Uniandes EPISTEME. Revista digital de Ciencia, Tecnología e Innovación
ISSN 1390-9150/ Vol. 7 / Nro. Especial / Año. 2020 / pp. 1311-1325

ARTÍCULO CIENTÍFICO
CIENCIAS SOCIALES

El *child grooming* o acoso sexual a menores por internet y la prueba informática

Child grooming or sexual harassment of minors online and computer testing

Santillán Molina, Alberto Leonel [I]; Vinueza Ochoa, Nelly Valeria [II]; Benavides Salazar, Cristian Fernando [III]; Benavides Salazar, Julio Cesar [IV]

[I.] us.albertosantillan@uniandes.edu.ec. Carrera de Derecho, Universidad Regional Autónoma de los Andes, Santo Domingo, Ecuador.
[II.] vinuezan@fiscalia.gob.ec. Fiscalía General del Estado, Quito, Ecuador,
[III.] us.cristianbenavides@uniandes.edu.ec. Carrera de Derecho, Universidad Regional Autónoma de los Andes, Santo Domingo, Ecuador.
[IV.] us.juliobenavides@uniandes.edu.ec. Carrera de Derecho, Universidad Regional Autónoma de los Andes, Santo Domingo, Ecuador.

Recibido: 01/09/2020
Aprobado: 02/10/2020

RESUMEN

Los elementos del tipo descrito en el artículo 173 del Código Orgánico Integral Penal que sanciona el child grooming, exige para la comisión de la infracción a las tecnologías de la información y comunicación, y que la evidencia digital sea considerada como un bastión principal en el proceso penal, para probar los hechos en juicio, siendo el objetivo de este trabajo de investigación, el explicar por qué la evidencia informática es importante para poder justificar la comisión del acto lesivo. La aplicación del método histórico lógico, permitió identificar cómo se encuentra establecida la sociedad de la información y las Tics, así como la influencia que incide en la comisión del delito de child grooming o contacto con finalidad sexual con menores de 18 años por medios electrónicos, y de esta manera determinar que el uso de las tecnologías de la información y comunicación, sirven para la ejecución de este injusto penal, así como también justificar su comisión con la prueba informática, y en aplicación directa del método de análisis jurídico-comparado, se pudo determinar en las disposiciones legales ecuatorianas así como las extranjeras que tratan este delito, el denotar la pertinencia de la investigación. Este trabajo académico permitió determinar cómo las TIC son

necesarias para la ejecución de la infracción penal y su comprobación procesal, concluyéndose que los sistemas de tratamiento de información, son una herramienta fundamental en la cotidianidad y que sirven como medio de prueba en el derecho procesal penal.

PALABRAS CLAVES: Child grooming; ciberdelitos; telemática; prueba informática.

ABSTRACT

The elements of the type described in article 173 of the Comprehensive Organic Penal Code that penalizes child grooming, requires for the commission of the infraction to information and communication technologies, and that digital evidence be considered as a main bastion in the process criminal, to prove the facts in court, being the objective of this investigative work, to explain why the computerized evidence is important to be able to justify the commission of the harmful act. The application of the logical historical method allowed us to identify how the information society and ICTs are established, as well as the influence that affects the commission of the crime of child grooming or contact for sexual purposes with minors under 18 years of age by electronic means. and in this way to determine that the use of information and communication technologies serve for the execution of this unjust criminal, as well as justify its commission with the computer test, and in direct application of the method of legal-comparative analysis, it is was able to determine in the Ecuadorian legal provisions as well as the foreign ones that deal with this crime, to denote the relevance of the investigation. This academic work made it possible to determine how ICTs are necessary for the execution of the criminal offense and its procedural verification, concluding that information processing systems are a fundamental tool in daily life and that they serve as a means of proof in criminal procedural law.

KEYWORDS: Child grooming; cybercrime; telematics; computer evidence.

INTRODUCCIÓN

Al analizar la sociedad de la información, se puede llegar a determinar que la misma se trata de un “grupo social que tiene como objetivo la captación, almacenamiento y transmisión de datos informáticos, encaminados a ejecutar acciones de carácter socio económicos, que impulsan cambios profundos a través de medios disponibles para la divulgación de información mediante tecnologías digitales” (Hilbert, 2009, pág. 27).

En atención a esta definición podemos advertir que este conglomerado social tiene como finalidad la “relación intersubjetiva” (Aboso, 2017, pág. 142), entre las personas

mediante el uso de las TIC, así como redes sociales y aquellos sistemas automatizados de información que permiten el viaje desfragmentado de la misma, lo que es determinante en el desarrollo de aquellas actividades sociales, políticas, culturales, económicas, financieras y también comerciales, que han permitido que una sociedad se encuentre en progreso al momento de realizar sus actividades diarias, y que de manera rápida pueda acceder aquellos bienes y servicios que se encuentran ofertados por instituciones y empresas del sector público o privado.

