REVISTA INTERNACIONAL
TECNOLÓGICA - EDUCATIVA DOCENTES 2.0
ISSN: 2665-0266 / VOL.10 (2), AGOSTO 2021
https://doi.org/10.37843/rted.v10i2.233

Caracterización del Derecho Informático: Influencia Docente y el Rendimiento Académico Enfocado desde la Consciencia Antijurídica

Characterization of Computer Law: Teaching Influence and Academic Performance Focused from Unlawful Awareness

Luis Andrés Crespo-Berti[1]

EDICIÓN: RTED Ensayos

Recibido: 3/junio/2021
Aceptado: 19/agosto/2021
Publicado: 29/agosto/2021

País

[1]Ecuador

Institución

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

Correo Eletrónico

[1]crespoberti@gmail.com

ORCID

[1]https://orcid.org/0000-0001-8609-4738

Citar así: APA / IEEE

Crespo-Berti, L. (2021). Caracterización del Derecho Informático: Influencia Docente y el Rendimiento Académico Enfocado desde la Consciencia Antijurídica. Revista Tecnológica-Educativa Docentes 2.0, 10(2), 21-29. https://doi.org/10.37843/rted.v10i2.233

L. Crespo-Berti, "Caracterización del Derecho Informático: Influencia Docente y el Rendimiento Académico Enfocado desde la Consciencia Antijurídica", RTED, vol. 10, n.° 2, pp. 21-29, ago. 2021.

Resumen

Este ensayo demandó un análisis interpretativo derivado de la cátedra Derecho informático en la colegiatura de la carrera de Derecho inserta en el eje profesional de la Universidad Regional Autónoma de los Andes, extensión Ibarra del Ecuador. Tuvo como propósito sustentar el escenario que encierra la conducta de los antisociales que emplean medios electrónicos, telemáticos o computacionales de cara a la llamada era digital por la ubicuidad del mundo conectado con base en un factor dual sindémico que ahora supone a más del brote pandémico, el avasallante oportunismo de los llamados clanes de la red por las interacciones que desbordan y exacerban el pronóstico de carga delictual en la vulneración del bien jurídico protegido por la legislaciones no solo local, sino en el tablero internacional como lo es la seguridad de los activos de los sistemas de información y comunicación como respuesta a la situación problémica que se expande a una velocidad vertiginosa a partir de una perspectiva didáctica sumida en los discentes. Reflexión que combinó el dominio jurídico-pedagógico que permitió enriquecer y robustecer con posturas explícitamente evaluadas por opiniones vertidas dadas a conocer sobre la real administración instruccional del Derecho informático como rama suigéneris de las Ciencias jurídicas con énfasis en penal.

Palabras clave: Antijurídico, conducta, consciencia, delito informático, hacker.

Abstract

This essay demanded an interpretive analysis derived from the Computer Law chair taught by its author in the tuition of the Law career inserted in the professional axis of the Autonomous Regional University of the Andes, Ibarra extension of Ecuador. Its purpose was to support the scenario that contains the behavior of antisocials who use electronic, telematic, or computational means on purpose the so-called digital age due to the ubiquity of the connected world based on a dual syndemic factor that now represents more than the pandemic outbreak, the overwhelming opportunism of the so-called clans of the network due to the interactions that overflow and exacerbate the prognosis and criminal burden in the violation of the legal right protected by the laws not only local but also on the international board, such as the security of the assets of the information and communication systems as a response to the problem situation that is expanding at a dizzying speed from a didactic perspective immersed in the students. The reflection that combined the legal-pedagogical domain allowed enriching and strengthening with positions explicitly evaluated by opinions expressed made known about the real instructional administration of computer law as a subgeneric branch of legal sciences with emphasis on criminal matters.

Keywords: Legislation, constitution, law, violation of human rights, justice.

Introducción

Históricamente la dogmática jurídico penal ha trazado la ruta idónea en la comprensión del binomio teoría general del delito y de la pena, más sin embargo las tendencias sobre el establecimiento de nuevos enfoques, ordenación de conocimientos, particularidades y categorías hacia la interpretación sistematizada en la construcción referencial del derecho informático positivo (escrito), caracteriza su finalidad (el para qué), no siendo otro que proporcionar la tan ansiada seguridad jurídica, de lo contario, se reputaría proscrita la justicia hacia la impunidad del agente que, para el caso fenómeno de estudio recae en el ciberdelincuente y de modo particular en el *hacker* en detrimento del colectivo social a escala global, con las singularidades que nadie escapa a éste flagelo inmanente en toda sociedad civilmente organizada (Alcivar et al, 2018).

