo permitido que aprueban actividades riesgosas soportadas en la ley, como las normas que rigen el tránsito vehicular o las lex artis médicas, y que un buen manejo de las mismas, reducirían la consumación de un resultado jurídicamente desaprobado.

Es por esto por lo que el insigne maestro alemán considera que: "la observancia de las normas de cuidado aumenta claramente la posibilidad de salvaguardar un bien jurídico, pero no lo garantiza con absoluta seguridad" (Roxin, 2013, pág. 380) que este no pueda ser vulnerado. Es por esto por lo que se puede sostener que en los delitos informáticos quién se encuentra obligado a garantizar que los sistemas de tratamiento de información se encuentren seguros, es el agente de seguridad informática responsable del proceso de hardening, que impida de mejor manera el acceso no consentido a los sistemas automatizados de información.

El proceso de hardening y el hackeo ético

El hackeo ético es una metodología que tiene como finalidad desde el campo de la informática (Hartley, 2015), explotar todas las vulnerabilidades que pueda presentar un sistema de tratamiento de información, cuyo objetivo final es el fortalecimiento de las medidas de seguridad para identificar cuáles son aquellos puntos de penetración que le permitan al hacker, realizar una intromisión disminuyendo el riesgo de hackeo a través de una auditoría, la cual deberá ser presentada al titular para que pueda escoger las mejores medidas que beneficien directa o indirectamente a este.

Los procedimientos que se utilizan en el hackeo ético son: "test de penetración, el test de vulnerabilidad y el pestesting" (González Pérez, 2015, págs. 66-70). Las finalidades de estos test radican en establecer cuáles son

los puntos vulnerables que permitan un acceso no consentido, y así mediante pruebas ofensivas, determinar qué tan eficientes son los mecanismos de defensa que tenga este sistema, y así a través de la detección de estas vulnerabilidades, establecer de manera clara, cuál es el riesgo que presentan cada una de ellas, e instaurar las medidas que sean mucho más seguras para el sistema.

Por lo tanto, se puede definir al hackeo ético como "la aplicación de metodologías con el uso de herramientas específicas, para ejecutar pruebas que identifiquen las vulnerabilidades ante una posible intromisión, y así implementar medidas que contrarreste el ataque e impedir la intromisión al sistema" (Osma et al. 2020, pág. 12).

Las fases que generalmente se ejecutan para un hackeo ético son: "el reconocimiento, la exploración, la obtención de acceso, el mantenimiento del acceso, y finalmente el cubrimiento de huellas" (González Pérez, 2015, pág. 13), las cuales son usadas también para un hackeo oscuro. En tal virtud se puede sostener que la misma metodología se usa para determinar las vulnerabilidades e implementar las medidas de seguridad, así como también para una intromisión.

El proceso de hardening es el endurecimiento de las medidas de seguridad que impidan de alguna manera el hackeo a los sistemas informáticos, y el agente de seguridad informática, es quien debe, desde su formación profesional tanto en tecnologías de la información y comunicación, así como en seguridad informática, impedir el acceso no consentido con la implementación de estas medidas de seguridad.

El acceso no autorizado a los sistemas de información

Las TIC se encuentran constituidas por "dispositivos tecnológicos que permiten almacenar, intercambiar, transmitir, editar y producir datos entre diferentes sistemas automatizados de información, mediante la interacción personal con herramientas de intercambio digital" (Desongles Corrales, 2006, pág. 14) a través de los diferentes medios electrónicos o virtuales.

Estos sistemas se encuentran configurados con la finalidad de permitir el acceso al titular o a quien tenga la autorización para poder ingresar al mismo. Las medidas de seguridad que se encuentran impuestas para impedir el acceso no autorizado, son establecidas a través del mismo proveedor del servicio de internet, o en su defecto por el fabricante del software.

El acceso no autorizado o hackeo consiste en la vulneración de las medidas de seguridad de un dispositivo electrónico o un sistema automatizado de información, al que solo puede tener acceso quien tenga la titularidad del mismo, o la autorización para ingresar a este, o también, en una extensión de esta definición, a quienes, con permiso para acceder al sistema, excede la autorización entregada a ellos y ejecutan actos no autorizados por el titular.