Por lo que se puede establecer que al tener automatizada todas sus operaciones, el ciberespacio se convierte en un "vector estratégico de comunicación que puede ser utilizado para influir en la opinión pública y en la forma de pensar de las personas, mediante la manipulación de información o campañas de desinformación, o acciones de carácter híbridas" (Ministerio de la Presidencia, 2019, pág. 3).

Es de capital importancia resaltar que todas las personas tenemos un rastro digital que comienza al momento de nacer, y que nos permitirá posteriormente con aquella identificación, poder acceder a aquellos canales electrónicos establecidos en las plataformas digitales que para el efecto tienen las empresas públicas o privadas.

Los pilares fundamentales que estudian en esta era digital donde entra el funcionamiento de las tecnologías de la información y comunicación son: a) el ciberespacio el cual se lo puede definir como aquella autopista tecnológica de carácter virtual donde viaja la información de manera desfragmentada; b) la ciberseguridad la que tiene como finalidad el estudio de aplicación de las medidas de seguridad que protegen los sistemas automatizados de información tanto física como lógica; y c) la ciberdelincuencia, en tratándose de aquellas personas con habilidades tecnológicas que tienen como objetivo primordial, el romper las medidas de seguridad, y ya en posesión de aquellos datos informáticos usarlos de una mejor manera para beneficio personal o de un tercero, por lo que se puede llegar a determinar que es obligación de los Estados mantener un Gobierno electrónico seguro, y así garantizar la invulnerabilidad de los sistemas que protegen "las infraestructuras críticas" (Lisa Institute, 2019, pág. 345/77), con conductas penalmente relevantes que sancionen aquella vulneración, y con normas de procedimiento adecuadas que aseguren su persecución y sanción.

En definitiva, la sociedad 2.0 "es una comunidad que se construye fundamentalmente con la opción de compartir de manera horizontal y fomentar la colaboración abierta de tareas y ética informática" (Calderón, Ciudadanía digital. Signo pensam, 2008, págs. 164-173) estableciendo de esta manera un "conocimiento crecidamente globalizado y tecnológicamente mercantilizado y dinámico, que funciona gracias al conocimiento

objetivo que posee la gran mayoría de los seres que actúan en la sociedad de la información" (Rendón Rojas, 2001, págs. 9-22).

Las Tecnologías de la Información y Comunicación en la sociedad actual

La información en esta era tecnológica se la puede definir como:

"El conjunto de datos que se encuentran interrelacionados y que de manera ordenada según una estructura específica, puede esta almacenarse procesarse y transmitirse a través de algún canal electrónico, además de transformar su formato para su introducción y comprensión por un ser humano, mediante un teclado conectado a una pantalla" (Desongles Corrales J. y., 2006, pág. 14).

Desde este enfoque se puede definir a las tecnologías de la información y comunicación como los "dispositivos tecnológicos que permiten editar, producir, almacenar, intercambiar y transmitir datos informáticos entre diferentes sistemas de información, que cuentan con protocolos comunes los cuales posibilitan la comunicación e interacción personal como herramienta de intercambio, difusión, gestión y acceso al conocimiento" (Cobo Romani, 2009, pág. 312).

De las definiciones que han sido insertadas en este documento, podemos llegar a establecer que el tratamiento de información en este siglo XXI ha constituido uno de los puntos más importantes en el desarrollo social, tomando en consideración aquella dependencia casi visceral por parte de la humanidad al uso de estas tecnologías, debido a la utilidad que presta y aquella versatilidad que permite realizar una serie de actividades de manera rápida y funcional, permitiendo al usuario acceder al sistema en cualquier parte del mundo con su usuario y contraseña.

Estos medios tecnológicos han permitido establecer el desarrollo de la humanidad en el campo social, económico, financiero, cultural, político, así como también han abierto las posibilidades para que personas dedicadas a actividades ilícitas, realicen actos que vulneran las medidas de seguridad de los sistemas informáticos, para beneficio propio o de un tercero, denotando así, que en la actualidad uno de los bienes más preciados es la información.