A partir de la ciberdelincuencia, se erige el hacker por su calificativo atribuido por su temida vanguardia en afán de lucro que rodea el entorno de acción (hecho fáctico punible por su carácter contestatario, crítico o experimental al margen del circuito electrónico habitual).

A renglón seguido, el concepto ilícito conductual conlleva no solo en su origen, sino también por la transferencia habitual de acciones de hacking durante el tracto sucesivo del camino criminal, constituyéndose hoy día, un modelo criminal normalizado, aspecto inadmisible.

En este propósito la representación ilegal antijurídica accionada dependerá cuando su acceso indebido al sistema informático sea para desviar fondos bajo formas ilícitas utilizadas en tele transferencia de datos, cuando exista encubrimiento operativo comercial o financiero, mediante mecanismos adyacentes. Esta dinámica incluye súper estructuras y flujos ilícitos confluyentes hacia puntos críticos y vulnerables a través de sistemas alternativos como salas físicas o virtuales de invite y azar, escrutinios electorales como se han visto en recientes procesos comiciales en la región, firmas cambiarias, instituciones financieras, cooperativas de ahorro y préstamo, operaciones de valores en mercados bursátiles, comercio electrónico, monedas electrónica o dinero electrónico, bienes raíces, bitcoin, criptomonedas, sistemas de pagos electrónicos tales como PayPal, SafetyPal, SEPA, Zelle, entre otros (Todoecommerce, 2018).

En tales circunstancias cabe destacar una noción al concepto de antijuricidad, teorizado como rasgo o carácter adjetivo del delito configurativo de la infracción informática. Definido como aquel desvalor posesivo hacia un hecho típico contra normativo a Derecho en general; pero comúnmente inmerso en el plexo penal (García, 2019; Quesada, 2017). Por tanto, la antijuridicidad supone conductas realizadas prohibitivas por el ordenamiento jurídico; en otras palabras, dicho comportamiento es contrario a Derecho. En la legislación patria se halla prevista a tenor de lo dispuesto en el artículo 29 del Código Orgánico Integral Penal: "Para que la conducta penalmente relevante sea antijurídica deberá amenazar sin justa causa un bien jurídico protegido" (…) (2019). Con tal preámbulo copula el descriptor consciencia definida en términos generales como el auto conocimiento cognitivo del mundo circundante, pero también se refiere a la moral o bien a la recepción normal de los estímulos endógeno-exógeno. *Conscientĭa* alude, literalmente, «con conocimiento» (del latín *cum scientĭa*) (RAE, 2014).

Desde el foco reflexivo, se arguye al despeje de una multiplicidad de interpretaciones preexistentes sobre posiciones encontradas respecto de la tipicidad subjetiva del delito informático (Robles, 2016). He allí el umbral 1 desde el foco del investigador como primer eslabón alusivo al título de este ensayo, por cuanto se considera importante retomarlo desde el ámbito académico a través del acto docente, toda vez que una perspectiva errada, pueden llevar a un ejercicio punitivo automatizado y a la desaplicación de fundamentos constitucionales en lo atinente a la seguridad jurídica (Artículo 82 constitucional, 2008). De

tal forma el objetivo general quedó circunscrito en sustentar el escenario de la conducta de los antisociales por el emplean medios electrónicos, telemáticos o computacionales a propósito del expansionismo digital por la gravosa situación proveniente de lo que denomina el autor como sindemia.

La perspectiva transciende por el grado del aporte en la propensión, participación e inclusión social y el cumplimiento de la responsabilidad social encomendada a través del acto docente en la transmisión del conocimiento patentizado en procesos de aprendizaje-enseñanza con el uso de las Tecnologías de Información y Comunicación, acorde al momento que se vive por segregación sanitaria mundial.

Así, el objetivo general centró su atención en sustentar el escenario que encierra la conducta de los antisociales que emplean medios electrónicos, telemáticos o computacionales de cara a la llamada era digital por la ubicuidad del mundo conectado.

Desarrollo

En este estadio se pone en contexto el modelo educativo puesto de relieve como derecho universal precautelado por la Institución de Educación Superior vinculada, aun en circunstancias excepcionales e imprevisibles como las que supuso un estado de excepción por calamidad pública decretado por el Estado ecuatoriano el año próximo pasado y a comienzos del presente.