La infracción al deber objetivo de cuidado en el delito informático y el Principio de legalidad

Las normas de cuidado son reglas que han sido impuestas en las diferentes actividades que conllevan algún riesgo en su ejecución, y que definitivamente su rebasamiento terminarían en la consumación de una conducta penalmente relevante, como es el caso de los delitos de tránsito o los de mala práctica profesional, en la que sus reglas son de capital importancia para que dentro del riesgo permitido, se pueda ejecutar dicha actividad con la mayor posibilidad de éxito, a pesar de lo riesgoso de la misma.

El infraccionar las reglas de cuidado debe entenderse como aquel acto que rebasa o incumple las normas que fueron impuestas para una actividad riesgosa que permite su ejecución, y que se genera por la falta de "previsibilidad, advertibilidad y evitabilidad del resultado como presupuesto o requisito de la conducta imprudente" (Roxin, 2013, pág. 999).

Hemos explicado que el proceso de hardening se sustenta en la seguridad informática que tiene como finalidad reducir al mínimo las vulnerabilidades que presenta un sistema de tratamiento de información, y que este impide de una u otra manera el acceso no consentido al mismo.

El técnico de seguridad informática es quien realiza los cambios en el sistema para evitar su penetración, por lo tanto, al manifestar que exista una infracción al deber objetivo de cuidado en el delito informático, debemos entender qué es este técnico, quién al rebasar las normas de cuidado, y no ejecutar correctamente este proceso de endurecimiento de las medidas de seguridad, permitiría, por falta de previsibilidad, advertibilidad o evitabilidad, el acceso al sistema por negligencia, impericia o imprudencia en la aplicación de las normas de cuidado.

"El principio de legalidad es la parte central del ordenamiento jurídico penal desde el cual nace la obligación del Estado de administrar justicia, haciendo conocer que la línea coyuntural de dónde proviene dicho principio es el delito, cuya conducta descrita por el legislador se encuentra sancionado con la amenaza de una pena" (Santillán Molina, 2015, pág. 15).

Analizado los tres puntos en los cuales ha sido desarrollado este apartado, se puede determinar primeramente que, en atención al principio de legalidad y principio de

irretroactividad de la ley penal, esta debe ser descrita con anterioridad al acto y principalmente cuando tratamos de delitos imprudentes, no podemos remitirnos tan sólo a una definición generalizada sobre la misma, en cuanto hablamos sobre la imputación al tipo objetivo y la infracción al deber objetivo de cuidado, razón por la cual debemos remitirnos obligatoriamente a la tipificación que el legislador realiza sobre esta.

Es menester explicar, que en la legislación ecuatoriana no se encuentra tipificado el ciberdelito imprudente o culposo. El delito informático esta descrito como una conducta típica y antijurídica que utiliza medios informáticos para ejecutar de manera dolosa algún acto contrario a derecho, sin embargo, no se encuentra descrito en la ley penal la vulneración de los sistemas automatizados de información por negligencia, impericia, inobservancia o desobediencia de aquellas leyes, reglamentos o Lex artis por parte del responsable del proceso de hardening, quién es el técnico de seguridad informática que robustece las medidas de seguridad que impide la vulneración de los sistemas automatizados de información.

METODOLOGÍA

La modalidad de la presente investigación fue cualitativa y para el desarrollo de esta se utilizaron los siguientes métodos:

1. El método histórico lógico tuvo como finalidad el identificar aquellas líneas de investigación que le permiten establecer de manera clara cómo se encuentra descrito el delito informático en el derecho penal moderno.

2. El método analítico-sintético aplicado a las definiciones relativas al delito informático, así como a la imputación al tipo objetivo, a la infracción al deber objetivo de cuidado y aquellas normas que, al ser infraccionadas, permitirían la presentación de una conducta imprudente con el rebasamiento del riesgo permitido.

3. El método de análisis jurídico se aplicó a las diferentes disposiciones legales relativas al delito imprudente, así como el delito informático como tal.

