REVISTA INTERNACIONAL
TECNOLÓGICA – EDUCATIVA DOCENTES 2.0
ISSN: 2665-0266 / VOL.9 (1), ABRIL 2020
https://doi.org/10.37843/rted.v9i1.89

CONGRESO INTERNACIONAL VIRTUAL
SOBRE LAS TECNOLOGÍAS DEL APRENDIZAJE
Y DEL CONOCIMIENTO

EDICIÓN: CIVTAC

Recibido: 19 de febrero de 2020
Aceptado: 2 de marzo de 2020
Publicado: 10 de abril de 200

Dirección autor:

[1]Universidad Regional Autónoma de los Andes, extensión Ibarra-Ecuador

Ecuador

E-mail / ORCID:

crespoberti@gmail.com

https://orcid.org/0000-0001-8609-4738

APA

Crespo-Berti, L. (2020). La acción nuclear del delito informático en la novísima reforma parcial del código orgánico integral penal. *Revista Tecnológica-Educativa Docentes 2.0, 9(1), 17-27.* https://doi.org/10.37843/rted.v9i1.89

IEEE

L. Crespo-Berti, "La acción nuclear del delito informático en la novísima reforma parcial del código orgánico integral penal", *RTED*, vol. 9, n.º 1, pp. 17-27, abr. 2020.

La Acción Nuclear del Delito Informático en la Novísima Reforma Parcial del Código Orgánico Integral Penal

The Nuclear Action of Cybercrime in the Latest Partial Reform of the Integral Criminal Organic Code

Luis Andrés Crespo-Berti[1]

Resumen

La investigación estableció las consecuencias que apareja el significado de la acción nuclear como elemento sustantivo de carácter penal en los delitos informáticos, previstos en el Libro I de la reciente reforma parcial de la codificación penal sustantiva ecuatoriana (2019). El objetivo consintió en realizar una interpretación en la calificación de la infracción desde el ámbito cibernético. La perspectiva trasciende por el grado de subjetividad de parte del legislador, al prescribir en modo subjuntivo la acción nuclear. El diseño de la investigación se inserta en el paradigma cualitativo, tuvo la característica de ser de tipo factible, en un nivel explicativo y de ordinario el método modelado de comparación constante, el exegético y el de las estructuras lógicas. Su finalidad fue la de explicar el comportamiento de una variable en función de otra. Los resultados proporcionaron comprobaciones como que el Estado ecuatoriano, a través del ejercicio de la acción penal debe operacionalizar en términos exegéticos, la adecuación de la conducta desplegada a los efectos de calificarlo adecuadamente *ab initio* del proceso penal para la correcta tipificación del delito perpetrado. Como corolario, la exégesis versus la génesis del comportamiento del infractor en consonancia con la consciencia y voluntad del acto volitivo.

Palabras claves: Acción nuclear, delitos informáticos, telecomunicaciones, telemática, seguridad informática.

Abstract

The investigation established the consequences of the meaning of nuclear action as a substantive element of a criminal nature in computer crimes, provided for in Book I of the recent partial reform of the Ecuadorian substantive criminal codification (2019). The objective agreed to make an interpretation in the classification of the infraction from the cyber field. The perspective transcends by the degree of subjectivity on the part of the legislator, by subjectively prescribing nuclear action. The research design is inserted in the qualitative paradigm, it had the characteristic of being of the feasible type, on an explanatory level and ordinarily the modeled method of constant comparison, the exegetical and that of the logical structures. Its purpose was to explain the behavior of one variable according to another. The results provided verifications such as that the Ecuadorian State, through the exercise of the criminal action must operationalize in exegetic terms, the adequacy of the conduct displayed in order to properly qualify it ab initio of the criminal process for the correct criminalization of the crime perpetrated. As a corollary, exegesis versus the genesis of the offender's behavior in line with the consciousness and will of the volitional act.

Keywords: Nuclear action, Cybercrime; telecommunications, telematics, computer security.

ISSN: 2665-0266 / Depósito Legal: LA2017000128 / ISBN: 978-980-18-0874-9. Volumen 9. No. 1. Abril 2020

Introducción

La teoría en que se fundamenta los hechos investigados reside en la acción nuclear del delito informático tras las reciente Ley Reformatoria del Código Orgánico Integral Penal, Registro Oficial Suplemento 107 del 24 de diciembre de 2019, codificación penal ecuatoriana focalizada en el comportamiento que ensaya el agente comisor del infortunio penal *in comento* con alcance específico en el empleo de Tecnologías de la información y comunicación (TIC), a través del uso indebido de las redes sociales en atención a la violación del objeto jurídico protegido por el Estado como lo es precisamente el constructo seguridad de los activos de los sistemas de información y comunicación.

El talante organizativo recayó en la realización de una valoración semántica-gramatical-legal en términos de calificación del delito informático, por cuanto abona gran interés dentro del estudio de estas disciplinas que dan paso a entidades paritarias lingüística-jurídica (Crespo-Berti, 2017a & Carrió (2011).

La integración de este dominio científico ofrece un componente resoluble en la determinación imputable del delito informático. Para el desarrollo del tópico, se abordaron los emergentes factores, el cognitivo expresado por: (a) exteriorización del pensamiento con base en la conducta lesiva del agente perpetrador y; (b) normativo, codificado legislativamente como acto típico, antijurídico y culpable, dando paso al análisis exhaustivo, interpretación y comparación constante de lo que acontezca en torno a las vicisitudes del proceso penal incoado al procesado por el supra mencionado delito informático.