Las tecnologías de la información y comunicación permiten al ser humano en este siglo XXI, alivianar aquellas actividades propias para su desarrollo, sin embargo la cibercriminalidad, que siendo una acción de bajo costo y que definitivamente presenta problemas para la persecución, juzgamiento y sanción debido a la territorialidad en cuanto a su comisión, y competencia para su juzgamiento, han permitido a estos técnicos delincuentes incentivarlos a la vulneración de estos sistemas de tratamiento de información, principalmente los relativos al honor privacidad e intimidad.

El delito de acoso sexual

Nuestro ordenamiento jurídico punitivo describe en el artículo 163 la conducta ilícita de acoso sexual, cuyo objeto radica en que a una persona se le solicite algún acto de naturaleza sexual sea para sí o para un tercero, aprovechándose de aquella situación laboral, docente, religiosa o de cualquier otra naturaleza, en la que de una o de otra manera implique superioridad por parte del agente delictuoso y que se encuentre presente esta subordinación de la víctima hacia el atacante, y que le sea imposible impedir el acto dependiendo de su relación contractual, docente o de cualquier otra índole.

La acción del dolo típico del agente debe recaer directamente sobre las legítimas expectativas del sujeto pasivo, de tal manera que pueda beneficiarse con la ejecución de la solicitud del favor de carácter sexual que este exige y así encuadrarse en la superioridad y subordinación que tipifica la norma penal.

El derecho que tiene una persona a la indemnidad sexual, a escoger y poder decidir con quien y en qué momento mantener una relación íntima que involucre de alguna manera un contacto de naturaleza sexual, es el bien jurídico que esta clase de delito protege, esta es la razón por la cual el legislador estableció como objeto de la infracción el solicitar favores de naturaleza sexual aprovechándose de su superioridad y que de esta manera afecte las ilusiones, metas y objetivos propuesto de la víctima.

El delito de acoso sexual es una conducta que se viene ejecutando durante mucho tiempo, razón por la cual al momento de su tipificación se establecieron sanciones que van entre uno y cinco años de pena privativa de libertad, y que la gradación de la pena va de acuerdo a las circunstancias de la infracción, esto es el grado de afectación a la víctima, o la incapacidad que puede producir, así como también la discapacidad o minoría de edad como elemento circunstancial del tipo, que le impide al sujeto pasivo decidir sobre el abordaje de naturaleza sexual.

Al analizar los elementos descriptivos del tipo objetivo del delito de acoso sexual, se puede llegar a establecer que las herramientas que se utilizan para poder cometer el acto lesivo no denota con especificidad cuál es el mecanismo que debería de utilizarse para solicitar el favor de naturaleza sexual, lo que sí exige este tipo penal es que debe de existir una clase especial de superioridad y que la víctima sea subordinada a la misma, lo que permite de manera clara la relación intersubjetiva entre los sujetos descritos en el injusto penal, de tal manera que se pueda evidenciar que esta solicitud se realice a través de una misiva, un mensaje escrito, redes sociales o cualquier otro medio que permita el viaje de la información a través del ciberespacio.

En tal virtud, se puede establecer que existe la consumación del delito de acoso sexual cuando se utilizan las tecnologías de la información y comunicación como medio directo

y efectivo para alcanzar la ejecución de la infracción resultante, que naturalmente no tiene que ver con la relación íntima sino tan sólo con la exigencia del favor de naturaleza sexual que exige el tipo descrito.

El derecho al propio entorno virtual

La multiplicidad de derechos todos relativos a la intimidad, privacidad, se lo considera como un derecho de nueva generación denominado “Derecho al propio entorno virtual” (Sanchis Crespo, Delincuencia informatica. Tipos delictivos e investigación. Con jurisprudencia tras la reforma procesal y penal de 2015, 2019, pág. 229), ya que tiene dentro de sus elementos constitutivos las nuevas tecnologías.

Este nuevo derecho se lo puede encasillar en la cuarta revolución industrial en la que se encuentran sumidas las tecnologías de la información y comunicación, caracterizada principalmente “por la fusión de estas tecnologías que desdibujan las líneas que separan en la especie las esferas físicas, digitales y biológicas” (Schwab, 2017, pág. 2), permitiendo que de una manera directa las Ciencias aplicadas informáticas, incidan en la vida cotidiana de las personas teniendo acceso a información privilegiada personal o pública, sin restricción alguna, y que para poder acceder a ella sin el permiso del titular, se debe vulnerar las medidas de seguridad de los sistemas automatizados de información que impiden el libre acceso a los datos personales.