En cuanto a la técnica de investigación científica, se utilizó el análisis de contenido y documentos con la finalidad de establecer sí en otras investigaciones existe una posición científica acorde a lo planteado en la presente investigación, que tenga que ver con la infracción al deber objetivo de cuidado en el delito informático.

DESARROLLO

El hackeo ético como ya lo hemos explicado lo que busca es establecer cuáles son las vulnerabilidades que presenta el sistema automatizado de información, y que el técnico de hardening es la persona que tiene la responsabilidad de manejar un proceso de endurecimiento de las medidas de seguridad para impedir la intromisión.

En tal virtud es necesario establecer que para poder garantizar que un sistema se encuentre seguro, el hackeo ético forma parte fundamental en el proceso de hardening mediante un robustecimiento de las medidas que impidan el acceso indebido a los sistemas.

Las pericias informáticas en la investigación penal

"La base del juicio penal es la comprobación conforme a derecho de la existencia de la infracción, y de la individualización de sus autores y cómplices, mediante el nexo causal que es el vínculo que une la infracción con el responsable. (Santillán, 2014, pág. 45).

En los delitos informáticos es de capital importancia llegar a determinar cómo se cometió la infracción, y una de las formas desde el punto de vista procedimental, es la preservación, extracción, materialización, análisis y valoración de la evidencia digital como elemento fundamental para poder cumplir con la base del juicio penal.

Debemos tener totalmente claro que la obtención de la evidencia digital es eminentemente técnica, en virtud que existen una serie de métodos, procedimientos y aplicaciones que se ejecutan al momento de analizarla, extraerla y plasmarla en papel mediante un informe pericial, y que ésta sirva como elemento fundamental para poder sustentar la manera de cómo se cometió el injusto penal.

Por tanto, podemos decir que a la evidencia digital se le asigna cualquier valor probatorio que permita acceder a la información que ha sido almacenada o transmitida en formato digital, de manera que pueda ser esta utilizada en juicio.

La evidencia digital se caracteriza por ser volátil, eliminable, anónima, alterable y duplicable, al punto de que puede ser alterada, manipulada o modificada mediante el uso de un dispositivo electrónico tales como una tablet, un ordenador o un smartphone, que definitivamente permita la transmisión de datos de manera digital.

El ciclo de vida de la evidencia digital parte desde la identificación que se realiza en el lugar de los hechos, la cual es levantada por peritos criminalísticos informáticos que realizan su recolección, para posteriormente hacer la preservación y aseguramiento en cadena de custodia, con el objetivo de establecer la autenticidad de la misma por orden de fiscalía como responsable de la investigación y autorizado por el juez de garantías penales, para

luego ser peritada con la finalidad de presentar los hallazgos ante las autoridades competentes.

El procedimiento para el análisis de la evidencia digital requiere la obtención de una imagen forense que es una copia exacta del dispositivo que se va a periciar, con el objetivo de que en este último se haga la manipulación y extracción de la información de relevancia para la investigación, y así no alterar, manipular o modificar el elemento que consta como evidencia, sino a la copia espejo, garantizando así su integridad.

Una de las preguntas que generalmente se realiza dentro de las pericias forenses a las que abordamos los abogados, es como poder llegar a determinar si efectivamente la información que ha sido obtenida por parte del perito es exactamente la misma que fue extraída del dispositivo incautado por la Policía Nacional, cumpliendo la orden de Fiscalía General del Estado.

Para esto en la materialización de la copia espejo o imagen forense se le asigna una firma Hash, cuya función criptográfica basada en un algoritmo matemático, permite la transformación de cualquier bloque arbitrario de datos, en una nueva serie de caracteres con una longitud fija, lo que impide que este sea cambiada, por lo que se puede verificar que esta imagen, por más que sea manipulada por el perito en el análisis de la información, nunca cambiará su estructura, por lo tanto será la misma, situación que no pasa cuando se manipula un dispositivo informático, ya que cada movimiento en este genera una serie de datos diferentes.

