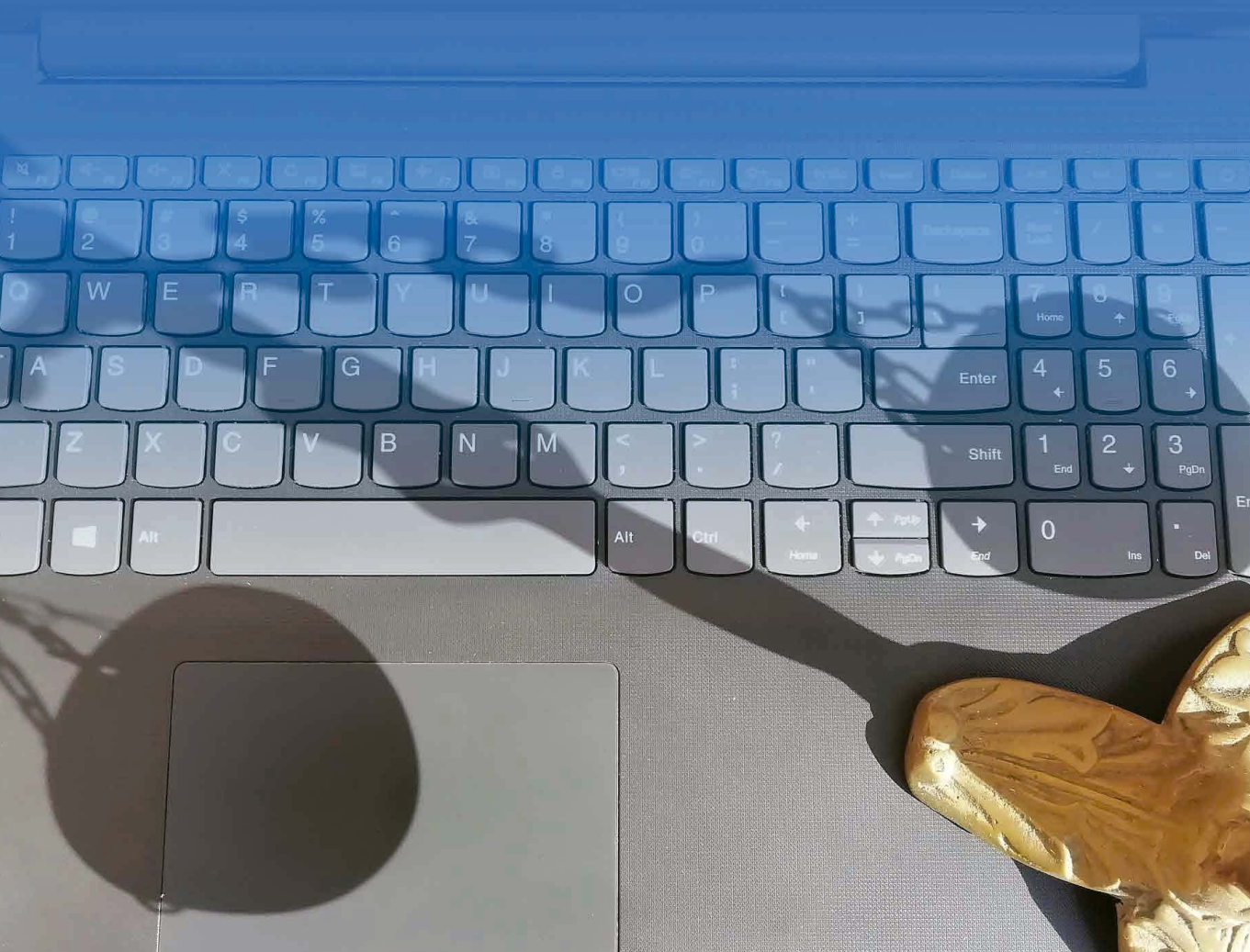
informática y DERECHO

2ª Época

Revista Iberoamericana de Derecho Informático

(Segunda Época - Primer Semestre 2023 - Número 13)



informática y DERECHO

2ª Época

Revista Iberoamericana de Derecho Informático

(Segunda Época - Primer Semestre 2023 - Número 13)

fiadi

Fundación
de Cultura
Universitaria

1.ª edición, junio 2023
ISSN: 2530-4496

Editorial Fundación de Cultura Universitaria
25 de Mayo 583 - Tel. 2 916 11 52
C.P. 11.000 Montevideo - Uruguay
ediciones@fcu.edu.uy
www.fcu.edu.uy

Impreso y encuadernado en Mastergraf SRL
Bvar. Artigas 4678 - Tel.: 2303 47 60
Montevideo - Uruguay
administracion@mastergraf com.uy

Depósito Legal 360.159 - Comisión del Papel
Edición amparada al Decreto 218/96

PRESENTACIÓN EDITORIAL

Apreciadas lectoras/Apreciados lectores:

Hemos llegado al número 13 de nuestra Revista FIADI en su Segunda Época.

Con la buena nueva de que asumimos a partir de ahora el cargo de Director de la Revista con el beneplácito y orgullo de que formamos parte de una nueva Directiva que hace historia, pues está encabezada, luego de 38 largos años, por la *primera mujer presidenta en la historia de la FIADI*: la muy apreciada colega *Dra. Bibiana Beatriz Luz Clara* de la hermana República Argentina. ¡Enhorabuena!

Es por ello que en ésta Presentación nos unimos a la felicitación que nos embarga en FIADI por este gran logro y reiteramos y reafirmamos nuestra disposición, como parte de la nueva directiva, de seguir propiciando un mayor acercamiento con todos y todas, fomentando esa visión iberoamericana de una FIADI cada vez más unida con mayor proyección en los/las jóvenes y una mayor empatía e inclusión de personas de todas las edades, concretando cada vez más ese enfoque inter y multidisciplinario para seguir sumando en cada momento y lugar.

Y es precisamente sobre esa base, tomando en cuenta que el programa del Congreso pasado incluyó varias mesas de trabajo al respecto, que abrimos el Call For Papers del número 13 de nuestra Revista Informática y Derecho 2.ª Época con la temática ampliada de *criminalidad y tecnologías*

Esté número estará dedicado a las novedades que nos traen los siguientes ejes asignados alrededor de la temática central que son:

1. Ciberdelitos/Criminalidad informática
2. Ciberacoso/Violencia digital
3. Ciberseguridad

En ese sentido es de destacar que contamos en este número con una publicación final de unos once (11) artículos, algunos pocos con rango solo de divulgación y otros más con una mayor profundidad científica. Con ellos buscamos incentivar la participación y ampliar las posibilidades de indexación en este nuevo período.

Acerca de la temática es preciso destacar lo relacionado hoy con el *debate abierto sobre ciberdelitos y el dilema de la ciberseguridad en su connotación actual*.