El derecho a la intimidad se encuentra amparado por “la autonomía individual integrada por sentimientos, hábitos, costumbres, relaciones familiares y posiciones económicas que integran el estilo de vida de una persona, y que se consideran reservadas al individuo cuyo conocimiento significa un peligro para la intimidad” (Palazzi, 1999, págs. 51-92) y que él mismo se encuentra amenazada por esta era digital que presenta innumerables herramientas que de una u otra manera contribuyen a que se puedan hackear los sistemas digitales, vulnerando el derecho a la autodeterminación informática, cuyo bastión de defensa tan sólo se encuentra garantizado por el derecho a la seguridad de la información.

“El proteger de cualquier invasión que pueda realizarse en el ámbito de la vida personal y familiar, y que la persona excluya del conocimiento ajeno a las intromisiones de terceros contra su voluntad” (Riquert, 2003, pág. 54), forma parte de aquel derecho constitucional a la intimidad que se lo puede encasillar dentro de la parte personal, así como el derecho a que la información digital se encuentra bajo reserva.

El acoso sexual a menores por las redes digitales, o child grooming

El término Child grooming es una frase proveniente de la lengua inglesa, la cual se puede entender cómo el hecho de que a una persona menor de edad se le realiza

persecución a través de medios informáticos, cuando el único objetivo es ganarse la amistad y poder acceder sexual o eróticamente a la víctima.

El tratadista español Eloy Velasco Núñez enuncia que:

El delincuente trata de generar una confianza impostada conseguida mediante la permanencia temporal e insistencias constantes a través de las nuevas tecnologías, para obtener el resultado de establecer un encuentro o varios, y mantener un cierto control emocional sobre el menor con escasa madurez sexual, para preparar en el mundo virtual, el terreno para el abuso o el delito de pornografía infantil, en que el proveedor sea el propio menor (Velasco Núñez, 2019, págs. 147-148).

Al analizar las conductas de acoso y acceso sexual, nos vamos a dar cuenta que existe una diferencia entre ellos, ya que en el acoso sexual a los menores mediante medios electrónicos se exige tener una conexión directa con la víctima en el que se solicita el favor de naturaleza sexual, y en el acceso el objeto ilícito es tener contacto con la víctima, pero que se relacionan específicamente por el bien jurídico que protegen como es la indemnidad sexual.

El artículo 173 del Código Orgánico Integral Penal tipifica el delito de Child grooming bajo la denominación de: “Contacto con finalidad sexual con menores de 18 años por medios electrónicos” (Asamblea Nacional del Ecuador COIP, 2014, pág. 20), estableciendo de manera clara y de forma directa que el objeto de la infracción es el acceso a una persona que, mediante el uso de un sistema automatizado de información sea este informático, telemático o de telecomunicaciones, o mediante el uso de dispositivos tales como: teléfonos celulares, tablets u ordenadores, proponga a un menor de edad un acercamiento que tenga carácter sexual o erótico, a través de la concertación de un encuentro material para dicho fin.

En atención a los elementos descriptivos del tipo objetivo, se puede llegar a determinar que la víctima de la infracción sea menor de 18 años, y que obligatoriamente este contacto tiene que realizárselo a través de las TIC’s, mediante redes sociales, correos electrónicos u otra comunicación directa mediante dispositivos digitales, que permiten el viaje de la información por el ciberespacio.

Es necesario tener presente la diferencia fáctica existente entre el acto de acoso sexual o aquel que tenga una finalidad erótica, dentro de los que se puede encuadrar los siguientes actos realizados por el agresor: 1. Manoseo que tenga como finalidad no llegar a lugares íntimos pero que implícitamente tengan ese objetivo; 2. Manipulación corporal que tácitamente indique llegar hasta una relación sexual; y 3. acciones directas en las cuales no existe un contacto con la víctima, pero que denote de una manera objetiva que al realizar estos actos representativos que tienen un carácter sexual erótico,

se puede llegar a determinar de que el fin que busca es el mismo, aunque el agente no acceda carnalmente a ella.

METODOS

La modalidad de la investigación fue cualitativa. Para el desarrollo de la presente investigación fueron utilizados los siguientes métodos:

1. Método histórico lógico que permitió establecer cómo se encuentran desarrolladas las TIC's, las sociedades de la información, y cómo se encuentra influenciada para la comisión del delito del Child grooming.
2. Análisis lógico aplicado a las diferentes definiciones sobre el uso de las tecnologías de la información y comunicación en la consumación de tipos penales, así como la comprobación mediante la prueba informática.
3. Método de análisis jurídico comparado que fueron aplicadas aquellas disposiciones ecuatorianas y extranjeras referente a esta clase de tipos penales, y su relación con la informática tanto en el campo sustantivo, así como la evidencia digital y cuáles son aquellos elementos fundamentales para la comprobación de la infracción.