La crisis mundial educativa producto de la pandemia por COVID-19 es muy grave y compleja, especialmente en lo relativo a la disminución de la calidad del aprendizaje y en la exclusión del sistema educativo de una ingente cantidad de educandos (Gianini, 2020; Banco Interamericano de Desarrollo, 2020). Sin duda las repercusiones negativas de la paralización de la educación presencial profundizaron las desigualdades sociales y económicas, deserción aumentativa, disminución y deserción de la promoción estudiantil, tanto del sector público como privado en detrimento de la calidad de los aprendizajes. Aunado al paradigma de complejidad de la realidad que encarna incertidumbre por la pandemia y sus variantes, por un lado, gracias a la tecnología se ha ido superando paulatinamente la buena marcha de la educación; pero por la otra en contraposición con repunte desmesurado en ataques provenientes de la ciberdelincuencia con afectación particularmente al colectivo estudiantil.

Por consiguiente, como punto nodal reflexivo a propósito de profundizar las estrategias pedagógicas puestas en marcha en la impartición de la asignatura Derecho informático inserta en unos de sus ejes trasversales derivado del sílabo desde los entornos virtuales de aprendizaje, fue lo atinente a los delitos informáticos por los modos de comisión que desembocan en la vulneración de la seguridad de los activos de los sistemas de información y comunicación tutelados por la legislatura penal nacional.

En ese sentido, se pretendió ilustrar lo concerniente al método de investigación dogmático-jurídico penal, acorde con los enfoques y teorías más predominantes. A continuación, se presenta la tipología versus la etiología de la consciencia por ser ésta el primer eslabón en la perpetración del delito informático inserto en el dominio científico en la tripleta clínico-jurídico-penal.

Tipos de Consciencia

Delimitado el concepto del subtítulo "consciencia antijuridicidad" correspondió ventilar el umbral 2 derivado del título del ensayo en lo atinente a la tipología de la consciencia, verificado en los siguientes términos: (a) consciencia psicológica, vista como la capacidad ceñida del individuo de advertir su propio ser; (b) consciencia moral, entendida como el antejuicio personal sobre la bondad o por el contrario la malicia de sus propias actividades o acciones; (c) consciencia social, entrelaza la sensibilidad ante las justicias o injusticias sociales; (d) consciencia escrupulosa, por la credulidad de actos incorrectos en acciones que no lo son; (e) consciencia laxa, aquella inclinada por relativas acciones y ponerlas fuera de la ley, (f) consciencia dudosa, oscilante entre la

licitud o ilicitud de una acción; (g) consciencia cierta, provista por la convicción segura y sin temor reverencial a equivocarse; (h) consciencia verdadera, concordante con la ley y; (i) consciencia errónea, diametralmente opuesta a la verdadera o equívoca con respecto a la ley (Montano, 2017).

Así la consciencia antijurídica exteriorizada se transforma en forma de conducta hacia el cometimiento de un delito informático en correspondencia con el reproche culpable de un hecho contrario a derecho. Por ende, es necesario que el agente tenga consciencia y obre en conocimiento antijurídico de su comportamiento; basta el insoslayable motivo de comprensión prohibida de un no hacer para saber que el hecho cometido está jurídicamente prohibido.

Por tanto, la consciencia no es más que el conocimiento antijurídico del hecho como categoría subjetiva de la culpabilidad, conteste comúnmente con la doctrina y la jurisprudencia, al considerar variables indispensables para la declaración de culpabilidad. Sin embargo, en praxis judicial, el conocimiento antijurídico formal se presume por los juzgadores, simplemente porque queda probado en juicio que se lacera el tan mentado bien jurídico protegido como lo es la seguridad de los activos de información y comunicación (Crespo-Berti & Benavides, 2018). Estamento determinante en las súper estructuras básicas del tipo penal informático.

Como umbral 3, se trae a colación que la consciencia antijurídica está relacionada íntimamente con los delitos dolosos, donde se considera la acción nuclear del delito informático, siempre el agente tendrá la voluntad deliberada de perpetrarlo a sabiendas de su ilicitud. Esto por ser infracciones de resultado, consumadas en un mismo acto o en du defecto por una sucesión de acciones interrelacionadas (Crespo-Berti, 2020b, c, d).