Ambas se han convertido en áreas claves de los estudios estratégicos. Su enfoque y desarrollo actual coincide con el advenimiento profundo de la Sociedad

de la información, y el dilema que se enfrenta a través de las redes entre computadoras y el fenómeno "Internet", cuya expansión ha configurado una dimensión moderna y ha afectado sensiblemente la vida cotidiana de los diversos sectores que integran el mundo global.

El funcionamiento diario de las estructuras que sustentan las interacciones sociales del actual siglo XXI depende de los flujos de datos que ocurren en la red y de la información y que se almacenan en el ciberespacio. Como se puede advertir, el ciberespacio es lugar de encuentro, intercambio de información y almacenamiento de datos… es por ello, que las redes cibernéticas se han vuelto indispensables para el funcionamiento de sistemas de infraestructura privada y social del Gobierno.

Al mismo tiempo que las capacidades de gestión social y gubernamental se han visto incrementadas por el uso de redes cibernéticas, también la información almacenada en el ciberespacio ha aumentado en volúmenes de cantidad e importancia; por esta razón, los acontecimientos que ocurren vulneran la estabilidad de las redes informáticas y la información contenida en el ciberespacio, representando graves amenazas para el orden social y las vidas de las personas.

Asimismo, las interacciones en el ciberespacio se han vuelto problemas de seguridad para Estados y comunidades. La clave para entender la relevancia de la seguridad en las redes es saber que los eventos que ocurren en las estructuras informáticas trascienden ya nuestra propia realidad virtual y necesitamos no solo mayor regulación y control en los diferentes ámbitos, sino también buscar implementar verdaderas campañas de educación informática, la adecuación y disponibilidad de servicios de protección virtual públicos y la búsqueda de cooperación entre actores locales y miembros de la comunidad internacional.

Finalmente, como siempre, sólo nos resta agradecer a quiénes colaboraron con sus aportes, a los que participaron formulando sus evaluaciones y a la destacada labor editorial realizada por una íntegra profesional, la Mtra. Yasna Vanessa Bastidas Cid; y a Uds. los queridos/as lectores/ras por seguir acompañándonos en una nueva edición de la Revista FIADI.

Atenta y Cordialmente,

Prof. Dr. José Heriberto García Peña

Director de la Revista
Vicepresidente de Investigación
e Innovación en FIADI

PRÓLOGO

La Revista Iberoamericana de Derecho Informático 2ª Época, se especializa en la publicación de artículos que fusionan los pormenores y desafíos bilaterales entre el derecho y la informática, relacionada esta última con el avance de las nuevas tecnologías y el impacto de estas en los derechos fundamentales de las personas.

Nuestra XIII edición dedica sus párrafos al análisis, desarrollo y reflexión sobre un tema de actual y de gran relevancia jurídica, la "Criminalidad y las nuevas tecnologías".

Las contribuciones a este nuevo número han sido otorgadas por destacados profesionales, docentes, investigadores y jóvenes investigadores que ponen a disposición de nuestros lectores un total de 11 artículos de gran calidad crítica, científica y académica.

Es una verdad absoluta que la aparición de la Internet ha promovido el desarrollo, avance y masificación de las nuevas tecnologías generando un intercambio global que plantea una modificación de los paradigmas de la comunicación. De tal manera que, ambas realidades están siendo uno de los instrumentos principales de cambio social en la actualidad.

La Internet y las nuevas tecnologías han supuesto una revolución positiva, generando nuevos empleos, nuevas profesiones, nos han acercado a las personas e instituciones de cualquier rincón del mundo, y han sido la causa y efecto de las discusiones más emocionantes en torno a los derechos fundamentales de las personas.

Los niños y adolescentes han nacido y crecido bajo el uso de la tecnología e Internet, de ahí es que se acuña el término "nativos digitales". Las tecnologías digitales brindan oportunidades de aprendizaje y educación e incluso la conectividad adquirida mediante las TIC (Tecnologías de la Información y Comunicación) ha cambiado las reglas del juego para algunos niños y adolescentes marginados, ayudándoles a desarrollar su potencial y a romper ciclos intergeneracionales de la pobreza.

Sin embargo, el uso inadecuado de las tecnologías digitales puede hacer que los niños y adolescentes sean más susceptibles de sufrir daños tanto en línea como fuera de ella, generando la necesidad de analizar la seguridad y el peligro al que se encuentran expuestos.

Así, el primer artículo de esta edición ha sido dedicado como su título lo indica a la "Ciberseguridad: el peligro al acecho de los niños, niñas y adolescentes", cuya autora es doña Laura Camila Peñuela Jiménez.

Ante nuestra nueva normalidad tecnológica y ante la facilidad de comunicación que permiten las redes sociales, aplicaciones, mensajería y otro tipo de usos de las nuevas tecnologías, el problema de la seguridad y el peligro no se centra solamente en los niños y adolescentes, sino que ha ido generando una especie de inmunidad en el ejercicio de la ciberviolencia que afecta tanto "a chicos como a grandes".

Por esta razón, es de especial relevancia la lectura del segundo artículo de nuestra edición, titulado "Ciberacoso en Perú, la amenaza sin rostro", escrito por el Dr. Fernando Martín Robles Sotomayor y doña Verónica Ramos Núñez, cuyas reflexiones pueden hacerse extensivas a cualquier país de cualquier continente.

Ahora bien, a medida que transcurría la pandemia por el virus COVID-19, la humanidad fue capaz de desarrollar sus más altos porcentajes de intelectualidad dando lugar a la tecnología más vanguardista de los últimos años. Así, la humanidad responde a los efectos del virus desde múltiples frentes adaptando la realidad a múltiples cambios en los diferentes aspectos de la vida (educación, innovación, políticas ambientales, espacios físicos, etc.). Es en este contexto que irrumpe poderosamente el "Metaverso", un universo digital con verosimilitud excepcional, pero que nuevamente deja ver las desigualdades entre los diferentes actores de la población.

Por este motivo, el cuarto artículo de nuestra edición, redactado por las doctorandas doña Paola Consuelo Ramos Martínez, y doña Claudia Bibiana Ruiz, lleva consigo una intensa reflexión sobre "La "meta" es un uní "verso" con perspectiva de género".

A partir del desarrollo acelerado de la internet, también emergen y surgen nuevos términos como *cibercrimen, ciberdelito o ciberdelincuencia,* que describen de forma genérica los aspectos ilícitos cometidos en el ciberespacio. El uso de los medios informáticos y de Internet para delinquir, ha dotado a los nuevos delincuentes un poder de difusión tal, que prácticamente cualquier lugar del planeta con conexión a la red, se encuentra vulnerable al alcance de sus métodos.

En este contexto, el maestro en derecho penal don Daniel Ernesto Peña Labrín nos sumerge en un interesante quinto artículo denominado "Rol de la prevención en la expansión de la ciberdelincuencia", donde nos enfatiza en la concientización y consecuentemente "evangelización" a los cibernautas en seguridad informática y ciberseguridad, reconociendo que el factor humano es la pieza del rompecabezas más fácil de atacar.