Como técnica de investigación se utilizó el análisis de contenido para llegar a determinar cuáles fueron las tesis básicas que se encuentran sustentando el tema, analizando varias fuentes documentales que tienen relación con la informática, la evidencia digital y la teoría del delito.

RESULTADOS

El verbo núcleo del tipo detallado en el artículo 172 del Código Orgánico Integral Penal es concertar, teniendo como objeto de la infracción el encuentro que tiene el agente con un menor de 18 años, mediante el uso de medios electrónicos y telemáticos con fines de naturaleza sexual o eróticos.

De los elementos descriptivos del tipo objetivo en el delito de child grooming se puede llegar a determinar los siguientes:

1. Medios electrónicos, telemáticos o digitales.
2. Concertación de cita con la víctima.
3. Minoría de edad.
4. Propuesta acompañada de actos de naturaleza sexual o erótico.
5. Coacción o intimidación para dicho acercamiento.
6. Suplantación de identidad.

7. Uso de las tecnologías de la información y comunicación.

En cuanto al elemento normativo del tipo objetivo podemos observar que este recae sobre la indemnidad sexual, así como la vulnerabilidad de aquella persona menor de 18 años ante el acto de seducción o engaño con la finalidad de alcanzar dicho consentimiento, así como también podemos analizar aquella coacción física, moral espiritual o de cualquier otra índole que se ejecute al momento del acto lesivo.

DISCUSIÓN

La evidencia digital

El sagrado derecho a la defensa tiene como finalidad garantizar para cada una de las personas investigadas, el poder acceder de manera total a cada uno de los elementos de convicción o evidencias que han sido individualizadas, levantadas y obtenidas garantizándose de manera directa el debido proceso

Con el advenimiento de la era tecnológica cuya característica principal es: “propiciar la transformación digital de la sociedad en tanto que todas las realidades actuales tengan una traducción informática que dota de infinitas posibilidades de tratamiento” (Sanchis Crespo, Delincuencia informatica. Tipos delictivos e investigación. Con jurisprudencia tras la reforma procesal y penal de 2015, 2019, pág. 253), han permitido el desarrollo de la sociedad y de agilitar todas sus actividades diarias, así como también comprobar la existencia de la infracción informática, mediante la recopilación de archivos digitales en las cuales se establecen protocolos y manuales que tiene como finalidad garantizar la cadena de custodia al momento de individualizarlos y levantarlos, mediante la “colección, preservación y necesidad garantizando que la prueba digital no se encuentre contaminada, y así su actividad probatoria penal se desarrollaría sin conculcación de los derechos para los justiciables” (Petrone, 2014, pág. 18).

La prueba digital como elemento fundamental para poder justificar el delito informático, pasa diametralmente por dos componentes principales; así el primero tiene que ver con aquellos principios que respaldan su legalidad tales como: “la especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad” (Sanchis Crespo, Delincuencia informatica. Tipos delictivos e investigación. Con jurisprudencia tras la reforma procesal y penal de 2015, 2019, pág. 269), que permiten para la investigación tecnológica sustentar la misma a través de la experticia informática, mediante un marco normativo debidamente sustentado; y el segundo de los componentes parte de la:

Necesidad de autorización judicial establecida para la resolución emitida por la autoridad competente, en la que se mantienen el secreto de las actuaciones, la duración de la misma, la posibilidad de prórroga, y que este control judicial garantice la no afectación

de los derechos de terceras personas (Sanchis Crespo, Delincuencia informatica. Tipos delictivos e investigación. Con jurisprudencia tras la reforma procesal y penal de 2015, 2019, pág. 269).

Estos principios han sido desarrollados por la autora española Sanchis Crespo, los cuales se encuentran sustentados en la Ley de Enjuiciamiento Criminal, en el cual explica que la especialidad “es una medida relacionada con la investigación de un delito concreto” (Sanchis Crespo, Delincuencia informatica. Tipos delictivos e investigación. Con jurisprudencia tras la reforma procesal y penal de 2015, 2019, pág. 272); la idoneidad de la cual se puede establecer que la evidencia digital como tal debe de encontrarse apoyada por la ley, “únicamente cuando se adopten medidas restrictivas de los derechos fundamentales que vayan a ofrecer una utilidad para la investigación del hecho delictivo concreto” (Otamendi Zoraya, 2017, pág. 107).