Hoy día en doctrina penal no se discute sobre lo cognitivo actitudinal del agente porque queda tácitamente expuesto, salvo que sea privada totalmente por un hecho fortuito o de fuerza mayor, incluso por coacción, de lo contrario mal podría reputarse como reo de delito informático. Ahonda Roxin, (2003): (…) "de ser parcial sí responde penalmente con su correspondiente atenuante específica respecto de la punibilidad para el delito que corresponda" (pp. 159-160), al constituir una circunstancia modificatoria de la infracción, respecto de la penal a imponer de parte del juzgador.

De otro lado, bajo una especial retrospectiva derivada del ensayo, porque podría devenir una imputación objetiva errada de parte del titular público en el ejercicio de la acción penal, cuando el agente no realiza dolosamente los hechos, pero incurso en error evitable de prohibición. El dolo (designio de causar un daño) no solo deviene en consideración cuando el agente ha previsto indebidamente el resultado típico, sino cuando ha tomado en cuenta la vulneración de los intereses sociales. Aspecto indescartable, dado que los delitos informáticos siempre serán dolosos más no culposos.

Como umbral 4 se erigen los llamados ciberdelincuentes, en su vértice más alto figura el *hacker* de sombrero negro, temido por su experticia en vulnerar con éxitos los códigos fuente de seguridad por los ataques cibernéticos que ensayan con singular éxito (Rando et al., 2019). Por consiguiente, en este estadio como arriba se acotó, será el único perfil en destacar. Se destaca el móvil en una escala geométrica del 1 al 10, responde en gran medida al aspecto económico antes pormenorizado al situarse en un nivel 9, con una proyección secundaria hacia el frenesí en usurpación de identidad y sustracción de datos personales para fines ilícitos.

A. El Hacker: Tipos de Ataque. En este apartado se analizó el tema clave sobre el software, concepto que define como todo lo intangible de una computadora. A tenor de Romero, et al. describe la tradicional tipología del ataque cibernético en los siguientes términos: "Un virus informático puede hacer muchas cosas, por ejemplo, eliminar archivos, evitar accesos a las computadoras, robo de información, bloqueo de funciones de un sistema operativo o de programas dentro de una computadora" (2018, p. 15).

En ese mismo sentido y dirección parafraseando a Vieites (2013), ahonda que

existen varios tipos de virus que se los puede definir de la siguiente manera: virus de sector de arranque (BOOT); virus de archivos ejecutables; virus de macros; virus de lenguajes de script; programa maligno; gusanos; troyanos; spyware; keyloggers; adwares; dialers; backdoors; rootkits; bacterias; bombas de tiempo, entre muchos otros.

Entre tanto, lo concerniente por la práctica en la formación instruccional, se apreció adaptación de saberes en los ataques más recurrentes en este último año a propósito de la pandemia se observó agravios en el seno comunitario estudiantil hacia el *phishing*, *spoof*, *port scanning* y *spamming* (Crespo-Berti, 2020e). Además de advertir una mutación en su conjunto que viene generando estragos a nivel de banca financiera mundial como lo es suplantación de identidad al solicitarse de parte operadoras de telefonía de la víctima a través de la técnica *sim swapping*, consistente en cinco pasos:

1. El *hacker* envían al correo enlaces de páginas falsas para que ingrese su información, como usuario o clave de su banca en línea.
2. El *hacker* busca obtener su información personal a través de redes sociales o llamadas telefónicas haciéndose pasar por una entidad conocida.
3. Con los datos personales que obtiene, solicita en la operadora telefónica de la víctima un duplicado de tarjeta SIM.
4. Con el duplicado de tarjeta SIM (*subscriber identity module*-módulo de identidad del suscritor), el *hacker* tiene acceso en la recepción del código de verificación que se envía a los celulares.
5. El *hacker* accede a la banca en línea para realizar transferencias, pagos, entre otras operaciones fraudulentas.

Respecto a la seguridad informática y el análisis de vulnerabilidades, según Marrero (2003), existen muchas amenazas de varias fuentes principalmente de internet que pueden ser: (a) correos electrónicos infectados por virus; (b) firewalls mal configurados; (c) suplantación de contraseñas; (d) contraseñas débiles; (e) robo y destrucción de información. En contra inteligencia, surge la encriptación de datos a los efectos de enervar la conducta criminógena.