Del mismo modo, en esta edición número XIII de nuestra Revista, los profesores de la Universidad Autónoma de Chihuahua, México, don Ricardo Ramón Torres Knight y doña Osiris Abril Méndez Morales, nos dibujan los lineamientos principales de las políticas de ciberseguridad mediante un sexto artículo titulado "Esfuerzos dentro del Estado de Chihuahua, México en materia de ciberseguridad".

A su vez, y para una mejor comprensión sobre el concepto de ciberseguridad, el séptimo artículo de esta obra titulado "Escenarios de atención digital y contemplaciones de ciberseguridad MX", cuya autoría pertenece al Dr. Carlos Ramírez Castañeda, analiza tres escenarios de impacto relacionados a la ciberseguridad bajo el ejemplo de México, partiendo con una escala en donde la información e integridad del usuario desde su navegación podría tener afectaciones, en un segundo escenario, señala al patrimonio e instituciones financieras como objetivo de comisión de delitos, y para finalizar realiza una reflexión sobre el escenario de acción nacional interno para la prevención.

Generalmente, cuando los ciberdelitos traspasan las barreras de la conciencia y ante la falta de control de la ciudadanía y la inexistencia de normas de índole preventivas no reactivas, las políticas de estado y de gobierno suelen decantar en la tipificación penal. Con todo, los Estados realizan su mejor esfuerzo para tutelar los derechos de las personas ya sea que estos recaigan sobre su honor, su patrimonio o su integridad. El octavo artículo de esta publicación recae sobre el interesante título "Aproximación a las falsificaciones informáticas en la legislación penal venezolana", en donde su connotado autor, el abogado don José Gregorio Pumarejo Luchón, expone de forma clara y precisa sobre la regulación de la falsificación de documentos electrónicos.

De igual forma, el artículo noveno de esta edición dedica sus líneas a las acciones que derivan de las autoridades estatales, policiales y judiciales con miras a buscar soluciones reales y objetivas que promuevan la protección de la población en los diferentes escenarios tecnológicos en que hoy se les presenta la vida. Así el Dr. Juan Alejandro Montoro Sánchez en su estudio titulado "La Orden de Conservación de datos: una medida de aseguramiento de fuentes de prueba imprescindible para la investigación de los delitos de odio cometidos en línea", aborda la regulación de la Orden de Conservación de Datos prevista en el art. 588 octies *LECrim (España)*, como medida idónea de aseguramiento de fuentes de prueba a disposición de la Policía Judicial y del Ministerio Fiscal para garantizar la eficacia de la investigación de los delitos de odio cometidos en línea.

Agregamos a estos importantes aportes algunas de las normas aprobadas en el Perú para combatir los delitos informáticos y la ciberdelincuencia, y que son examinadas por la Maestra doña Carmen Milagros Velarde Koechlin en el título décimo de este número denominado "Prevención de los ciberdelitos. Algunas reflexiones desde casos ocurridos en el Perú". En particular, el artículo recoge casos especiales como la norma de neutralidad de la red que faculta el bloqueo de nombres de dominio o aplicativos informáticos maliciosos, así como el uso de la geolocalización para las investigaciones de determinados delitos. Se resaltan casos de lucha contra la ciberdelincuencia y delincuencia como son el caso The Pirate Bay, el caso Picap y el caso de la suplantación de identidad a través del uso de la biometría con huella dactilar.

Finalmente, esta edición número XIII nos presenta y representa a través de un excepcional comentario jurisprudencial, un "caso de la vida real". Sus líneas fueron trazadas por el Dr. Rodrigo Alejandro Gómez Torres, docente e investigador de la Universidad de Salamanca, España, y aborda minuciosamente en su título "Plataformas digitales como medios para la concreción de violencia digital

en contexto de género", el equilibrio en el debido proceso, el derecho de defensa y los derechos de la víctima de violencia de género en un proceso judicial argentino.

Sirvan estos valiosos artículos de investigación para incentivar el estudio y dedicación de todos aquellos lectores y profesionales que hoy intentan encontrar el punto exacto donde confluyen el derecho y las nuevas tecnologías. Estaremos siempre agradecidos por el reconocimiento que le otorgan a través de la lectura a nuestra ardua labor de llevar a ustedes un número más de nuestra excelentísima revista.

Mtra. Yasna Bastidas Cid

Editora General

Revista Fiadi 2.ª Época

INFORMÁTICA Y DERECHO

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO
(SEGUNDA ÉPOCA)

FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES
DE DERECHO E INFORMÁTICA

ISSN 2530-4496 – N.º 13, 2023, PP. 15-28

CIBERSEGURIDAD: EL PELIGRO AL ACECHO DE LOS NIÑOS, NIÑAS Y ADOLESCENTES

CYBERSECURITY: THE LURKING DANGER FOR CHILDREN AND ADOLESCENTS

Laura Camila Peñuela Jiménez[1]
Tutor: Rodrigo Cortés Borrero

1 Estudiante de la facultad de Derecho; Miembro del semillero de investigación Derecho Informático y de las Tecnologías en la sociedad de la Información; Universidad Santo Tomás sede Villavicencio. Contacto: aurapenuelaj@usantotomas.edu.co

Resumen

Los niños, niñas y adolescentes son sujetos de especial protección en el derecho, es por ello que como sociedad su seguridad y bienestar son uno de los principales objetivos, sin embargo las nuevas generaciones cuentan con acceso directo y fácil a través de las nuevas tecnologías a la espacios como la WEB 3.0 o el Metaverso, espacios nuevos para muchos, inexplorados y blancos para ciberdelitos. Existen testimonios de adultos acerca de sus acciones en la WEB 3.0 o el Metaverso, quienes incluso siendo personas conscientes de las normas y peligros a los que se exponen, han caído en las trampas y engaños de personas inescrupulosas convirtiéndose en víctimas de los diferentes ciberdelitos. Es por ello que es necesario analizar la seguridad y el peligro ante los cuales se encuentran expuestos los niños, niñas y adolescentes quienes navegan a través de la WEB 3.0 o el Metaverso gran parte del tiempo.

Palabras clave

adolescentes, ciberdelito, ciberseguridad, metaverso, niños, WEB 3.0

Abstract

Children and adolescents are specially protected by law, which is why as a society their safety and welfare are one of the main objectives, however, new generations have direct and easy access through new technologies to spaces such as Web 3.0 or the Metaverse, new spaces for many, unexplored and targets for cybercrime. There are testimonies of adults about their actions in the WEB 3.0 or the Metaverse, who even being aware of the rules and dangers to which they are exposed, have fallen into the traps and deceptions of unscrupulous people becoming victims of various cybercrimes. That is why it is necessary to analyze the security and danger to which children and adolescents are exposed, who navigate through the Web 3.0 or Metaverse most of the time.