Generalmente lo que se obtiene de los equipos electrónicos es toda la información relacionada con sus identificadores, marca, modelo, serial y todo dato importante que tenga que ver con el caso investigado. Tratándose de aquellos sistemas automatizados de información que tienen un complejo entramado de funcionalidades, se tiene que remitir obligatoriamente a aquellas aplicaciones o sistemas operativos que permiten ejecutar el sistema de hardening que impide el acceso no autorizado a un sistema automatizado de información.

En informática forense es importante establecer que la parte fundamental para iniciar con una pericia informática es el adquirir, preservar, obtener y presentar aquellos datos que han sido procesados electrónicamente, y que de alguna manera tienen que guardarse mediante un medio digital o computacional.

Se pueden realizar informes periciales sobre cuentas de correos electrónicos tales como Hotmail, Yahoo!, Outlook o corporativos de empresa, de las que se necesitan de la autorización judicial para poder acceder a las mismas, o en su defecto el consentimiento informado en el cual se le confiere la autorización a cada una de las personas que están realizando el peritaje integral.

Así también se puede realizar análisis de cuentas en redes sociales tales como Facebook, Twitter, Instagram o cualquier otra red social que permite el intercambio de información entre aquellos usuarios que han sido debidamente registrados, ya que se trata de información pública que ha sido subida voluntariamente por los titulares para que ésta pueda ser accedidas por cualquier persona que tenga un perfil de usuario en dicha red, y que le permita acceder a esta información mediante la aceptación de amistad, o definitivamente mediante la presentación de imágenes como en el caso de Instagram.

Otra de las pericias que se pueden realizar es el análisis de las direcciones electrónicas en sitios y páginas web, con la finalidad de establecer cuál es el contenido digital que se encuentra alojado en dichos servidores web, documentando de esta manera todas las acciones ejecutadas en estos servidores o dispositivos que alojan la información de manera digital.

Asimismo, con la finalidad de establecer accesos a aplicaciones o archivos, la informática forense también permite acceder a bases de datos mediante la auditoría y revisión de registros, así como reportes que hayan originado un incidente informático.

Se puede hacer un análisis informático a dispositivos de almacenamiento de datos cumpliendo con aquellos principios que enseña la informática forense, mediante la identificación, fijación, preservación, extracción y materialización de la información digital, con el objetivo fundamental de valorar, con la intervención de aquellos investigadores forenses, agentes investigadores policiales y fiscales especializados, cuáles son los elementos digitales localizados dentro del equipo que sirvan para tributar a la consecución de la obtención de la verdad dentro de una investigación penal.

Por lo expuesto, en la investigación de los delitos informáticos, es de capital importancia la evidencia digital con la finalidad de obtener toda la información y sobre ésta de manera técnica, determinar la participación de la persona presuntamente responsable del acto lesivo, así como la identificación del tipo penal y cuál es la conducta penalmente relevante que ha sido ejecutada por el autor del hecho delictivo.

El principio de objetividad en el delito informático

El principio de objetividad en el sistema acusatorio oral recae exclusivamente sobre Fiscalía General del Estado, ya que constitucionalmente esta es la institución que se

encuentra en la obligación jurídica de realizar una investigación de un hecho al cual se cataloga como presuntamente delictivo, del cual se debe de "obtener de manera clara no solamente los elementos de cargo que le permitan al fiscal sustentar una acusación, sino también de aquellos que les sirven como descargo en favor del procesado o investigado" (Santillán Molina, 2015; Ricardo et al. 2021), y así de manera clara, precisa, concordante, unívoca y relacionada, poder llegar a determinar si el hecho se ejecutare de una manera determinada y si la persona que está siendo investigada o procesada ha participado en el mismo.

Los elementos de cargo o de descargo que servirán para sustentar las actuaciones fiscales en una investigación, son aquellos indicios, huellas o marcas que ha dejado la infracción, así como aquellos instrumentos con que se cometió o el resultado de la misma, o cualquier otro medio de información que le permita confrontar de manera clara en un solo bloque probatorio que justifique el nexo causal que une la infracción con sus responsables.