Así Santos (2014), aporta la encriptación simétrica con base en métodos criptográficos que emplean una misma clave para cifrar y descifrar un mensaje. Tales extremos establecen comunicación al crear un acuerdo de uso de clave, para que posteriormente ambos usuarios tengan acceso a la misma clave, donde el remitente cifra su contenido y el destinatario la descifra con el mismo mecanismo.

En entrevista sostenida con el Ing. Marvin Soto, *hacker* ético costarricense, profesor investigador de la Universidad de Costa Rica y miembro fundador de *Cybercom (2021)*, ahonda a tenor:

> Cada vez que ve (Sic) una cantidad en aumento desproporcionado en los seguidores de una cuenta de alguna red social de algún personaje emergente; ¿se pregunta cuántos de esos seguidores son reales? ¿Cómo puede saber si alguien en línea es real, un *bot* o una identidad sintética? El fraude de identidad sintética (*Synthetic Identity Fraud*), es una de las formas de robo fragmentado de identidad de más rápido crecimiento. Se produce cuando los delincuentes utilizan una combinación de datos de diferentes personas, así como información totalmente inventada para cometer ilícitos (p.1).

En virtud de lo expuesto, cada vez se hace más imperioso blindarse, como bien indicó el informante clave, (…) "catalicemos primeramente que Internet ya no es solo un mundo virtual, es una dimensión extendida de la realidad que impregna nuestras vidas, ¡es parte de nuestro día a día! Es decir, trabajamos, socializamos, convivimos, compartimos, informamos, hacemos negocios y nos comunicamos a través de esta plataforma global" (Versionante, 2020).

Finalmente, la brecha punible es inevitable en selectividad consciente de cada uno en el terreno del deber ser, como toda determinación reversible. Al tratarse de conductas criminales irremediablemente inmanente en el seno de toda sociedad, se

apuesta a una respuesta científico-jurídica que deba ser continuamente debatida por especialistas capaces de examinar científicamente los fenómenos criminales que acechan constantemente sin escapar a esta realidad el ámbito educativo, así como evaluar propuestas político-criminales concretas que necesariamente dimanen de la función ejecutiva de los países en general (Zúñiga, 2016).

B. Cátedra Derecho informático carrera de Derecho de la Universidad Regional Autónoma de los Andes del Ecuador. Por último, a lo denominado por el sugestivo subtítulo del ensayo "influencia docente y el rendimiento académico enfocado desde la consciencia antijurídica", el umbral 5 encarna actualmente en la realidad educativa diametralmente opuesta desde hace dieciséis meses. La emergencia sanitaria declarada por la Organización Mundial de la Salud exaltada por el virus del síndrome respiratorio agudo severo tipo-2 (SARS-CoV-2), por su mutación exacerbada declarada variante por especialidad médica-inmunológica, ha sido la causa de la mayor interrupción histórica en el sistema educativo. La globalidad estudiantil mundial de unos 1.200 millones de juveniles alumnos, no han podido concurrir a los centros educativos de los países debido a la pandemia. Secretaría Nacional de Educación, Ciencia, Tecnología e Innovación, por su acrónimo (SENESCYT, 2021).

La altiplanicie del cuerpo profesoral mundial se ha visto forzado súbitamente a cambiar su estratagema didáctica y pedagógica, con meridiana claridad, calidad, calidez y pertinencia de los contenidos frente a las necesidades de los discentes. La creatividad e iniciativa de los docentes de la educación superior han tenido como frente a diversos recursos y medios (con qué) de métodos desarrolladores insertos en las Tecnologías de la Información y la Comunicación (TIC), mediante novedosas propuestas metodológicas y maniobras pedagógicas en mérito a ser divulgadas y conocidas por la comunidad educativa.

En esa misma línea de pensamiento, la asignatura Derecho informático pertenece a una disciplina inserta en el rediseño de la malla curricular del ciclo profesional de la carrera de Derecho de la UNIANDES del Ecuador, concibe el eje de formación relacionado con la práctica, esencial en su diseño (Guzmán, 2014). Los dicentes en su conjunto demuestran competencias proactivas que son desarrolladas instruccionalmente en modalidad híbrida ensayado durante el acompañamiento docente y complementado a través del aprendizaje autónomo asíncrono en el entorno virtual de aprendizaje (EVA) institucional.