Keywords

Adolescents, Cybercrime, Cybersecurity, Metaverse, Children, WEB 3.0, Cybercrime, Web 3.0

Introducción

La WEB se ha convertido en una herramienta útil para el ser humano a partir de la cual se cuenta con la oportunidad de realizar diferentes actividades, de tal forma que se podría afirmar que la tecnología y la WEB es indispensable para gran parte de las actividades diarias, desde el inicio del día con apps que funcionan como despertadores, agendas, cronogramas, relojes los cuales a través de la web se conectan a nivel mundial, incluso algunos usan la WEB 4.0 al contar con sistemas de Google Home o HomeKit de Apple.

Sin embargo, el ser una herramienta tan utilizada permite que sea un espacio para ciberdelitos, si bien se repite la difusión de recomendaciones cómo aquellas de: 1) No enviar información personal, 2)No registrar nombres reales, 3) No enviar claves, contraseñas, códigos de seguridad a través del mismo, 4) No confiar en cualquier correo o mensaje, esto con el fin de evitar la comisión de diferentes ciberdelitos, aquellos como la infección de un malware, los ataques de phishing y pharming keylogger, botnet y crypto jacking.

A pesar de existir los diferentes protocolos de seguridad y mecanismos de ciberseguridad establecidos por las diferentes entidades y plataformas muchas personas han sido víctimas de los ciberdelitos mencionados anteriormente.

De esta forma es posible afirmar que aún contando con el conocimiento de los métodos o protocolos y de los diferentes ciberdelitos personas adultas que son conscientes de los diferentes casos de otras víctimas, que conocen y leen cada uno de los términos y condiciones que acepta y aún así son víctimas de ciberdelitos.

Ahora bien, en el presente artículo se analiza, reflexiona, cuestiona y se propone acerca de la realidad, peligros y ciberseguridad a la cuales se encuentran expuestos los niños, niñas y adolescentes en espacios como la WEB 3.0 y WEB 4.0, el metaverso y en específico en los videojuegos.

Es claro que las últimas generaciones han tenido un contacto a temprana edad con las diferentes tecnologías y con acceso directo a la WEB, de esta forma conociendo el uso de las diferentes plataformas desde funciones educativas, plataformas de streaming y videojuegos. Desde una visión cercana se podría pensar que el uso de la WEB en estas categorías no podría generar un peligro para los niños y niñas que hacen uso de estas plataformas ya sea para educación o entretenimiento.

Sin embargo es necesario analizar que muchos adultos han sido víctimas de ciberdelitos; así como existen muchos niños, niñas y adolescentes que se encuentran en el uso de las mismas plataformas, de esta forma se debe cuestionar ¿Los niños, niñas y adolescentes se encuentran en peligro al hacer uso del internet, de plataformas educativas, entretenimiento e incluso el Metaverso?

Los niños y niñas, la nueva generación en la WEB 3.0

Las nuevas generaciones nacen teniendo un acceso directo con la tecnología e ingresando a la WEB 3.0, desde el momento en que los padres sustituyen su responsabilidad de prestar atención al menor con una tablet o ipad para

distraerlo durante largos periodos de tiempo. Incluso se refiere a la generación Z aquella que nació en el mundo de las tecnologías y generación Alfa aquellos que cuentan con el 100% de tecnología en su entorno desde el momento en que nacen, es por ello que es evidente que se presentarán choques culturales entre las diferentes generaciones.

En la actualidad quienes son adultos han tenido que realizar la transición de aprender y conocer cómo funcionan las nuevas tecnologías; una característica particular de esta generación, es que se pueden identificar aquellos que nacieron sin tecnología e internet a su alcance por lo cual tienen desconfianza y precaución ante las diferentes acciones que se puedan realizar por medios electrónicos y a pesar de esto no ha sido suficiente para evitar que sean víctimas de situaciones comunes como la estafa, robo de datos o incluso el ataque con algún malware, entre otros.

A diferencia de la generación Z y Alfa se evidencia un acercamiento más temprano al funcionamiento y manejo de las tecnologías y el internet; de tal forma que se ignora por completo las advertencias y precauciones establecidas por las plataformas, aceptando términos y condiciones sin leerlas previamente. Un punto importante resulta ser la participación de los padres o tutores al tener la responsabilidad de conocer el tipo de contenido o plataformas a las cuales accede el menor.

Las expectativas de uso de la web para niños, niñas y adolescentes

De acuerdo con la ONU (Organización de las Naciones Unidas, 2021) "El Comité de los Derechos del Niño, formado por 18 expertos individuales, recomienda que los Estados adopten medidas legislativas y administrativas contundentes para proteger a los niños de los contenidos perjudiciales y engañosos"

Por lo cual el cuidado de los menores se puede dividir en tres aspectos, primero desde el hogar, los padres, madres y personas a cargo del menor deben generar un acompañamiento constante del contenido que consume y al que se expone el menor, no necesariamente limitando por completo el uso de este pero si generar un espacio libre de violencia al menor. Algunas opciones son establecer horarios y tiempos para el uso del mismo por parte del menor.

En un segundo plano se encuentran las instituciones de cuidado o educación a cargo de los menores, implementando cursos, programas, campañas de reconocimiento de los peligros y ciberdelitos a los cuales los menores se pueden exponer y ser víctimas de cualquier ciberdelito o ciberviolencia.

Y por último, el estado o gobierno el cual a partir de sus funciones legislativas puede implementar planes de concientización, educación y aplicación para los padres de familia y personas a cargo.

Promover la concientización ciberdelitos como el grooming, el phishing, el ciberbullying, la pornografia, el acoso y la suplantación de identidad, entre otros a los cuales cualquier persona se encuentra expuesta pero son los menores un blanco fácil para cometerlos. Sin embargo, el ideal de los menores ante la WEB es que esta sea utilizada con fines productivos y positivos, es decir, poder

generar enriquecimiento al conocimiento a partir del uso de plataformas, fomentar la creatividad, las interconexiones e inclusive a través del metaverso poder encontrarse en espacios positivos y sanos para los menores.

Los peligros en los videojuegos para niños, niñas y adolescentes

Actualmente los videojuegos en línea es un tema bastante común, es muy extraño el juego que no genera una interconexión en línea con los diferentes usuarios. Por lo cual, el menor está teniendo contacto con diferentes personas de manera remota mientras participa en el videojuego.

A través del videojuego el menor está teniendo contacto con una persona a quién no le ve su rostro o su identidad de esta forma el menor se está exponiendo a interactuar con personas desconocidas qué en un buen caso puede ser un niño o niña de su misma edad o en una situación negativa podría ser un adulto con intenciones negativas ya sea de abuso, acoso o situaciones de grooming en la cual está simulando ser un menor de edad para ganar la confianza del menor.

Ante el anterior escenario pueden surgir diferentes consecuencias una de ellas es que el menor establezca confianza con esta persona y sufre algún tipo de abuso; o por medio de la confianza la persona acceda a datos del grupo familiar o del hogar con el fin de estafar o robar.