Ciertamente tenemos la excepcionalidad de la necesidad de la prueba pericial informática, en la cual se la considera de capital importancia al momento de “la comprobación del hecho, así como la determinación de su autor, la localización de aquellos medios de prueba que se encuentren dificultad para obtenerlos (Sanchis Crespo, Delincuencia informatica. Tipos delictivos e investigación. Con jurisprudencia tras la reforma procesal y penal de 2015, 2019, pág. 276), permitiendo de esta manera presentar ante el juzgador elementos claros y precisos que coadyuven a comprobar el cometimiento de la infracción, y finalmente la proporcionalidad que debe observarse ante el “sacrificio de derechos fundamentales y que estos no sean superiores al beneficio de la adopción de la medida” (Sanchis Crespo, Delincuencia informatica. Tipos delictivos e investigación. Con jurisprudencia tras la reforma procesal y penal de 2015, 2019, pág. 269).

La obtención de los elementos de convicción que sirvan como base para poder sustentar una acusación, requiere obligatoriamente de técnicas especiales de investigación tales como: la interceptación de comunicaciones telefónicas o telemáticas que determinen de manera fehaciente la inculpación al sujeto activo de la infracción en la concreción del resultado, en el que se ha exigido la reunión con fines de naturaleza sexual, así como también el registro de aquellos dispositivos de almacenamiento masivo que habiendo obtenido ya la autorización judicial, habilita a los investigadores a realizar allanamientos a domicilios y obtener todo equipo que tenga el carácter de electrónico o informático sean estos tablets, celulares, computadores, laptop, o cualquier otro artefacto que permita el almacenaje masivo de información, como pueden ser las tarjetas de memoria, USB, pendrive, memorias externas, hard drive, o aquellos soportes físicos como son los CD, en los que se encuentren almacenada información, así también las nubes de

computación “cloud computing” donde se guardan datos informáticos en servidores tales como: Google Drive, OneDrive, iCloud, Dropbox y que de manera especial permitan obtener la autorización judicial para la preservación, apertura, examen, extracción, análisis y materialización de la información contenida en estos soportes tecnológicos.

Es necesario garantizar los derechos de las personas que están siendo investigadas, razón por la cual se necesita autorización del juzgador para esta interceptación y grabación de comunicaciones orales y en video, mediante los seguimientos y vigilancias que permitan almacenar la información en dispositivos electrónicos o cualquier otro medio, capaz de captar imagen y realizar seguimiento, así como la localización del agente, y que estas garanticen que efectivamente fue el sujeto activo quien cometió el acto lesivo.

Los elementos descriptivos del tipo objetivo del artículo 173 del Código Orgánico Integral Penal, exige de manera taxativa que el medio para la comisión de la infracción es la informática y la electrónica, sin embargo este autor considera demasiado exigua la terminología referida, ya que en su lugar debería de utilizarse “las tecnologías de la información y comunicación” que abarca de una manera mucho más amplia aquellos sistemas automatizados que permiten el tratamiento, almacenaje y manejo de la información, ya que la evidencia digital es el punto central en la tipicidad como elemento que tiene que ser probado dentro del juicio, lo que permite vincular este delito que se encuentra íntimamente relacionado con el automatismo informático y toda su infraestructura digital.

Por lo expuesto, podemos llegar a determinar que en cuanto a la evidencia digital obtenida a través de una investigación tecnológica, la cual deberá ser sustentada en el juicio ante el órgano jurisdiccional competente, esta “parte de la garantía constitucional que se encuentra asociada al sacrificio de derechos fundamentales, que opera como fuente legitimante”, (Manchena Gomez y Gonzalez-Cuellar, 2015, pág. 212), para que en base al principio de verdad procesal, el juzgador tenga la suficiente claridad que le permita sustentar su decisión de que los hechos se suscitaron de una manera determinada, y así basado en una experticia científica, con una evidencia aceptable, técnicamente pueda sustentar su decisión.

La carga probatoria

“La base del juicio penal es la comprobación de la existencia de la infracción y la individualización de sus autores y cómplices, mediante el nexo causal cuyo vínculo une el injusto penal con sus responsables” (Santillán Molina, Mas alla de la duda razonable, 2014, pág. 41).

El principio doctrinario de legalidad de la prueba que se encuentra establecido en el numeral sexto del artículo 454 del Código Orgánico Integral Penal que en lo medular ordena, que esta prueba solamente tendrá valor cuando ha sido pedido en el momento procesal oportuno, la cual, siendo elemento de convicción, ya ha sido examinada y contra examinada en la investigación fiscal por los sujetos procesales, así como ejerciendo su derecho a solicitar la exclusión cuando considere que la misma ha sido obtenida violando derechos fundamentales, obliga de manera imperativa a que se maneje de manera correcta las cadenas de custodia, así como las autorizaciones judiciales y que las pericias que han sido elaboradas para poder obtener dicha información relevante para el proceso, se las haya realizado en base a las garantías del debido proceso.