En el plexo de las medidas adoptadas por la Universidad Regional Autónoma de los Andes del Ecuador, Casa de estudio vinculada, fueron orientadas en respuesta inmediata a una situación pandémica que sorprendió a todos y que desestabilizó el sistema social, generó cambios trascendentales por el impacto pandémico en su régimen de estudios, aunque con la ayuda de la tecnología se logró dar continuidad al proceso educativo universitario. Así la naturaleza de la modalidad virtual garantizó los principios de igualdad y equidad inherentes a la educación como un derecho humano.

Sin duda el Derecho a la educación es un recurso de gran importancia dentro de la sociedad al ser una disciplina que se adapta a los cambios sociales y que permite resolver las situaciones sobrevenidas, para ello crea normas jurídicas que regulan el funcionamiento social, nace de la sociedad y a la vez la moldea, impulsa las transformaciones sociales y está presente en los cambios para estimularlos. De manera que, ante las contingencias educativas enfrentadas en Ecuador como consecuencia de la crisis sanitaria, el Derecho ha sido fundamental para permitir enmarcar las decisiones regulatorias en las leyes vigentes y, a la vez, controlar y contrarrestar decisiones que pudieran violentar los derechos educativos.

La sinergia desarrollada frente a las desigualdades asociadas desde la cátedra de Derecho informático hacia los discentes se reflexiona sobre estrategias abordadas y planteadas en el siguiente procedimiento en propensión a la participación, inclusión social

y el cumplimiento de la responsabilidad social encomendada.

- ✓ Se elaboraron orientaciones metodológicas dirigidas a los dicentes del curso en modalidad híbrida, quienes asistieron sostenidamente a las prácticas asistidas promovidas desde la cátedra. El haber determinado su objetivo, se analizó e interpretó la relación del contenido de la asignatura Derecho informático que cursan los educandos del séptimo nivel semestre de colegiatura de la carrera de Derecho. Se impartieron las UNIANDES previstas en los planes de clases derivados del programa analítico de la asignatura tratada vinculada con el contenido del sílabo de la asignatura correspondiente al eje de formación profesional de la carrera.

El docente preparó a los estudiantes para que sean capaces de resolver problemas profesionales; relacionados con la informática con el Derecho, lo que les resulta necesario como futuros abogados del país. El docente explicó a los dicentes el aporte de esta práctica a su formación, generando su motivación para participar. Socializó las actividades ejecutadas, teniendo en cuenta sus características e intereses.

- ✓ Se dirigió la preparación previa de la práctica asistida. Para ello se realizaron coordinaciones con el departamento de Telemática de Universidad para garantizar la participación de los estudiantes en la práctica.
- ✓ Se realizaron talleres a los discentes ahondando y enriqueciendo el contenido requerido para la ejecución de la práctica. De la asignatura Derecho informático se trató lo relacionado con la utilización de métodos y técnicas en la investigación cuantitativa. Para ello el investigador desarrolló previamente una guía didáctica instruccional de Derecho informático, acerca de la Ciencia de datos.

En los talleres se analizó la pertinencia utilizada en el desarrollo de la práctica asistida, el método de observación científica, de campo y de carácter participante. Se debatió en torno al aporte de estos tipos de observación para obtener información sobre la Ley de Comercio Electrónico, Firmas y Mensajes de Datos del Ecuador (2002) en sana comparación legislativa con la Ley Especial Contra los Delitos Informáticos de Venezuela (2001). Se enfatizó en el registro de los datos, mediante notas de campo. Como resultado del taller, los dicentes elaboraron como técnica del método seleccionado la guía de observación.

- ✓ Se ejecutó la práctica asistida desarrollada intencionalmente, el día 01 de junio de 2021, en ocasión al día nacional del niño por ser vulnerable a los delitos informáticos, verbigracia de la pedofilia virtual de acelerada infracción hoy día.

A partir de la guía formativa, los dicentes registraron la data para su posterior análisis e interpretación de resultados. Centró su atención en los datos obtenidos, de este modo establecieron comunicación en tiempo real con apoyo del docente frente a las instancias jurisdiccionales del país. Se delimitó las distintas resoluciones de los asuntos presentados en los tribunales en materia de ilícitos informáticos e incluso con las estadísticas oficiales emanadas de la unidad de análisis del delito informático del Ministerio del Interior (cartera estatal de gobierno) y de la fiscalía general de Estado.