En tal sentido, conceptualmente se define como delito informático inserto en el ámbito cibernético, contexto desarrollador de violencia y más de cerca desde el foco doctrinario como ciberdelito (Ley Orgánica Integral de Prevención y Erradicación de Violencia de Género contra las Mujeres, 2018). En palabras del agente investigador de policía judicial adscrito al Cuerpo de policía técnica especializada en criminalística se lo conceptualiza como: (…) “toda aquella acción antijurídica que se realiza en el entorno digital, espacio digital o de internet”. (Lara, 2020).

Es así como confluyen los delitos informáticos, cuyo medio de comisión se verifica con el empleo ilícito de dispositivos tecnológicos de difusión masiva con la finalidad de causar daños, provocar pérdidas o impedir el uso de sistemas informáticos, verbigracia de: grabaciones y fotografías sin consentimiento o autorización legal; suplantación de claves electrónicas; daño o pérdida intencional de información; violación de intimidad de las personas, entre otras.

El tópico, por demás retador, dada su condición *sui genéris*, a más del afán de destacar preeminentemente su valor agregado en el abordaje, se procedió a explicar la acción nuclear del delito informático derivado del principio constitucional de legalidad consagrado en el Capítulo Octavo, Artículos 75, en lo atinente a los derechos de protección: “Toda persona tiene derecho al acceso gratuito a la justicia y a la tutela judicial efectiva, imparcial y expedita de sus derechos e intereses (…) en ningún caso quedara en indefensión”. (Constitución del Ecuador, 2008).

En lo tocante al punto nodal del problema, se traslada en perspectiva creciente sobre la estructura de los tipos penales como producto del tecnicismo legisferante vista como acto político (Zafaronni, 2009). Puede sostenerse si los actores intervinientes en el proceso penal *per se*, es exhaustivamente encuadrada de conformidad con el verbo rector que expresa la acción delictiva, a propósito de las características gramaticales que el legislador expresa en el modo subjuntivo de cara al tipo penal, lo que genera una posición subjetiva asumida por la legislatura nacional.

Con base en los supra argumentos expuestos, mismos que aterrizan en la dimensión semántica del modo gramatical presente en la redacción de los tipos penales informáticos que el legislador reitera en el catálogo sustantivo en lo atinente desde el foco de los delitos informáticos tasados en valores afirmativos (a) hipotéticos; (b) inciertos o; (c) las presunciones caracterizadas por el rasgo *Irrealis* antagónico al *Realis* del modo indicativo expuesto en el estilo redaccional del legislador, expresado en modo subjuntivo, lo que a ciencia lingüística cierta traduce en el habla expuesta en el derecho positivo un modo subjetivo en lo que atañe al diseño gramatical del mandato advertivo punitivo que deviene del supuesto legal del hecho del tipo.

En primer lugar, se requiere de un examen exegético de parte del titular del ejercicio público

ISSN: 2665-0266 / Depósito Legal: LA2017000128 / ISBN: 978-980-18-0874-9. Volumen 9. No. 1. Abril 2020

de la acción penal con una proyección secundaria hacia el juzgador y finalmente, en defensa técnica antes (indagación previa) y durante la fase del procedimiento penal (instrucción fiscal), la subsunción conductual penal del *Sub judici* de Autos y adecuarla correctamente al tipo violado, quienes deberán reducir en adecuación al *Tipo* hacia una valoración semántica y gramatical del núcleo sesgando toda posibilidad cierta y determinada de una incorrecta calificación del delito como en efecto pudiera ocurrir desde la esfera del Ministerio fiscal (Crespo-Berti, 2017b).

En vínculo con lo anterior, se sostiene que el operador de justicia que aplica la ley pudiera incurrir en iniquidad y no al ejercicio reglado, inmanente en todo Estado democrático de (…) "deberes y derechos individuales y sociales vistos como garantías fundamentales" (…) (Artículo 76, Numeral 6, constitucional), en tanto y en cuanto se trate de la concreción justa del tipo penal.

Se pretende entonces, significar la importancia del núcleo esencial previsto en el precepto legal que por imperativo o de prohibición sea vulnerado, pues en esencia, blindará de protección al procesado en virtud del derecho de rango constitucional defensorial en todo estado y grado del proceso y a la propia administración de justicia no habiendo lugar a la *Contraditio in terminis*.

De otro lado, es imperioso la exégesis en una misma unidad de tiempo, básicamente de los elementos básicos de las súper estructuras del tipo por encontrarse allí el núcleo rector, vale decir, la acción nuclear del delito informático.

Dicha contribución vertebra en profilaxis de atenuar en términos eufemísticos posible arbitrariedad, abuso, equivocación, desacierto por error excusable o en sentido *lato sensu*, juicio o criterio falso llegada el momento de calificar el delito informático imputado en tanto y en cuanto atañe al comportamiento ilegal como elemento normativo, previendo incurrir en los siguientes supuestos: (a) recurrencia facultativa del juez en ejercicio del principio discrecional en reducción al criterio objetivo acorde con la normativa; (b) adecuación entre los factores intervinientes en el proceso penal frente a la situación fáctica que se ventila; (c) la dinámica jurisdiccional no se limita a establecer las pruebas del hecho que acrediten el mecanismo que subsume el tipo penal (Constitución 2008, Artículo 76, Numeral 4); (d) la exclusión deductiva subjetiva focalizada del juez e inducción a su vez a la valoración objetiva a los efectos de comprobar la antijuridicidad de la conducta del comisor.

Entre tanto, el concepto metodológico asumido fue de tipo interpretativo al determinar la etiología del fenómeno en ciernes al generar un sentido de entendimiento en forma estructurada. Se precisa el método cualitativo y de ordinario el deductivo, el de comparación constante, el analítico, el sintético, el exegético, el hermenéutico, el crítico inferencial y el lógico-histórico (Supo, 2014; Crespo-Berti, 2017 & Hernández et ál., 2014), lo que favoreció en la investigación hipotética en ciernes: ¿Qué incidencia tiene la debida interpretación del comportamiento infligido por el agente comisor versus el delito informático perpetrado frente a los distintos factores intervinientes en el proceso penal ecuatoriano? A los efectos de esta, el objetivo general del estudio quedó circunscrito en realizar una interpretación calificadora del delito informático de parte de los factores intervinientes en la esfera del proceso penal.