En el ciberdelito las "proposiciones fácticas" (Zavala Baquerizo, 2010, pág. 301) son aquellos elementos qué tienen que ver estrictamente con el uso de los sistemas automatizados de información, en este caso tendríamos los dispositivos electrónicos tales como: tablets, computadoras de escritorio, laptop, smartphone, es decir todo aparato que se encuentre conectado a la red, y que sirva como evidencia digital o electrónica, donde se pueda almacenar, tratar o procesar información que pueda ser obtenida a través de técnicas forenses y que puedan ser visualizadas mediante la presentación documental de estos hallazgos en una investigación fiscal, con el objetivo de determinar cómo se cometió el delito informático.

La aplicabilidad del principio de objetividad en el campo de los delitos informáticos, tiene que ver específicamente con la experticia que para el efecto tenga el fiscal encargado de la investigación y el apoyo de la Unidad de Criminalística de la Policía Nacional para obtener los elementos que sirvan para sustentar una acusación, o en su defecto mantener activo el estado de inocencia en favor de la persona procesada o investigada, al momento de no encontrar elementos que sirvan para sustentar su participación en un injusto penal informático.

Explicación desde la criminalística y la informática el porqué de la importancia en el análisis del proceso de hardening en la aplicación del principio de objetividad.

La criminalística en la actualidad se la considera como una "pieza fundamental del procedimiento penal en la que brinda información veraz y objetiva a los encargados de procurar y administrar justicia" (Ramírez et al. 2005, pág. 175), cuyo objetivo de estudio es el identificar los indicios para reconstruir los hechos del injusto penal, y de esta forma indicar como se cometió el acto lesivo, así como la identificación de sus autores o cómplices.

En el campo que nos ocupa y la obligación del técnico en seguridad informática quien es el responsable del proceso de hardening sobre el sistema de tratamiento de información, es cuando a través de un análisis forense al mismo, se puede llegar a detectar el dolo o la culpa del responsable del proceso, primeramente si fue deliberado al dejar el sistema sin seguridades que permitan el acceso no consentido a los archivos, o por su falta de conocimiento, imprudencia, impericia, o rebasando el riesgo permitido desatendió sus responsabilidades y por descuido permitió la intromisión del hacker oscuro.

Por tanto, al analizar la responsabilidad del técnico del proceso de hardening, primeramente, se debe determinar su participación en cuanto al elemento subjetivo del tipo penal y establecer el dolo o la culpa, ya que, al infraccionar el deber objetivo de cuidado, la imputación objetiva seria directa sobre el agente, pero que necesariamente, de acuerdo al principio de legalidad, esta conducta debe estar tipificada en nuestro ordenamiento jurídico penal para ser punible.

Posada Maya (2017), desarrolla un estudio sobre la imputación objetiva en el cibercrimen, planteándolo desde "la producción de efectos idóneos en el mundo digital directamente o como efecto lógico de los procesos de tratamiento de datos o información por medio de sistemas informáticos" (Maya, 2017, pág. 100), cuyo denominador común es la ejecución del acto indebido por el autor en el interior de un sistema automatizado de información, y que deben tomarse en cuenta los riesgos que aportan en concreto y la existencia de este en el ciberespacio. (Hernández, 2007).

La posición de este autor se sustenta en el nacimiento de la ciberacción y la existencia de resultados lógicos e inmateriales, que se las puede constatar en algunas de las modalidades del cibercrimen, y que en ésta pierde relevancia en nexo de la causalidad tradicional como un nexo natural de pertenencia entre la acción y el resultado material. (Schünemann, 2018).

Esto se refleja en la "interacción entre el autor y la máquina, input-output, cuyas instrucciones electrónicas dadas a la máquina, se encuentran dirigidas a manipular el sistema" (Maya R. , 2012, pág. 236).

En un sentido no muy distante el autor José Agustina sobre imputación objetiva en delitos informáticos considera, que el "ciberespacio es un terreno propicio para generar

una sensación social de inseguridad y miedo conducente a pánico u ofuscación colectiva" (Agustina, 2021, pág. 757), lo que denota que la ejecución del acto se ejecuta en el interior del sistema, sumándose así "una pluralidad de ejecutores con mayor o menor autonomía con el auxilio de IA, inteligencia artificial" (Hildebrandt, 2008, pág. 170).