Es por ello que en este punto ya podemos evidenciar qué el internet es una herramienta valiosa y que contribuye a en situaciones de tiempo, a las facilidades y a la realización de las diferentes actividades del ser humano. Sin embargo el internet es una plataforma tan amplia a la cual todas las personas tienen acceso y que no todas las apps o plataformas cuentan con ciberseguridad y controles parentales para resguardar la integridad y los derechos de los niños, niñas y adolescentes.

Otro punto evaluar de los videojuegos el tipo de contenido que transmite cada videojuego esto en consecuencia de que muchos de los videojuegos suelen compartir contenido violento o explícito al cual muchos menores tienen acceso, estando expuestos a situaciones explícitas de violencia, sexuales y de contenido no apto para menores, un ejemplo es un videojuego que se ha hecho viral llamado Huggy Wuggy.

Su misión en el videojuego, que transcurre en una fábrica de juguetes abandonada y donde el participante se tiene que ir escapando de juguetes malvados, es abrazar hasta dejar sin aliento. A pesar de que el videojuego no se recomienda para niños de menos de 12 años, Huggy Wuggy se ha viralizado, gracias sobre todo a YouTube y TikTok, en todo el mundo (solo hay que hacer una búsqueda en cualquier red social) hasta el punto que ha conseguido salir de las pantallas y convertir su formato de peluche en uno de los más reclamados entre los niños de 5 a 12 años. (Escriche, 2022)

Ante esto, es importante aclarar que la violencia no es una actividad cotidiana del ser humano y que solo en casos de supervivencia llegaría aparecer, pero en el caso de los menores que se encuentran en una etapa de crecimiento y desarrollo, quienes copian y adaptan todas las situaciones que observan de

su alrededor, por lo cual se podría evidenciar qué los menores adapten rasgos violentos a sus conductas basado en el personaje mencionado anteriormente ya que en el desarrollo del videojuego es través de los abrazos que genera la muerte y dolor a los otros.

Un factor importante en esta situación es que las personas conocen el contenido del videojuego, siendo explícitamente violento e incitador a la violencia, las personas difunden y comparten este videojuego hasta el punto de convertirse en información viral, la cual es una característica atractiva para las nuevas generaciones que viven a través de las tendencias

Otro juego con contenido no apto para menores es Roblox, esto es razón que el contenido explícito y sexual es de categoría adulta y solo esta población debería tener acceso al mismo, por consiguiente ningún menor debe tener acceso a este tipo de contenido por las diferentes consecuencias que establecen en su desarrollo.

El juego Roblox que es la novedad entre niños al ser una plataforma para crear juegos y aunque cuenta con estrictos protocolos de seguridad, los jugadores sin importar su edad pueden acceder de forma rápida y sencilla a encuentros de índole sexual.

Está plataforma establece algo particular y es el hecho de que incluso los adultos se han sentido vulnerados al usarla porque en un inicio las personas encontrarán divertido crear salas de juegos el inconveniente surge cuando dichas Salas son invadidas por avatares imitando contenido sexual. (León, 2022)

De esta forma a pesar de que el Internet tiene beneficios es evidente que hace falta regular diferentes plataformas o contar ciberseguridad y controles parentales al momento de ingresar a ellas, ya sea a través de filtros para identificar a los adultos de los niños porque incluso si existe contenido que resulta incómodo o abusivo para los adultos, las secuelas que puede generar en un niño al tener acceso a ellas pueden llegar a ser irremediables a nivel psicológico y desarrollo.

Acerca de la clasificación de PG-13

Las películas y series son el entretenimiento en el hogar más común que existe, consumir los programas de televisión a través de plataformas de streaming es más común a través de plataformas como Twitch, Youtube, Netflix, Disney, HBO, entre otros.

De primera mano se puede analizar las plataformas de video, ya sea contenido educativo, de juegos, comida, series o programas; en un inicio puede resultar un espacio con beneficios como los tutoriales para aprender algo nuevo, repasar temáticas o conocer de algo en específico; sin embargo muchas veces los padres o tutores a cargo del menor no tienen las medidas necesarias como los controles parentales de las apps y dejan al azar la navegación del menor por las diferentes plataformas.

Claramente existen diferentes plataformas que se han establecido parámetros para evitar que los menores estén expuestos a contenido no apto para ellos

un ejemplo es YouTube qué ante cualquier infracción de la persona que suba el video bloquea la cuenta y elimina el video para el público.

Por el contrario existen plataformas como tiktok qué no cuentan con tal regulación o no es tan estricta ya que a través de los hashtags los niños, niñas y adolescentes pueden acceder a contenido sexual o pornográfico sin ningún tipo de filtro. Un caso en particular son las plataformas de streaming como lo es Netflix o Disney plus en la cuales se encuentra que para evitar que los menores acceden a contenidos no apto para ellos establecen los límites de edad para cada contenido y permiten el "control parental" una opción aparentemente sencilla pero qué puede contribuir a que los menores no accedan a contenido no apto para su edad.

Si bien se conoce que existe una clasificación de contenidos y que la categoría "PG-13", especifica que el contenido no es apto para menores de 13 años, más allá de una etiqueta o categoría ¿las plataformas realizan un seguimiento de la persona que está consumiendo su servicio? Esto en razón que la plataforma al emitir contenido no apto a menores estaría incurriendo en promover o exponer a los menores, claramente como se mencionaba antes la protección a los menores de ser víctimas de ciberdelitos y ciber violencias comprende varios factores y roles, pero a partir del anterior planteamiento, se puede evidenciar que es necesario que un ente regulador establezca más normas que regulen el contenido que se está vendiendo y al que pueden acceder los menores.

Los peligros de la web 3.0 y el metaverso

Los ciberdelitos día a día se convierten en el blanco de muchos delincuentes qué a través de la confianza de las personas las convierten en víctimas de los mismos, es por ello qué es importante exponer diferentes situaciones a las que cualquiera podría estar inmerso.

En un inicio contamos con aquella situación en la cual el el adulto responsable cuenta con sus datos bancarios guardados en su laptop a la cual por x motivo el menor tiene acceso, ya sea para jugar algún videojuego o consumir algún tipo de contenido de visual; los menores no cuentan con esta responsabilidad o conciencia económica de identificar cuando realmente se debe efectuar una compra y realizar transacciones.

Por ello un menor que tenga acceso a datos bancarios podría realizar compras de contenido de videojuegos, ya sea equipaje, ropa, modificaciones para su avatar o dado el caso comprar a través de plataformas cosas que resulten interesantes, que a partir de la inocencia de un niño es algo sencillo y lo haría por su bienestar y diversión.

Ante esta situación se podría decir que existen soluciones como la devolución y el trámite con el respectivo banco o la plataforma de ventas.