Estas relaciones jurídicas de poder se caracterizan –en lo que respecta al individuo como sujeto jurídico– en tendencia al no admitir su culpabilidad penal, incluso por derecho propio como mecanismo de defensa de no auto incriminarse en todos los casos en que tales circunstancias sean perseguidas por la justicia.

Desarrollo

A tenor de Muñoz (2008), quien sostiene que: "Las teorías surgidas a partir de las orientaciones funcionalistas dominan el constructo penal". (p. 88). Las garantías constitucionales consagran la potestad (Ius Puniendi) en que debe sustentarse la norma penal. Estandarización versus diferenciación elemental de estudio del contenido y funcionamiento del sistema jurídico penal.

Se afirma como opera el constructor de los tipos penales: El coideario Alvarado (2007), deja en evidencia que: "El tipo penal debe tener elementos suficientes para determinar cuál es la conducta que se encuentra prohibida u ordenada, expresándose así

ISSN: 2665-0266 / Depósito Legal: LA2017000128 / ISBN: 978-980-18-0874-9. Volumen 9. No. 1. Abril 2020

el principio de legalidad. De lo contario, contravendría un mandato constitucional" (p. 292).

Así, en materia penal, se prescribe el deber de prescribir un hecho y asociarlo a una pena. En su clásica formulación, el aforismo con el que se le identifica en latín: *Nullum crimen nulla poena sine lege*, se derivan 4 subcomponentes, mejor conocidos como subprincipios ponderables:

1. *Lex Stricta*: envuelve prohibición por analogía, por su aforismo: *Nullum crimen nulla poena sine lege stricta*.
2. *Lex Scripta*: implica posibilidad cierta y determinada de garantizar la prohibición del derecho consuetudinario para fundamentar y agravar la pena, por su aforismo: *Nullum crimen nulla poena sine lege scripta*.
3. *Lex Praevia*: prohíbe retroactividad de la ley penal más severa, por su aforismo: *Nullum crimen nulla poena sine lege praevia.*
4. *Lex Certa*: impide leyes penales y penas indeterminadas. Por su aforismo: *Nullum crimen nulla poena sine lege certa*.

Todo postulado axiológico en una dimensión desde los referentes empíricos apertura una ventana de expectativa valorativa hacia un contexto social y democrático más humano y, más equitativo visto como uno de los principios generales más sublimes del derecho.

Verificado de lo que resulta de los planteamientos anteriores, los hallazgos provenientes surcan sistémicamente hacia la hermenéutica expuesta por el legislador en el diseño del supuesto legal del hecho punible, que recae sobre un sistema abierto de comunicación inserto en el Código Orgánico Integral Penal de 2019, en el seno de la convivencia social en estrecha relación semántica al redactar preceptos normativos penales que las contiene.

Se discute que, para una mejor interpretación por parte de los actores intervinientes en la determinación del delito cometido, sea practicado un análisis exhaustivo de las estructuras de los tipos penales, verbigracia del núcleo rector, a los efectos de precisar en términos exegéticos su justa calificación infraccional en aras del principio de celeridad y economía procesal y más de cerca la institución de la defensa técnica.

Adicionalmente, en un intento de aporte, es promover postura transcompleja en cada uno de los sectores comunidad científica-academia-tribunales con competencia en materia penal en funciones de control en su labor de impartición de justicia, respecto a la perspectiva unificadora del lenguaje en atención al dictamen calificatorio del delito al incoarse un proceso penal. Indagatoria acorde con el objetivo general del estudio.

En el marco de las consideraciones anteriores, se precisa convenir que de las tres categorías o modalidades que encierran los núcleos (simple, complejo alternativo y complejo compuesto), que presentan las normas penales, plurivalencia que el legislador le imprime en su concreción, coadyuvará *In bonam partem* como método de interpretación válido integral del sistema normativo penal al no encuadrar a todas las normas penales en un sistema unitario, lo que favorecerá su ceñido al enorme e ilimitado descriptor que encierra la acción, vista como la exteriorización (aspecto cognoscente) en la internalización del *Iter criminis* (camino criminal), endógeno y consentido del agente comisor visto como la querencia de producir un resultado lesivo en los delitos intencionales o por el contrario, que opere la culpa con o sin representación.

Partiendo del presupuesto medular con base en la estructura simple de una norma penal entendida como regla de comportamiento compuesta por el precepto normativo (supuesto legal), conocido como el *Tipo* sancionatorio *Punibilidad* (consecuencia jurídica), misma que apareja una pena restrictiva de libertad y de los derechos patrimoniales. Por tal virtud, Muñoz Conde (2007), expone: "Como toda norma jurídica la norma penal consta de un supuesto de hecho y de una consecuencia jurídica." (p.14).

Se afirma que lo anteriormente sostenido, tiene su base en el análisis de la teoría general del delito fenómeno de identidad de la ley penal. En el plano internacional resaltan los postulados de: Politoff, Matus, & Ramírez (2004); Mir Puig. (2004); Luzón Peña (1996); Rodríguez Devesa & Serrano Gómez (1995), entre otros. Notables que influenciaron enormemente con sus pensamientos y planteamientos pasados en la evolución doctrinaria del delito, al papel que juegan la memoria histórica

ISSN: 2665-0266 / Depósito Legal: LA2017000128 / ISBN: 978-980-18-0874-9. Volumen 9. No. 1. Abril 2020

y el contexto en su desarrollo. En el ámbito regional es también punto de contención, por tanto, en menester mencionarse los trabajos de: Peña & Almanza (2010); Garrido Montt (2003); Etcheberry (2001): Estos investigadores destacan la actualidad, pertinencia y prioridad de este tema.