En este sentido el autor sostiene, que la ejecución del acto lesivo en el interior de un sistema de tratamiento de información, es donde se puede observar la presencia del "yo real o el yo digital", (Maya R. , 2019, pág. 220), el mismo que se refiere a la representación del individuo hacia el resultado final de la acción y las interacciones sociales en el ciberespacio y su conjunción entre el hombre y la máquina, lo que impide, desde su óptica, el establecer una responsabilidad culposa en el autor del injusto penal, mucho más cuando en el ciberespacio el yo virtual, puede dividirse en "múltiples usuarios" de acuerdo al grado de complejidad en el uso de su identidad y de los dispositivos usados.

Los autores mencionados han sustentado, que la ejecución del acto lesivo en los delitos informáticos se encuentra consumado en el interior del sistema automatizado de información, y que en el mismo se utilizan entidades virtuales para su consumación, como en el caso de la construcción de software de inteligencia artificial programados para vulnerar sistemas automatizados de información.

La presente investigación no aborda la ejecución del acto lesivo en el interior del sistema donde efectivamente se pueden utilizar entes virtuales en la consumación del delito informático, sino la falta de previsibilidad por parte del agente de seguridad informática responsable del proceso de hardening, quien infraccionando su deber objetivo de cuidado, por descuido, imprudencia o falta de previsibilidad, permite una intromisión al sistema que está bajo su cuidado, cuya obligación legal o contractual denota responsabilidad de cuidar la no intromisión a dicho sistema.

Por lo expuesto, la comisión de la infracción culposa en el ciberdelito, queda justificada única y exclusivamente para quien tiene la responsabilidad de resguardar que el sistema no sea vulnerado y que por ende impida una intromisión, ya que el delito informático en la actualidad se encuentra descrito desde el dolo como elemento subjetivo del tipo, mas no en la culpa, ya que en nuestra legislación no se ha abordado la conducta desde la previsibilidad, advertibilidad y evitabilidad del resultado como presupuesto o requisito de la conducta imprudente.

CONCLUSIONES

El ciberdelito es de capital importancia el uso de medios informáticos tales como tablets, ordenadores o smartphone que permitan el ingreso físico o virtual a los sistemas automatizados de información, para proceder a su alteración, manipulación o modificación de datos informáticos, como elementos de su antijuridicidad.

Que el hardening es un procedimiento de seguridad informática que tiene como finalidad asegurar un sistema mediante la reducción de sus vulnerabilidades, el cual es ejecutado por un técnico especializado en TIC, así como seguridad informática y de la información.

Que las normas de cuidado en seguridad informática se refiere la previsibilidad con la que debe actuar el técnico al momento de evitar la vulneración del sistema mediante la aplicación de medidas que impidan una intromisión.

Que el infraccionar las reglas de cuidado debe entenderse como aquel acto que rebasa o incumple las normas que fueron impuestas para una actividad riesgosa que permite su ejecución, y que se genera por la falta de previsibilidad, advertibilidad y evitabilidad del resultado como presupuesto o requisito de la conducta imprudente.

Que la teoría de la imputación objetiva se sustenta en la concreción un resultado causado por una conducta humana, cuando dicha acción ha creado un peligro jurídicamente desaprobado, que se ha realizado en el resultado típico y que pertenezca al ámbito de protección de la norma infringida.

Que la responsabilidad legal o contractual del endurecimiento de las medidas de seguridad informática y de la información, recae sobre el técnico quien debe realizar los cambios en el sistema para evitar su penetración.

Que en la fase procedimental en los ciberdelitos y en aplicación del principio de objetividad, es de capital importancia llegar a determinar cómo se cometió la infracción, para lo cual el manejo de la evidencia digital y su peritaje forense es vital para tal fin.

Que al analizar la responsabilidad del técnico del proceso de hardening, se debe determinar su participación en cuanto al elemento subjetivo del tipo penal y establecer el dolo o la culpa, ya que, al infraccionar el deber objetivo de cuidado, la imputación objetiva seria directa sobre el agente.