Una situación de peligro en la ciberseguridad ocurre en el momento en que dichos datos son difundidos de manera errónea a través de una plataforma, un juego, un chat o incluso como se mencionó anteriormente al establecer confianza con alguno de los otros jugadores el menor dentro de su ingenuidad compartiría

dichos datos confiando en su "Nuevo amigo". Facilitando situaciones de robos, estafas o incluso fraude de identidad cómo se identifica en Estados Unidos.

Es un delito que provoca escalofríos en padres y abuelos: un delincuente roba la identidad de un niño y utiliza sus datos personales para abrir cuentas de tarjetas de crédito o realizar compras con su celular. Estos delitos pueden pasar desapercibidos durante años porque los niños no declaran impuestos ni solicitan préstamos, lo que normalmente indicaría un fraude de identidad. (Masterson, 2022)

Una situación ejemplo diferente es aquella en la cual por medio de la confianza el menor establecer lazos de amistad con un completo desconocido a través de las diferentes plataformas de videojuegos y a través de esta confianza podría llegar a ser víctima de pornografía infantil.

Un punto importante en la actualidad es la innovación del metaverso, aquella realidad virtual a la que se puede acceder con los dispositivos adecuados a través de un avatar pero en el cual se encuentra un mundo dónde se pueden realizar diferentes actividades.

Sin embargo al ser un espacio tan nuevo no cuenta con las regulaciones necesarias para establecer ciberseguridad o en dado caso, los parámetros para el uso del mismo porque existen muchas cuestiones: en un inicio ¿quién sería el encargado de regular el metaverso? ya que alrededor del mundo todas las personas lo usan y de ser así no correspondería a sus inversores y a sus creadores regular pero dicha regulación ¿Cómo podría relacionarse con la regulación interna de cada uno de los países que hacen parte?

A partir de esta pregunta se generan muchos más interrogantes pero el principal es ¿el metaverso cuenta con los filtros necesarios para evitar que un menor acceda contenido explícito y no apto para su edad, para poder garantizar una infancia y adolescencia adecuada y sana dentro de los parámetros de la tecnología?

Existe casos de personas adultas sintiéndose violentadas y abusadas dentro del metaverso, de esta forma, si una persona adulta consciente de la realidad, consciente de que se encuentra en una realidad virtual, que se identifica con un avatar y desafortunadamente sintió ser violentada (Frutos, 2022) se siente violentada por actos dentro del metaverso un espacio y que uno es regulado ¿qué se podría esperar para los menores dentro de un espacio con tanto libertinaje?

Por otro lado, un riesgo que no se podría establecer como ciberdelitos pero que se encuentra en el desarrollo de los menores con la tecnología y el internet son las tendencias, hoy en dia existen los influencers que a través de las redes sociales y el internet, difunden mensajes y tendencias entre los jóvenes y lo que se evidencia actualmente entre los menores y los jóvenes es aquella pérdida de identidad por consumir contenido sin creatividad, que mueve masas con ideas vacías, porque al querer ser como un influencer, al querer imitar sus comportamientos su forma de vestir y su forma de actuar se está generando un conflicto en el desarrollo de cada uno de los menores.

La respuesta ante los ciberdelitos en menores en Colombia

¿Qué está ocurriendo? ¿Qué sucede con los menores víctimas de ciberdelitos y ciber violencias? ¿Realmente son escuchados y protegidos o se convierten en un número más en las estadísticas?

Actualmente, en Colombia cuando un menor es víctima de cualquier tipo de ciberdelito o ciberviolencia se inicia un proceso penal de acuerdo al tipo penal cometido.

Una vez iniciado este proceso penal se genera una red de apoyo al menor, contando con profesionales en psicología y derecho quienes se encargan de establecer los daños ocasionados y el impacto del ciberdelito en el menor, cabe aclarar que este red de apoyo es para cualquier tipo de delito en menores, no es limitante a los ciberdelitos y ciber violencias.

Colombia es un país amplio en leyes pero que desafortunadamente queda corto en cuanto a protocolos de acción, se comprende que los menores requieren especial atención y protección desde la familia, las instituciones y el estado, sin embargo, se podría afirmar que las respuestas pueden llegar a ser lentas ante un ciberdelitos, muchas veces es por desconocimiento de alguna de las partes involucradas.

Desde la víctima que no conoce qué debe hacer o ante quien debe acudir, que debe contar y por que debe hacerlo, los ciberdelitos se han asimilado con resignación y muchas veces cuando un menor es la víctima del delito se recurre al lamento pero no a las vías jurídicas y cuando lo hacen, puede llegar a ocurrir qué es la institución la que desconoce del protocolo y de las garantías que debe brindar.

Es por ello, que como segundo punto se puede reconocer que sería importante contar con un protocolo de primera mano a las víctimas menores de edad expuestos a ciberdelitos y ciber violencias, es decir, un vacío jurídico dentro de la legislación Colombiana.

Ciberseguridad para niños y niñas

La ciberseguridad es importante para la protección de datos, el uso correcto de las plataformas, los videojuegos, el internet y todo aquello que lo compone. Es por ello que se han implementado algunas estrategias para proteger a los niños, niñas y adolescentes de las amenazas que se pueden presentar en el internet.

La iniciativa se desarrolla dentro del convenio firmado entre el Ayuntamiento de Cuenca y el Incibe, entidad cuya misión es reforzar la ciberseguridad, la confianza y la protección de la información y la protección de la información y privacidad en los servicios de la Sociedad de la Información, aportando valor a ciudadanía, empresas, administraciones, red académica y de investigación española, sector de las tecnologías de la información y las comunicaciones, y sectores estratégicos en general. (VocesdeCuenca, 2022).

Esta iniciativa de España podría ser una estrategia didáctica que otros países podrían adaptar a su cultura, en razón que el internet y la ciberseguridad no

son temáticas exclusivamente de España, sino que nos competen a todos alrededor del mundo, los niños, niñas y adolescentes deben ser instruidos sobre los peligros a los cuales se encuentran expuestos y cómo evitarlos, los ciberdelitos se enfrentan teniendo conocimiento de ellos y de las formas para evadirlos y no ser una víctima más.

Otro ejemplo lo ha tomado Chile y Colombia, quienes a través de su gobierno han difundido una serie de consejos para evitar que los niños, niñas y adolescentes estén expuestos a los peligros de las plataformas.