Parafraseando queda patentizado universalmente que toda norma penal conforma una estructura lógica semántica que formula una carga deóntica, expresada mediante un orden dual condicional, a saber: el precepto normativo sumado a lo punible (Alvarado, 2007).

El modo semántico redaccional acogido por el legislador patrio confecciona normas penales integrales por un primer aspecto hipotético que viene dado por el comportamiento y un segundo pronunciamiento hipotético que acarrea una consecuencia ante su inobservancia. De tal manera que, desde el foco del apostolado general del delito, se reconoce a esta dualidad de confirmaciones en sintonía con la dogmática penal como supuesto y consecuencia jurídica respectivamente.

Queda claro que la prescripción imperativa del mandato o prohibición es en esencia el supuesto jurídico al que en doctrina penal reconoce distintivamente como el *Tipo*, constituye la parte de la norma que tácitamente contiene el elemento deóntico que tanto en la dogmática jurídico penal recibe el nombre de *Deber Jurídico* como fundamento del tipo penal. Respecto a esta última noción, el referente Islas (1991) adoptado, define deber jurídico como: "La prohibición o el mandato categóricos en un tipo penal." (p.77).

Con referencia a la contención que supone los deberes condicionados en los mandatos advertivos punitivos positivos o negativos que el legislador le imprime en la concreción de normas penales, lógicamente necesarios de naturaleza predominante descriptivos e imperativamente referidos como un hacer, o de prohibición como no hacer, lo que ciertamente constituye normas penales.

No obstante, de las incidencias que se produzcan, para el Estado ecuatoriano, exigir el control y mitigación del delito es materia de vital importancia. El mayor desafío para el gobierno y para las instituciones que combaten la dinámica criminógena, es lograr minimizar la manifestación delictual en desmedro del colectivo social (Crespo-Berti y Benavides, 2018).

Esta situación hace que las corporaciones judiciales encargadas de reprimir el expansionismo delictual se vean necesariamente el replanteo nuevos retos y nuevas alternativas que le garanticen mayor eficacia en su encargo; asimismo, una mayor integración y cooperación interna, en procura de atenuar el delito que por sus efectos desestabilizadores serpenteantes avanza consecuencialmente con mayor fuerza y se afianza en el *Modus vivendi* de una parte de la población.

En este sentido, Gargarella (2012), arguye lo siguiente: "Mi escepticismo ante la tarea de los órganos políticos (el Parlamento, el poder ejecutivo) parte de la convicción de que tales órganos distan de funcionar de un modo aceptable, como distan de representar adecuadamente a la ciudadanía". (p.29).

Por las insuficiencias sustantivas expuestas de manifiesto es necesario y fundamental que el legislador patrio al establecer una norma penal, la diseñe de una forma clara, precisa, concisa y concreta en cumplimiento con la dogmática jurídica, sus diferentes teorías, enfoques y doctrinas que apunten al ejercicio pleno del derecho penal de conformidad con la sinestesia del lenguaje (Crespo-Berti, 2017a).

Estructura básica de los tipos penales informáticos

Parte del problema central planteado bajo la percepción fundante de considerar el sentido común (forma habitual y diligente de avocamiento), que recae en el estudio de los elementos estructurales básicos de los tipos penales, en luminiscencia de la acción nuclear.

Las estructuras básicas de los tipos penales quedan circunscritas bajo los siguientes componentes:

1. Sujeto activo: Recae *Intuito personae* quien exterioriza, planifica y ejecuta (*Iter criminis*) la acción penal en detrimento de un bien jurídico protegido. El sujeto activo del delito puede ser indeterminado o calificado por el mismo alcance prescrito normativamente.
2. Sujeto pasivo: Consiste en la víctima, misma que también puede ser calificada por el legislador, tal es el caso de pornografía infantil, por ejemplo, necesariamente tendrá que ser una niña, niño o adolescente. Lo que

ISSN: 2665-0266 / Depósito Legal: LA2017000128 / ISBN: 978-980-18-0874-9. Volumen 9. No. 1. Abril 2020

se sanciona es que se fotografíe, filme, grabe, produzca, transmita o edite -núcleo complejo alternativo- materiales informáticos (…) "electrónicos o de cualquier soporte físico o formato que contenga representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual" (COIP, 2019; Articulo 103). Desde el punto de vista fenomenológico, puede existir pluriofensividad en el sujeto pasivo, es decir, hoy día y dadas connotaciones presupuestarias victimológicas revitalizada por la criminología vista como una Ciencia auxiliar al Derecho penal, pueden ser consideradas víctimas parentales consanguíneos, afines y colaterales incluso. Aspecto con el que se coincide plenamente, porque en el abusado genéricamente hablando, verbigracia ¿quiénes son los que sufren el resultado lesivo infligido al párvulo? Obviamente que; los progenitores, los parientes y ascendentes verticalizados, los colaterales o cualquiera que propicie muy de cerca o le una un lazo de afinidad, incluso de haberlo, el tutor como ocurre con relativa frecuencia en estos estratos sociales tan vulnerables.

3. Núcleo**:** Fenómeno objeto de estudio.

4. Objeto material: Consistente en un equipo o dispositivo de telecomunicación, concepto que comprende todos aquellos componentes mediante el establecimiento a distancia entre personas, ordenadores y redes de sistemas (Salvadori, 2011, p. 27-53).