Los indicios, huellas o marcas que ha dejado la infracción así como aquellos instrumentos con que se la cometió, o el resultado de la infracción si es que pueden ser recogidos y habidos, deberán ser individualizados por parte del personal del Sistema de Medicina legal y Ciencias forenses, que en este caso serían los peritos informáticos, los cuales deberán realizar los siguientes actos que en aplicación de las reglas de la cadena de custodia, pueda garantizarse su inviolabilidad desde el momento de su levantamiento, es así que deberán:

1. Identificar qué clase de evidencia se trata.
2. Levantar aquellos indicios con la finalidad de establecer determinadamente de cuáles son sus características.
3. Conservar la integridad de dichos elementos para así poder garantizar la individualización de cómo fueron encontrados al momento de levantar la evidencia.
4. Preservar la evidencia en contenedores adecuados que permitan garantizar la inalterabilidad de los mismos desde su levantamiento, traslado en cadena de custodia, y entrega al perito para su reconocimiento y examen.
5. Rotular el indicio y así identificar de qué elementos se trata; y,
6. Ejecutar las reglas básicas para mantener la cadena de custodia.

La Constitución de la República del Ecuador en su artículo 76 garantiza el derecho a la presunción de inocencia, y en el Código Orgánico Integral Penal en el numeral cuarto del artículo 5 establece la obligación de los sujetos procesales a que, planteando sus teorías ejerzan el derecho a la defensa, es así que el procesado puede plantear una teoría jurídica positiva como un argumento alternativo al planteado por Fiscalía General del Estado, en atención a las proposiciones fácticas encontradas al momento mismo de la infracción, y levantados los indicios conforme al procedimiento normal y conservados

y trasladados en cadenas de custodia; o en su defecto pueden plantear una teoría jurídica negativa, que no exige ningún planteamiento por parte de la defensa del procesado, sino que se acoge a la presunción de inocencia, en la que la carga de la prueba le corresponde estrictamente a Fiscalía General del Estado, quién en aplicación del principio de objetividad detallado en el numeral 21 del artículo 5 del mismo texto legal invocado, le corresponde recabar todos los elementos de convicción para poder sustentar una acusación, así como también aquellos elementos que coadyuven a la defensa del procesado para que de esta manera se pueda garantizar su derecho a la defensa, y así, en su obligación constitucional, Fiscalía pueda romper el estatus de inocencia y sustentar ante el juez aquellos elementos indiciarios que permitan coadyuvar a que el juzgador llegue a una conclusión determinante y al convencimiento de que la infracción se ha cometido de una manera específica, y de que el procesado es autor de la misma.

Por lo tanto, la carga de la prueba tanto en la teoría jurídica positiva como en la negativa planteada por la defensa de los procesados, le corresponde única y exclusivamente a Fiscalía General del Estado, ya que es este en atención a su rol constitucional y legal, quien se encuentra en la obligación de investigar los hechos, recabar los elementos de convicción y presentarlo en base a las garantías del debido proceso ante el juzgador, en la audiencia preparatoria de juicio y ante el Tribunal de Garantías Penales, en el juicio, para que éstos alcancen el valor de prueba, y así poder sustentar su acusación y que los hechos investigados lleguen a recibir una sentencia conforme lo establece la ley.

Es por esto que los agentes fiscales deben tener mucho cuidado al momento de obtener los elementos de convicción que servirán de base para la acusación, así como también para la teoría planteada por los sujetos procesales, ya que la violación al debido proceso en cualquiera de las etapas en las que se desarrolla el proceso penal, nulitaría el mismo, y por ende la posición jurídica del acusador social.

En tal virtud, en el delito de child grooming o acoso sexual a niñas, niños, o adolescentes a través de la red, se necesita justificar cada uno de los elementos descriptivos y normativos del tipo objetivo, detallados en el Orgánico Integral Penal, para así poder alcanzar una sentencia condenatoria en contra del procesado, el mismo que haya adecuado su conducta al tipo penal descrito en el artículo 173 del texto legal invocado.

CONCLUSIONES

Los sistemas automatizados de información se han convertido en una herramienta fundamental en la vida cotidiana de los seres humanos, y que sirve como medio de prueba en el derecho procesal penal.

En el tipo penal de child grooming se ha podido llegar a determinar que las tecnologías de la información y comunicación son de capital importancia para la ejecución de la infracción, así como su comprobación desde el punto de vista procesal.