Colombia durante el 2012 ejecutó una campaña llamada "Internet Sano", mediante la cual se buscaba concientizar acerca de temas como la pornografia y ciberdelitos a los cuales niños y jóvenes pueden llegar a ser víctimas. Por ello se mencionaba que:

> Adicionalmente se ha hecho una invitación a los proveedores de Internet, para que hagan parte de esta iniciativa que pretende respaldar la masificación del buen uso de las TIC (Tecnologías de la Información y Comunicación) a través de actividades promocionales, con la entrega de controles parentales en cada activación, con contenidos ilustrativos para niñas, niños y adolescentes. Además se entregarán premios a los colegios que usen efectivamente las TIC y que adopten ésta iniciativa como suya propia. Los objetivos de "Internet Sano", son dictar medidas de protección contra la explotación, la pornografía y el turismo sexual y demás formas de abuso sexual con menores de edad en Internet, a través de disposiciones preventivas y sancionatorias. Busca además prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores de edad en Internet de acuerdo a lo establecido en la Ley 679 de 2001. (Mintic, 2012)

Entel, en conjunto con el Equipo de Respuesta ante Incidentes de Seguridad Informática Entel, (CSIRT) de Gobierno, dependiente del Ministerio del Interior, han elaborado una serie de consejos para navegar de manera segura. En esa línea, existen softwares o aplicaciones para dispositivos móviles que permiten realizar un control del uso y así aportar al cuidado responsable para una navegación más segura. (Televisión Regional, 2022).

De esta forma se puede concluir que los gobiernos deberán a través de la didáctica y la academia instruir a las personas, en especial a los niños, niñas y adolescentes de los diferentes ciberdelitos a los cuales se encuentran expuestos al hacer uso del internet o la WEB 3.0 e incluso del Metaverso, pues con un solo click cualquier persona puede llegar a robar información extremadamente importante y confidencial para cualquier persona. Por ello, las campañas de socialización y concientización resultan ser un mecanismo clásico pero en muchas ocasiones efectivo. Así como invertir en la ciberseguridad de las diferentes plataformas es otra de las posibles soluciones o prevenciones ante los ciberdelitos, estableciendo un espacio seguro para todos los niños, niñas y adolescentes.

La ciberseguridad en la ley, la norma y los convenios

La ciberseguridad en muchas ocasiones se suele limitar el término a la protección de datos dentro de la empresa pero considero que el término es más

amplio, aquellas garantías de protección y seguridad que se brinda al usuario al momento de acceder a una plataforma o herramienta en la WEB y a la hora de hablar de dichas garantías para menores es donde la ley debe regir aún más y ser más clara y minuciosa para evitar cualquier tipo de vacío o laguna jurídica. Actualmente en las legislaciones existen leyes, convenios, conceptos que trabajan de la mano de la ciberseguridad para generar un espacio seguro para niños, niñas y adolescentes así:

1. La convención de Budapest:

   Un convenio donde los estados miembros se encargaban de regular la ciberdelincuencia, comprendiendo la necesidad de la política penal para proteger a la sociedad de los ciberdelitos.

2. Ley 679 del 2001 de Colombia:

   La presente ley se encarga de establecer las medidas para proteger a los niños, niñas y adolescentes de la explotación, turismo sexual y pornografia, tipos penales que se pueden llegar a cometer a través de la WEB.

3. Ley 1273 de 2009 de Colombia:

   Mediante la cual se crea el bien jurídico tutelado de "protección de la información y de los datos", es decir, Colombia establece un bien que debe protegerse a través del derecho.

4. Ley 1098 de 2006 de Colombia:

   Mediante el cual se crea el código de infancia y adolescencia en Colombia, que tiene como objetivo establecer las garantías y protección a los niños, niñas y adolescentes.

5. El Estado Mundial de la Infancia 2017 – Niños en un mundo digital

   UNICEF emitió un documento llamado Niños en un mundo digital a partir del análisis de la evolución de la tecnología y del mayor acceso con el que cuentan los niños alrededor del mundo.

   Estableciendo las oportunidades que ofrece la conectividad, las brecha que puede existir y en efecto, los peligros a los cuales se expone una persona y un menor en el mundo digital.

6. Ley Federal de Telecomunicaciones y Radiodifusión en México

   Se encarga de garantizar el derecho a los niños, niñas y adolescentes de acceder al tecnologias de la información y la comunicación

Conclusiones

La conectividad, la WEB, el mundo digital, el metaverso y cada una de las plataformas y herramientas que surgen con la evolución de la tecnología generan muchos beneficios como peligros. Ninguna persona está exenta de ser víctima de un ciberdelito y es por ello que todos debemos tener conocimientos acerca de los peligros a los cuales nos exponemos, de los mecanismos de protección a los que se puede acudir y comprender que así como tenemos conocimiento debemos compartirlo y en especial usarlo para proteger a los más pequeños en la sociedad, al futuro, a los niños, niñas y adolescentes.

Los videojuegos y las plataformas de streaming son ese primer contacto en el cual se pueden encontrar peligros, situaciones cotidianas que en muchas ocasiones se pasan por alto.

Es por ello que las leyes son el mecanismo al cual podemos recurrir para establecer los lineamientos para generar protección y garantías de la seguridad de los niños, niñas y adolescentes.

Es decir, leyes que exijan a las plataformas de generar filtros y controles parentales para la protección de los menores, a las instituciones educativas y gubernamentales de promover la concientización, la instrucción acerca de los ciberdelitos y la ciberseguridad; a las instituciones judiciales y penales de establecer protocolos de primer acto con las víctimas ante la comisión de un ciberdelito. En conclusión, corresponde al derecho proteger y establecer los mecanismos para cuidar y proteger a los más vulnerables: los niños, niñas y adolescentes de los ciberdelitos en la WEB.

Referencias

Convenio de Budapest. Sobre la ciberdelincuencia. Budapest, 23.XI.2001

Escriche, E. (2022). *Huggy Wuggy, el peluche que tus hijos quieren pero no deberían tener.* https://es.ara.cat/sociedad/huggy-wuggy-muneco-peluche-no-deberia-recomendado-ninos_1_4432784.html

Frutos, A. (2022). *Escándalo en el metaverso: una mujer declara ser víctima de una violación virtual.* La vanguardia. https://www.lavanguardia.com/tecnologia/20220203/8032429/escandalo-metaverso-mujer-violacion-virtual-nbs.html

León, C. (2022). *Roblox, un juego* "inofensivo" *que expone a niños a contenido no apto.* Posta. https://www.posta.com.mx/nuevo-leon/roblox-un-juego-inofensivo-que-expone-a-ninos-a-contenido-no-apto/579176

Ley 679 del 2001. Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución. Diario Oficial nro. 44.509, de 4 de agosto de 2001.

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos". Enero 5 de 2009.

Ley 1098 de 2006. Por la cual se expide el Código de la Infancia y la Adolescencia.

Ley Federal de Telecomunicaciones y Radiodifusión. Nueva Ley publicada en el Diario Oficial de la Federación el 14 de julio de 2014.