5. Objeto jurídico: Realidad corpórea o intangible susceptible considerado como bien jurídico. Constituye uno de los elementos positivos adjetivos del delito que recae sobre la antijuridicidad de la conducta que para el caso objeto de estudio radicar en: seguridad de los activos de los sistemas de información y comunicación, razón última del derecho penal.

En contexto el catálogo sustantivo recoge su enunciación en el Libro Primero, Capítulo III, Sección 3ra. Artículos del 229 al 234, ambos inclusive: Delitos contra la seguridad de los activos de los sistemas de información y comunicación. De igual modo, también entran en el mote de los delitos informáticos los normados en los Artículo 103, 173, 174, 178 (Código Orgánico Integral Penal, 2019).

Entra tanto el sujeto activo del hecho punible reside en personas habilidosas que infligen la ley, vistas como aquellas que poseen ciertas pericias exponenciales que no presenta el denominador común de los delincuentes. Tales infractores ostentan conocimiento en la manipulación de *softwares*, por lo general operan desde su entorno laboral al desempeñarse como operarios de sala de máquinas. En otros casos, actúan en concierto en lugares clandestinos con cierta sofisticación de *hardwares* destinados con fines inescrupulosos, en un intento de perpetuarse al lado del delito.

Con el avance del tiempo se ha podido comprobar que los autores de los delitos informáticos son de diversa clase. Se diferencian por la naturaleza de la actividad ilícita que despliegan. Se caracterizan por ser osadas (Acurio del Pino, 2015). De esta forma, la persona que accede a un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

Desde el foco de lo perceptivo versus lo persuasivo la doctrina clasifica una diversidad de sujetos activos existentes, entre los que figuran: (a) *hackers;* (b) *crackers;* (c) *lamers;* (d) *newbie o;* (e) *script kiddie*. El *hacker* con capacidad de dominar en buena medida varios aspectos simultáneos como son: lenguajes de programación, manipulación de *software*, telecomunicaciones, así como también es capaz de precisar lo franqueable que puede ser un computador o una red informática. Obviamente que el fin último es el afán de lucro, más sin embargo es muy visceral su querencia, desde darse a conocer, por motivación, pasatiempo hasta para realizar actividades sin fines lucrativos, incluso como *hobby*.

Tipología de la ciberdelincuencia

Por esta forma de criminalidad informática desarrollada por los *hackers,* con frecuencia se refería al entorno *underground* de computadoras. Su rápida maniobra conlleva a que sea entendida como una comunidad abierta. Por lo generalizado que se hallan los *hackers,* han pasado de ser grupos clandestinos a comunidades identitarias bien definidas. Por sus objetivos el *hacker* posee un alto

ISSN: 2665-0266 / Depósito Legal: LA2017000128 / ISBN: 978-980-18-0874-9. Volumen 9. No. 1. Abril 2020

grado de conocimiento en tecnologías. Básicamente son clasificados por la doctrina e incluso legalmente como: (a) *hackers* de sombrero negro; (b) *hackers* de sombrero gris y; (c) *hackers* de sombrero blanco.

El apelativo atribuido al *hacker* de sombrero blanco recae en el individuo quien rompe los códigos fuentes de seguridad por razones inintencionales para poner a prueba la seguridad de su propio sistema o mientras labora en una sociedad mercantil en la producción de aplicaciones computacionales de seguridad. En el contexto cibernético, la denominación sombrero blanco alude a un *hacker* ético. Además, esta categoría incluye a individuos que procesan pruebas de accesos, evaluaciones de vulnerabilidad, entre otros en el marco de un convenio establecido. El Consejo Internacional de Consultores de Comercio Electrónico (EC-Council), ente desarrollador de aprendizajes en línea, abarca al *hacker* ético. Además, existen certificaciones como *Certified Professional Ethical Hacker* por su acrónimo CPEH, así como *Certified Penetration Testing Engineer* (CPTE), acreditadas por la Agencia Nacional de Seguridad de los Estados Unidos (NSA) e Iniciativa Nacional para los Estudios de Carreras en Ciberseguridad de los Estados Unidos (NICCS).

El *hacker* de sombrero negro es un individuo que infringe políticas de seguridad informática para beneficio personal por razones pérfidas. Configuran el prototipo temido de un criminal informático. Los *hackers* de sombrero negro acceden sin autorización a redes seguras para dar cuenta de datos e información ajena con fines maliciosos.

El *hacker* de sombrero gris es un personaje que actúa en concierto con otros *hackers* de sombrero negro. Éste posee pericia de navegación por Internet. Vulneran partes informáticas interrelacionadas a propósito de comunicarse *A posteriori* con el administrador del sitio *Web* de su dominio por presuntas averías. Praximetría fraudulenta en ejecución de lucro en el ofrecimiento a título oneroso la solución al problema implantado.

El *craker* al igual que el *hacker*, también es proclive al mundo informático. Como principal diferencia por su finalidad es producir un daño a los sistemas *software* con incidencia en los ordenadores, computadores personales (PC). El término *cracker* en inglés equivale a intruso, rompedor, sus objetivos generales son: violar ilegal o moralmente un sistema cibernético, producir el mayor daño posible. Usualmente el concepto *hacker* se confunde con el de *cracker* siendo que los principales acusados de ataques a sistemas informáticos se han denominado *hackers* en lugar de *crakers* (Sarasola, s.f.).

Entre tanto, el adiestramiento del *cracker* se traduce en desprogramar los dispositivos computacionales protegidos (descodifica, contamina, vulnera), ya que los programas desde su originalidad son blindados por activación seriada. Otros hacen la activación por medio de artificios con base en procedimientos de registro vía *web* u otro mecanismo físico (activación por hardware) o por algún archivo de registro. El crackeo de *software* es una acción ilegal en prácticamente todo el mundo, dado que para lograrlo es necesario utilizar inversamente el ingenio que conlleva a sortear las limitaciones que fueron impuestas por el autor para evitar su copia ilegal (Sarasola, s.f.).