Los sistemas automatizados de información constituyen uno de los pilares fundamentales en la sociedad del siglo XXI, en virtud de la dependencia del *homo tecnológicus* en el uso de las TIC's.

La relación intersubjetiva que facilita la vida en sociedad, abre canales digitales para la ciberdelincuencia.

Para la adecuación de la conducta del agente al tipo penal de child grooming es necesario que la víctima tenga menos de 18 años, y que dicho contacto se realice a través de los sistemas de tratamiento de información.

La evidencia digital permite darle claridad al juzgador para que pueda sustentar su decisión de una manera precisa y determinada, en base al conocimiento técnico que presente el perito con el automatismo informático y toda su estructura digital.

La prueba pericial informática presentada en la audiencia de juicio, es pilar fundamental en la comprobación del injusto penal, así como la determinación del autor y la localización de aquellos medios de prueba que en ocasiones se vuelve difíciles de obtenerlo.

La Fiscalía General del Estado es la responsable legal y constitucional de la presentación de los elementos de convicción como medios de prueba ante el Tribunal de Garantías Penales.

REFERENCIAS

Aboso, G. (2017). Derecho Penal Cibernético. La cibercriminalidad y el derecho penal en la moderna sociedad de la información y la tecnología de la comunicación. Buenos Aires: Editorial BdeF. Ltda.

Asamblea Nacional del Ecuador COIP. (2014). *Código Organico Integral Penal.* Quito: Corporacion de Estudios y Publicaciones.

Calderón, C. (28 de Junio de 2008). *Ciudadanía digital. Signo pensam*. Obtenido de Ciberactivismo: http://www.netoraton.es

Cobo Romani, J. (2009). El concepto de tecnologías de la información. Benchmarking sobre las definiciones de las TIC en la sociedad del conocimiento. *Revista Zer*, 312.

Desongles Corrales, J. (2006). *Conocimientos Básicos de la Informática.* Sevilla: MAD.

Hilbert, M. (2009). La sociedad de la información en América Latina y el Caribe. Desarrollo de las tecnologías y tecnologías para el desarrollo. Santiago de Chile: Ediciones CEPAL, Comisión Económica para América Latina y el Caribe.

Lisa Institute. (28 de Oct de 2019). *Lisa Institiute*. Obtenido de Infraestructuras críticas: definición, planes, riesgos, amenazas y legislación, España 2020, Diario Oficial de la Unión Europea, 2008, Art. 2, literal a) Definición de infraestructuras críticas.

Manchena Gomez y Gonzalez-Cuellar, N. (2015). *La reforma de la Ley de Enjuiciamiento Criminal en 2015.* Madrid: Castillo de Luna Ediciones Jurídicas.

Ministerio de la Presidencia, R. c. (17 de Enero de 2019). *Boletin Oficial del Estado*. Obtenido de Estrategia Nacional de Ciber seguridad 2019, p 3. BOE, núm. 103: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-6347

Otamendi Zoraya, F. (2017). Las últimas de la Ley de Enjuiciamiento Criminal. Una visión práctica tras una año de vigencia. Madrid: DYKINSON S.L.

Palazzi, P. (1999). El Habeas Data en el Derecho Argentino. *Derecho y Nuevas Tecnologias, Ad-Hoc*, 51-92.

Petrone, D. (2014). *Prueba informática.* Ciudad Autónoma de Buenos Aires : Ediciones Didot.

Rendón Rojas, M. Á. (2001). Un análisis del concepto sociedad de la información desde el enfoque histórico. Información, cultura y sociedad. *Scielo*, 9-22. Obtenido de Un análisis del concepto sociedad de la información desde el enfoque histórico. Información, cultura y sociedad.

Riquert, M. A. (2003). Proteccion Penal de la Intimidd en el espacio virtual. Buenos Aires: Ediar.

Sanchis Crespo, C. (2019). Delincuencia informatica. Tipos delictivos e investigación. Con jurisprudencia tras la reforma procesal y penal de 2015. Valencia: Tirant lo Blanch.

Santillán Molina, A. (2014). *Mas alla de la duda razonable.* Santo Domingo: Editorial Juridica del Ecuador.

Schwab, K. (24 de abril de 2017). *TyN Magazine*. Obtenido de La Cuarta Revolución Industrial: qué significa y como responder a ella: https://www.tynmagazine.com/que-significa-y-como-responder-a-la-cuarta-revolucion-industrial/

Velasco Núñez, E. (2019). Delincuencia informatica. Tipos delictivos e investigación. Con jurisprudencia tras la reforma procesal y penal de 2015. Valencia: Tirant lo Blanch.