Al final de la práctica asistida se procedió con sus conclusiones y recomendaciones, sin perder de vista los objetivos trazados. Se brindó asesoría constante mediante tutorías individuales y grupales a través de las plataformas remotas educativas a los dicentes en la elaboración de un informe que registró el resultado de la práctica, con énfasis en la identificación del tipo penal informático: medios de comisión;

objeto material; nexo causal; condición objetiva de punibilidad; circunstancias de modo, tiempo y lugar; referencias de ocasión e; instrumentos, así como la valoración de medidas profilácticas de prevención, desde la perspectiva de futuros profesionales del Derecho en el país. De este modo, la práctica asistida se enfocó en la formación del abogado.

Conclusión

El ensayo evidenció en el actual contexto institucional educativo el vínculo entre el docente-discente, adecuado en la concepción de las actividades de aprendizaje asistidas por el profesor, así como las actividades de aprendizaje colaborativo, el componente de prácticas de aplicación y experimentación del aprendizaje autónomo a través del aula invertida, todo bajo un modelo integrador (Crespo-Berti et al., 2019). Ello respondió a la búsqueda y hallazgos constantes en el conglomerado de educandos en formación profesional provisto del establecimiento de interrelaciones de la disciplina Derecho informático, lo que robusteció la solidez de los saberes adquiridos por los dicentes.

Respecto de la reflexión -postural conductual- de los antisociales quienes emplean medios electrónicos, telemáticos o de telecomunicaciones por lo franqueable que pueden llegar a ser los sistemas de información y comunicación, hacia los fundamentos de seguridad informática en cualquier escenario, incluso el empresarial, se colige construcción sobre la base del siguiente andamiaje de certidumbre: (a) privacidad; (b) probidad y (c) disponibilidad (Carpentier, 2016).

La formulación expuesta queda circunscrita por un lado en: autenticación de usuarios, gestión de privilegios y cifrado de información y por el otro: monitoreo de tráfico de red, implementación de actualización de software confiables, sistemas de control de cambio y el establecimiento de copias de seguridad.

Especial atención colma el descriptor software, por su sensible forma de ataque. De acuerdo con Beynon-Davies (2015), el término software o programa es utilizado para describir una secuencia de varias instrucciones que es leído por un computador, escritos en un determinado lenguaje de programación que pueden ser clasificados de la siguiente manera: lenguaje de máquina, lenguaje ensamblador y lenguajes de alto nivel.

Por último, se impetra el potencial presupuesto de la antijuricidad formal y material como rasgo delictual converge en el delito informático doloso (Muñoz Conde & García Arán, 2010). Supuesto en esta clase de infracciones informáticas la realización típica debe ser querida o realizada con cargo por el agente (*hacker*), implicación que constituye una exigencia indeclinable que pueda reconocerla como contradictoria del orden jurídico.

En los casos de culpa consciente, conocida la posibilidad de causar el resultado, debe representarse o poderse representar además de encontrarse jurídicamente prohibido.

En los de culpa inconsciente, a la previsibilidad de la realización fáctica, debe conectársele también la previsibilidad de la prohibición. No bastará que el agente (*hacker*), pueda percatarse de las propiedades de la acción que la caracterizan como peligrosa - por ejemplo, del acceso a un sistema avanzado de computadoras o redes informática recurrente en que incurre. Deberá también reconocerla como acción prohibida. El error inevitable sobre este extremo excluye la culpabilidad, cuando se halla inmerso en la esfera del caso fortuito o de fuerza mayor, el agente no podrá percibir que la acción, causa el resultado lesivo del bien jurídico protegido como lo es la seguridad de los activos de los sistemas de información y comunicación a escala nacional e internacional.

Referencias

Alcivar, C.; Blanc, G. y Calderón, J. (2018). Aplicación de la ciencia forense en los delitos informáticos en el Ecuador y su punibilidad. *Revista Espacios*, 39, (42), 15, 2018. http://www.revistaespacios.com/a18v39n42/a18v39n42p15.pdf

Banco Interamericano de Desarrollo (2020). La educación

superior en tiempos de COVID-19. Aportes de la segunda reunión del diálogo virtual con Rectores de Universidades Líderes de América Latina. Nueva York: BID.

Beynon-Davies, P. (2015). Sistemas de información: introducción a la informática en las organizaciones. España. Reverté.

Carpentier, J. (2016). La seguridad informática en la PYME: Situación actual y mejores prácticas. España. Ediciones ENI.

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

Constitución de la República del Ecuador (2008). Registro Oficial N° 449 del 20 de octubre de 2008.