El *lammer* es un individuo que aparentemente ostenta varias habilidades como las del *hacker*, aspecto que no es correcto. Esta categoría de antisociales suele se principiantes, poseen escaso conocimiento sobre informática. En su mayoría, el *lammer* ejecuta visitas en sitios *web*, descarga programas que hayan diseñado ingenieros o telemáticos con conocimiento previo, luego generan ataques con ese *software*, pese en no tener conocimiento sobre el verdadero *hack* de una computadora. El riesgo que se corre con este tipo de personas reside en el frenesí del empleo de herramientas nuevas que hagan vulnerable los sistemas automatizados.

El *newbie* es aquel principiante en modo de *hacking*, vale decir, es un *hacker amateur*. Intenta ingresar a sistemas s*oftware* con ciertos obstáculos por su poca pericia. De esta forma ganan práctica en aprender las técnicas de *Malware (malicious software),* a los efectos de infiltrarse en un sistema para dañarlo o para sustraer datos. Por lo general son discípulos de terceros expertos (*hackers*) experimentados para emular sus objetivos en la generación de resultados lesivos. Los *newbies* son más prudentes que los *lammers*, asimilan los métodos de *hacking*, de allí su apasionamiento informático hasta llegar a convertirse en un *hacker*.

ISSN: 2665-0266 / Depósito Legal: LA2017000128 / ISBN: 978-980-18-0874-9. Volumen 9. No. 1. Abril 2020

El *script kiddie,* es el último eslabón de los capos *web*. Se trata es su más pura esencia de simples usuarios de Internet, sin conocimientos sobre *hack* o *crack*. En realidad, poseen claras tendencias maliciosas en insertarse en el mundo del delito, aun cuando no son duchos en el medio; pero lo intentan. Simplemente son internautas que se limitan a recopilar información en las redes sociales, convirtiéndose en futuros antisociales. Claramente, mal gastan su tiempo en búsqueda hallazgo de programas de *hacking* en la Red con miras a ejecutarlos sin las debidas precauciones sin percatarse intencionalmente de las advertencias de intervención de cada aplicación. Con esta acción, liberan *Exprofeso* virus residentes en memoria de los ordenadores; de acción directa; de sobreescritura; de sector de arranque; marco virus polimórficos; de secuencias de comando *web* por doquier, entre otros. Esta conducta conlleva a aplicaciones de *hacking.*

Es así como el fenómeno criminal en el Ecuador con tendencia natural del cometimiento delictual, dada las crecientes modalidades de violencia acaecidas que encarna el riesgo-país, en aras de contrarrestar el ataque frontal del ciberdelito, demanda una mayor propuesta de represión punitiva.

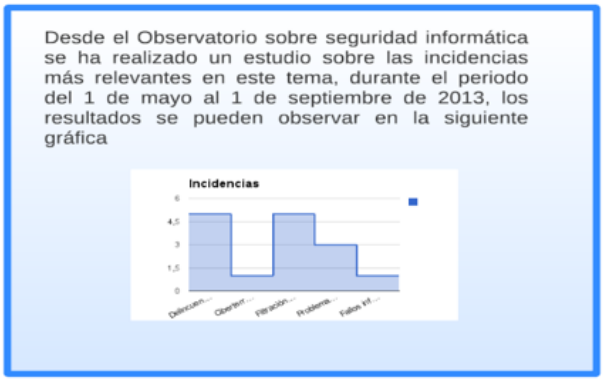
Los avances legislativos en el Ecuador alcanzados recientemente representan una oportunidad extraordinaria de afrontar los nuevos brotes de criminalidad, dada la propensión de adecuar los tipos penales informáticos tomando en cuenta el amplio espectro que supone las Ciencias penales en atención a su Ley Fundamental (2008).

De acuerdo con las estadísticas llevada por el ente rector competente, éste es, unidad de análisis de información del delito del Ministerio del Interior (sistema DAVID), los delitos informáticos de mayor trascendencia nacional a nivel de cometimiento figuran sin priorizar los siguientes:

1. Pornografía infantil.
2. Violación del derecho a la intimidad.
3. Revelación ilegal de información en base de datos.
4. Interceptación de comunicaciones.
5. Pharming / Phishing (infección del servidor del sistema de nombres de dominio DNS o al propio ordenador del usuario en suplantación de identidad respectivamente).
6. Fraude informático.
7. Ataque a la integridad de sistemas informáticos.
8. Delitos de información pública reservada legalmente.
9. Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.

Gráfico 1

Problemas en la seguridad informática



Nota. Elaborado por D. Fernández, 2013.

Del indicador gráfico se desprende con mayor incidencia en la situación problémica con base en la tensión seguridad informática responden básicamente al ataque de la delincuencia informática *Per se*, por ascendencia de filtración de por ascendencia de filtración de datos con una proyección secundaria a los problemas de seguridad. Entre tanto, las categorías paritarias de menor impacto recayeron en el ciberterrorismo en igualdad de condiciones con fallos informáticos. Se colige que mientras más avances tecnológicos surjan, mayor arraigo situacional-conflicto de ataque informático (Fernández, 2013).

De otro lado, desde el foco del cuerpo de seguridad del Estado, el organismo de policía nacional sugiere en adopción atenuante del delito informático ciertas acciones a ser consideradas para evitar en lo posible victimización:

1. No publicar información personal en portales *web* desconocidos o redes sociales.

ISSN: 2665-0266 / Depósito Legal: LA2017000128 / ISBN: 978-980-18-0874-9. Volumen 9. No. 1. Abril 2020

2. No confiar en ofertas o precios muy bajos al comprar cualquier servicio.
3. Crear contraseñas seguras.
4. No compartir con otras personas claves de seguridad.
5. No guardar contraseñas en computadores públicos para evitar las estafas.
6. Verificar cuentas bancarias en computadores personales.
7. Tener instalado un buen antivirus.
8. Conservar los mensajes, correos electrónicos con información indebida.
9. No confiar en correos electrónicos desconocidos. Verificar el spam continuamente para mirar quien está a la zaga.
10. Supervisar constantemente cuando un menor de edad se encuentra en la red.