Que la comisión de la infracción culposa en el ciberdelito queda justificada única y exclusivamente para quien tiene la responsabilidad de resguardar que el sistema no sea vulnerado y que por ende impida una intromisión.

Que el delito informático en nuestra legislación es doloso, pero se ha demostrado académicamente que existe la posibilidad de una conducta culposa abordada desde la previsibilidad, advertibilidad y evitabilidad del resultado como presupuesto de la conducta imprudente.

REFERENCIAS BIBLIOGRÁFICAS

Agustina, J. R. (2021). Nuevos retos dogmáticos ante la cibercriminalidad. Estudios Penales y Criminológicos, 41, 705-777.

Desongles Corrales, J. y. (2006). Conocimientos Básicos de la Informática. Editorial MAD.

Gaviria Trespalacios, J. (2005). La inimputabilidad: concepto y alcance en el código penal colombiano. Revista Colombiana de Psiquiatría, 34, 26-48.

Gómez, Á. (2014). Enciclopedia de la seguridad Informática. Editorial Alfaomega.

González, P. (2015). 'Pentesting'persistente y estratégico: nuevos ataques y nuevos modelos. Red seguridad: revista especializada en seguridad informática, protección de datos y comunicaciones, (68), 66-67.

Hartley, R. D. (2015). Ethical hacking pedagogy: an analysis and overview of teaching students to hack. Journal of International Technology and Information Management, 24(4), 6.

Hernández Basualto, H. (2007). El nuevo derecho penal de adolescentes y la necesaria revisión de su" teoría del delito". Revista de derecho (Valdivia), 20(2), 195-217.

Hildebrandt, M. (2008). Ambient intelligence, criminal liability and democracy. Criminal Law and Philosophy, 2(2), 163-180.

Maya, R. P. (2012). El delito de transferencia no consentida de activos. Revista de Derecho, comunicaciones y nuevas tecnologías, (8), 1-27.

Maya, R. P. (2017). El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual. Nuevo Foro Penal, 13(88), 72-112.

Maya, R. P. (2019). La responsabilidad penal de los agentes de inteligencia artificial: entre la ficción y una realidad que se aproxima. In Un juez para la democracia: libro homenaje a Perfecto Andrés Ibáñez (pp. 561-581). Dykinson.

Osma, J. A. A., González, E. F. S., Aguirre, C. A. P., & Saavedra, M. (2020). Revisión sobre hacking ético y su relación con la inteligencia artificial. Reto, 8(1), 11-21.

Ramírez, S. G., de González Mariscal, O. I., & Casillas, L. A. V. (2005). Temas de derecho penal, seguridad pública y criminalística: cuartas jornadas sobre justicia penal (No. 264). Universidad Nacional Autónoma de México.

Ricardo, J. E., Vázquez, M. Y. L., Palacios, A. J. P., & Ojeda, Y. E. A. (2021). Inteligencia artificial y propiedad intelectual. Universidad y Sociedad, 13(S3), 362-368.

Roxin, C. (2013). Derecho Penal. Parte General. Fundamentos. La Estructura de la Teoría del Delito. Thomsom-Civitas.

Roxin, C., & Vásquez, M. A. A. (2007). La teoría del delito en la discusión actual (pp. 225-258). Grijley.

Santillán Molina, A. (2014). Mas allá de la duda razonable. Estudio aplicado al Código Orgánico Integral Penal. Editorial Jurídica del Ecuador.

Santillán Molina, A. (2015). El proceso penal acusatorio y la aplicación de los principios. Editorial Jurídica del Ecuador.

Schünemann, B. (2018). Dominio sobre la vulnerabilidad del bien jurídico o infracción del deber en los delitos especiales. Derecho Pucp, (81), 93-111

Suarez, A. (2016). Manual de delito informático en Colombia. Análisis dogmático de la ley 1273 de 2009. Universidad Externado de Colombia,

Zavala Baquerizo, J. (2010). Tratado de Derecho Procesal Penal (Vol. II). Edino.