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

Crespo-Berti, L.; Hernández, R.; Infante, M. (2019). Prácticas asistidas enfocadas en la formación de los estudiantes: experiencias en UNIANDES, Ecuador. *Revista Espacios*, 40, 8, 2019, 8. http://www.revistaespacios.com/a19v40n08/19400808.html

Crespo-Berti, L. (2020b). La acción nuclear del delito informático en el Código Penal Panameño: perspectiva híbrida desde el foco de la teoría finalista / funcionalista [sesión de conferencia]. Universidad Autónoma de Chiriquí, PA. 6to. Congreso Internacional Científico (modalidad virtual). https://www.youtube.com/watch?v=4ZFNbSm1YLU

Crespo-Berti, L. (12/04/2020c). La acción nuclear del delito informático en el novísimo Código Orgánico Integral Penal del Ecuador. [sesión de conferencia]. Grupo Docentes 2.0. 4to. Congreso Internacional Virtual Sobre las Tecnologías del Aprendizaje y del Conocimiento (CIVTAC). https://www.youtube.com/watch?v=Xo77DXyZ_2s

Crespo-Berti, L. (2020e). La red 5G y su impacto en las Ciencias jurídicas desde la perspectiva penal. [sesión de conferencia]. Universidad Regional Autónoma de los Andes, EC. VII Congreso Internacional UNIANDES: impacto de las investigaciones jurídicas. https://tinyurl.com/xrz2k34w

Ley Especial Contra los Delitos Informáticos (2001). *Gaceta Oficial de la República de Venezuela N° 37.313 del 30 de octubre de 2001.*

Ley de Comercio Electrónico, Firmas y Mensajes de Datos (2002). *Registro Oficial Suplemento N° 557 del 17 de abril de 2002.*

García, M. (2019). *La antijuridicidad como requisito de la responsabilidad civil*. Universidad de Murcia.

Gianini, S. (2020). *Tres formas de planificar la equidad durante los cierres de escuelas por Coronavirus*. Blog de educación mundial. https://tinyurl.com/7p6yt7mp

Guzmán, C. (2014). El proceso extensionista universitario como vía para la pertinencia en la formación del futuro profesional. *ESPACIENCIA*, 5,1, 2014, 17-24.

Marrero, Y. (2003). La criptografía como elemento de la seguridad informática. *Acimed,* 11(16).

Montano, P. (2017). La objeción de la conciencia como causa de justificación. *Revista de Derecho de la Universidad de Montevideo*, 1(15), 113-142. http://dx.doi.org/10.22235/rd.v1i15.1379

Muñoz Conde, F. y García Arán, M. (2019). Derecho Penal. Parte General, Tirant lo Blanch, Valencia.

Quesada, J. (2017). Antijuridicidad material. *Revista Digital de la Maestría en Ciencias Penales*. Universidad de Costa Rica. 10, 10. ISSN 1659- 4479. RDMCP-UCR.

Rando; E.; González, P.; Aparicio; A.; Martín R. y Alonso, CH. (2019). *Hacking Web Techonologies, OxWORD*, https://tinyurl.com/yr7fmxcw

Real Academia Española (2014). *Diccionario de la lengua española*. [Dictionary of the Spanish Language] (23ra. ed.).

Robles, F. (Ed.). (2016). *Delitos informáticos y por medios electrónicos en el derecho penal peruano*. UPC.

Romero, M., Figueroa, G., Vera, D., Álava, J., Parrales, G., Álava, C., Murillo, A. y Castillo, M. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades*. Áreas de Innovación y Desarrollo, S. L. https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Roxin, C. (2003). Derecho Procesal Penal. Argentina. El Puerto.

Santos, J. (2014). Seguridad y alta disponibilidad. Bogotá. Ra-ma.

Secretaría Nacional de Educación Superior, Ciencia y Tecnología (2021). Estadísticas de Educación Superior, Ciencia y Tecnología. Ecuador. https://tinyurl.com/2ravj2uh

Todoecommerce. (2018). *Ataques Informáticos*: *Principales Problemas De Seguridad*. http://www.todoecommerce.com/ataques-informaticos.html.

Vieites, A. (2013). *Auditoría de seguridad informática*. Bogotá. Ediciones de la U.

Zúñiga, L. (2016). *La pena en un estado social y democrático de derecho", en Lecciones de derecho penal: teoría del delito*. (San José, Costa Rica: Jurídica Continental, 344-345.