Particular interés merece la función legislativa, no sólo en el alcance redaccional de las normas sancionadoras del delito informático, sino cómo categoriza el núcleo que las componen. Se aporta nociones del cómo debiera hacerse una valoración lingüístico-legal tomando en consideración los efectos que de ello se desprenden. Se pretendió resignificar el idóneo proceder en la argumentación político-legislativo- que relaciona el mandato advertivo punitivo en atención al criminal oculto (Magliona & López, 1999), dejando un claro mensaje al colectivo social por los fines que persigue.

Dicho hallazgo demandó describir previamente en qué contexto sociopolítico se desarrolla la función legislativa en la actualidad, que se adopten decisiones incriminadoras como resultado de un análisis a fondo. Se deja una ventana abierta para que estudios de menor o mayor complejidad, induzcan propositivamente al progreso legislativo en concordancia con la legitimidad material del Derecho penal.

Conclusiones

Analizada la etiología que describe el proceso de actualización del Derecho penal, *In bonam partem* en la integración del sistema normativo penal, se apunta cuál debe ser el rol del penalista frente a la situación *In comento*; quehacer que vertebra en subsunción del hecho punitivo para con la calificación del delito en aras de evitar retrasos procesales que incidan en reposición de causas, todo de conformidad con el principio de celeridad en correspondencia con el de economía procesal.

Por razones de hecho y de derecho, el principio de legalidad sancionado por el pleno unicameral (2014), en el Artículo 5, Numeral 1**,** subsume inequívocamente los hechos punibles. Formula un ecosistema donde confluye en sinergia los elementos necesarios de los tipos penales en la determinación del proceder que se halle prohibido u ordenado, sesgando en positivo hacia el estrato jurídico del país, toda posibilidad en enjuiciar una conducta concreta calificada como delito o, por lo contrario, no haber lugar a ello.

Pende en instancia legislativa con meridiana claridad el arraigo grandilocuente en el empleo de un lenguaje objetivo, sencillo en la prosa, para que de esta forma el mandato advertivo punitivo derivado del *maximun Nullum crimen nullu poena sine lege*, se adecúe plenamente. En tal caso, como opción yuxtapuesta es el tamiz que tanto el juez como el titular del ejercicio público de la acción penal, esclarezca en sinapsis (relación) el hecho punible versus el delito infligido.

A este respecto cabe preguntarse si de lo que arriba se desprende, se deslegitimaría la expiación impuesta por el Estado en el ejercicio del *Ius Puniendi*. Negativa respuesta, por cuanto al momento de tener que adecuar una determinada norma penal al *Sub judici* de Autos, los efectos jurídicos serían inequívocamente impuestos dentro de esfero aplicativo de la norma. Caso contrario, le corresponde al juzgador no aplicar sanción alguna, debiendo en tal caso articularse con el legislador para que adecúe la legislación examinar casos dudosos, requiere de una praximetría en términos exegéticos, de allí la exhaustividad del estudio de las estructuras básicas de los tipos penales en determinación del núcleo rector desplegado en forma de conducta o comportamiento lesivo con clara incidencia calificadora del delito consumado.

En el marco antes expuesto (Zafaronni, 2009), ahonda que: (…) “lo fundamentalmente jurídico es lo emergente siempre constante y compatible con el hecho fáctico comprobable y las funciones: sistemática y, conglobante, mismas que generan una

ISSN: 2665-0266 / Depósito Legal: LA2017000128 / ISBN: 978-980-18-0874-9. Volumen 9. No. 1. Abril 2020

afectación en el pragma mundano" (p.93). Consecuencialmente el método complejo de investigación dogmático jurídico penal traza el camino idóneo en que el tipo objetivo sistemático siempre requerirá exteriorización actitudinal con resolución de continuidad con consecuencias lesivas.

Así el nexo causal entre el comportamiento punible siempre apareja un resultado perjudicial, si no, evidentemente no habrá conflicto (no basta para que se impute la conducta con el objeto, ya que no habría tipo sistemático). Aspecto que vertebra en sede de tipicidad subjetiva del tipo penal, dado que siempre los ilícitos informáticos serán infracciones dolosas, no habiendo lugar a culpa con o sin representación, e incluso no cabe tentativa, por ser un delito de resultado (Crespo-Berti, & Andrade, (2019).

No obstante con base en lo sustentado en los supuestos de hechos como uno de los dos elementos que compone la norma penal, enunciativa en qué caso o situación fáctica se aplicará, a más de los datos cualitativos recogidos, analizados e interpretados, instituyen una serie de problemas en términos de lenguaje legal juicioso, (dificultades que se resuelven sencillamente a través de solución práctica -*Quid pro quo*- experiencia sensitiva), con base en el ordenamiento jurídico penal positivo vigente acorde con los más elementales principios generales de justicia aplicados al derecho.

Por último, se destaca que los delitos informáticos constituyen una gamificación, extensa, prolija, compleja por mutación exacerbada de paquetes conmutados que ensayan los clanes que actúan tras compleja malla de números de dirección pública de *Internet Protocol* (IP) ambivalentes, que logran la no identificación de manera lógica, recurrentemente jerarquizada a una interfaz de un dispositivo, habitualmente un ordenador impersonal dentro de una red que identifique el punto de enlace a Internet, al poseer un alto grado de tecnicismo operativo al vulnerar con relativa impunidad el objeto jurídico protegido por el Estado inserto en seguridad de los activos de los sistemas de información comunicacional, razón última del derecho penal.

Referencias

Acurio del Pino, S. (2015). Derecho penal Informático. Una visión general del Derecho informático en el Ecuador con énfasis en las infracciones informáticas, la informática forense y la evidencia digital. Ecuador: Corte Nacional de Justicia.

Alvarado, I. (2007). La estructura de los tipos penales y los alcances del principio constitucional de legalidad en las construcciones típicas contra el ambiente. Revista del Posgrado en Derecho de la UNAM, p. 292.

Carrió, G. (2011). Notas sobre Derecho y lenguaje. 5ta. ed. Argentina: Abeledo Perrot. ISBN: 95020-03-09-8.

Código Orgánico Integral Penal (2014). Registro Oficial N° 107, del 24 de diciembre de 2019.

Constitución de la República del Ecuador (2008). *Registro Oficial Suplemento N° 449 del 20 de octubre de 2008.* https://www.wipo.int/edocs/lexdocs/laws/es/ec/ec030es.pdf

Crespo-Berti. L. (2017). Serie: Epítome de la metodología de investigación científica contemporánea. Vol. III. Ecuador: Autor. ISBN: 978-9942-28-749-6.

Crespo, L. (2017a). Transperspectivas Epistemológicas, Educación, Ciencia y Tecnología: Educación y Sociedad Cruzando el Puente hacia la Complejidad de REDIT. *Rivista scientifica EspressivAmente N° 1 06 / 2017. ISSN: 2239-4044.*

Crespo-Berti, L. (2017b). La acción nuclear del delito en el Código Penal Peruano. Perú: Universidad Católica Los Ángeles de Chimbote. *Revista Jurídica In Crescendo. 4 (1): ISSN: 2410-0110, pp. 59-76.*

Crespo-Berti, L. & Benavides, M. (2018). Las pruebas en el proceso penal ecuatoriano. España: Gedisa. ISBN: 978-84-17690-04-5.

Crespo-Berti, L. & Andrade, D. (2019). Tipicidad subjetiva: vacío de tipicidad culposa en el derecho penal sustantivo ecuatoriano. Revista Universidad Ciencia y Tecnología de la Universidad Nacional Experimental Politécnica Antonio José de Sucre, Venezuela, Vol. 23, N° 91, abril 2019, pp. 4-11. ISSN: 2542-3401, pp. 4-11.

Etcheberry, A. (2001): Derecho Penal. Parte General. 3a ed. Chile: Jurídica.

Fernández, D. (2013). Delincuencia y fraude informático. Ecuador: Observatorio sobre seguridad informática.

Garrido, M. (2003): Derecho penal. Parte General. Vol. I. Chile: Jurídica.

Gargarella, R. (2012). La Justicia frente al gobierno. Ecuador: V&M Gráficas, p. 29. ISBN: 978-9942-07-025-8, p. 29.

Hernández-Sampiere, R., Fernández, C. & Batista, P. (2014). Metodología de la Investigación. 6ta. ed. McGraw-Hill. ISBN: 978-1-4562-2396-0.

Rodríguez, J. & Serrano, A. (1995). Derecho penal español. Parte general. 18va ed. España: Dykinson.

Islas. O. (1991). Análisis lógico de los delitos contra la vida. México: Trillas. ISBN: 9682460743.

Ley Orgánica Integral de Prevención y Erradicación de Violencia de Género contra las Mujeres (2018). Registro Oficial Suplemento 175 del 05 de febrero de 2018.

Luzón, D. (1996). Curso de Derecho penal. Parte general I. España: Universitas, pp. 36-63.

Mir, S. (2004). Derecho penal. Parte general. 7ma. ed. España: Reppertor, pp. 151-159.

ISSN: 2665-0266 / Depósito Legal: LA2017000128 / ISBN: 978-980-18-0874-9. Volumen 9. No. 1. Abril 2020

Magliona, C. & López, M. (1999). Delincuencia y fraude informático. Chile: Jurídica de Chile.

Muñoz, C. (2008). Estudios jurídicos. Panamá: Ediciones Panamá viejo. ISBN 978-987-722-314-9.

Muñoz, F. (2007). Introducción al derecho penal. España: Bosch. ISBN: 987-98334-3-0, p. 14.

Peña, O. & Almanza, F. (2010). Teoría del delito: manual práctico para su aplicación en la teoría del caso. Perú: Asociación Peruana de Ciencias Jurídicas y Conciliación – APECC. ISBN: 978-612-45532-2-6, pp. 45-77.

Politoff, S.; Matus, J. & Ramírez, M. (2004): Lecciones de Derecho Penal Chileno. Parte General. 2a ed. Chile: Jurídica, p. 613.

Salvadori, I. (2011). Los delitos contra la confidencialidad, la disponibilidad y la integridad de los datos y sistemas informáticos. Regulación Española. Revista Novum Jus, Vol. 5, N° 1, enero-junio 2011, ISSN: 1692-6013, pp. 27-53.

Sarasola, I. (s.f.). Que es cracker informático. Disponible en: http://cracker88.galeon.com/ [Acceso: 27-01-2020].

Supo, J. (2014). Niveles y tipos de investigación: Seminario de investigación [mensaje en un blog]. Recuperado de: http://seminariosdeinvestigacion.com/niveles-de-investigacion/

Zaffaroni, R. (2009). Estructura básica del derecho penal. Argentina: Ediar. ISBN: 9789505742516, p. 93.

ISSN: 2665-0266 / Depósito Legal: LA2017000128 / ISBN: 978-980-18-0874-9. Volumen 9. No. 1. Abril 2020