Masterson, K. (2022). *Los niños se convierten en blanco para el robo de identidad y el fraude.* AARP. https://www.aarp.org/espanol/dinero/estafas-y-fraudes/info-2022/robo-de-identidad-infantil.html

Mintic. (2012). "Internet Sano", *una estrategia para proteger la identidad de niños y jóvenes en la red.* https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/

Noticias/720:Internet-Sano-una-estrategia-para-proteger-la-identidad-de-ninos-y-jovenes-en-la-red

ONU. (2021). *Expertos piden medidas contundentes para proteger a los niños de la violencia en internet.* https://news.un.org/es/story/2021/03/1489942

Televisión Regional. (2022). *Ciberseguridad: consejos para resguardar a los niños en estas vacaciones de invierno.* Televisión Regional. https://www.itvpatagonia.com/cultura/ciberseguridad-consejos-para-resguardar-a-los-ninos-en-estas-vacaciones-de-invierno/2022/07/06/62c5bca051144200092ea6e1

UNICEF. (2017). Estado mundial de la infancia 2017. Niños en un mundo digital. https://www.unicef.org/media/48611/file

Voces de Cuenca. (2022). 'Cuenca Game' conciencia a niños y jóvenes sobre ciberseguridad para un uso seguro de internet. Voces de Cuenca. https://www.vocesdecuenca.com/cuenca/cuenca-game-conciencia-a-ninos-y-jovenes-sobre-ciberseguridad-para-un-uso-seguro-de-internet/

INFORMÁTICA Y DERECHO

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO
(SEGUNDA ÉPOCA)

FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES
DE DERECHO E INFORMÁTICA

ISSN 2530-4496 – N.º 13, 2023, PP. 29-44

CIBERACOSO SEXUAL EN PERÚ, LA AMENAZA SIN ROSTRO

CYBER SEXUAL BULLYING IN PERU, THE FACELESS THREAT

Fernando Martín Robles Sotomayor[1]

Verónica Ramos Núñez[2]

1 Doctor en Derecho, especialista en Derecho Informático, catedrático universitario y Fiscal Superior.

2 Estudiante universitaria del curso de Derecho Informático del 10 ciclo de la carrera profesional de Derecho y Ciencias Políticas.

Resumen

El acoso ha ido evolucionando con el desarrollo de las Tecnologías de la Información y las Comunicaciones (TIC), lo que ha permitido que nazca el ciberacoso sexual, en algunos casos conocido como el ciberbullying, planteándonos como objetivo el determinar las dificultades ante el enemigo invisible en Perú, el ciberacoso sexual, siguiendo una metodología cualitativa de tipo básica que nos ha permitido analizar el delito de ciberacoso sexual, concluyendo que la lucha contra el ciber-acoso con propósito sexual debe realizarse preventivamente ya que un 75% de casos del ciberacoso sexual, no es denunciado por temor, riesgo de sentirse humillados, o por vergüenza de los agraviados, además de la poca efectividad y sanción benigna por la comisión de este delito pese a que existe la legislación penal que ha incorporado en el Perú los delitos de ciberacoso y ciberacoso sexual.

Palabras clave

acoso sexual, ciberacoso, delito informático, tecnología de la información y la comunicación, Perú.

Abstract

Bullying has evolved with the development of Information and Communication Technologies (ICT), which has allowed the birth of sexual cyberbullying, in some cases known as cyberbullying, with the objective of determining the difficulties facing the invisible enemy, in Peru, sexual cyberbullying, following a basic qualitative methodology that has allowed us to analyze the crime of sexual cyberbullying, concluding that the fight against cyberbullying for sexual purposes must be carried out preventively, since 75% of cases of sexual cyberbullying , is not denounced for fear, risk of feeling humiliated, or shame of the aggrieved, in addition to the ineffectiveness and benign sanction for the commission of this crime despite the existence of criminal legislation that has incorporated cyberbullying crimes in Peru and cyber sexual harassment.

Keywords

Sexual harassment, cyberbullying, computer crime, information and communication technology, Peru.

Introducción

La delincuencia informática ha ido creciendo y especializándose a la par que las tecnologías (TIC) se han desarrollado, cuando en la década de los 90 se establecía la doctrina sobre delitos informáticos en Latinoamérica, no se tenía idea de lo que podría representar en cuanto a ciberdelincuencia el avance a la web 2.0 y por ende a todo el mundo de las redes sociales en las cuales las personas pueden interactuar y conocerse virtualmente desde cualquier lugar del mundo. Si bien ese desarrollo tecnológico abrió las puertas de internet a todas las personas, que pudieron comenzar a colaborar en lo que se pensó sería una inteligencia colectiva provechosa para toda la humanidad, también dio apertura a una serie de actividades delincuenciales que anteriormente se producían únicamente de manera física, y que, al hacerse a través de las tecnologías, se volvían mucho más perjudiciales al tornarse en permanentes el algunos casos, con el beneficio de que el autor podía "esconderse" con mayor facilidad y salir impune del delito cometido.

Una de esas figuras delictivas es el acoso sexual, que con el desarrollo tecnológico se convirtió en ciberacoso sexual, denominación que evidentemente, nace de la unión de dos términos: 1) acoso y 2) ciber; cuyo conocimiento inicial, es muy importante para delimitar el tema.

De manera oportuna, iniciemos por el tema del acoso, el cual no es un término reciente ni ha dejado de usarse, pero lo que sí ha sucedido es que ha evolucionado. El portal web "stopbullying.gov" define al acoso como aquel comportamiento agresivo y no deseado entre niños o adolescentes ya sea en edad escolar, universitario e incluso entre adultos, que precisamente involucra un desequilibrio de poder real o percibido.

El acoso puede alcanzar diferentes esferas de la conducta humana, acoso laboral, acoso escolar, acoso físico, acoso psicológico, pero cuando nos referimos al acoso sexual, consideramos interesante lo referido por Olaya-Martínez (2020, p. 144), que nos dice que se trata de un comportamiento de tono sexual tal como acercamientos, miradas, susurros y contactos físicos, observaciones de tipo sexual, exhibición de pornografía, aproximaciones sexuales indirectas (empleo de símbolos, mensajes escritos, silbidos a distancia), soborno sexual, y comentarios sexuales que no son autorizados ni correspondidos.

Como consecuencia del acoso, las víctimas pueden padecer de problemas graves y duraderos. Precisamente, el acoso es el comportamiento agresivo y no deseado que incluye un grupo de acciones como amenazas, rumores, ataques físicos y verbales, y la exclusión de alguien de un grupo de manera intencional. En ese sentido el concepto inicial de que el acoso se daba entre pares, niños o adolescentes por lo común, a nivel delictivo se extiende hacia un agente adulto y una víctima menor de edad.

Antiguamente, solo podíamos hablar de tres tipos de acoso: verbal, social y físico; sin embargo, con el desarrollo de las TIC, indudablemente una revolución para toda la humanidad que ha puesto en marcha la transformación digital, el término ciber se ha vuelto un tanto común, de manera independiente o como prefijo de muchos otros conceptos relacionados con las tecnologías.

El término "ciber" surge como diminutivo de cibernético y se convierte en prefijo de múltiples términos relacionados con el uso de la informática y el internet. Con un conocimiento más amplio y profundo, Téllez (2016, pp. 149-150) nos dice que el término cibernética surge en la década de 1940 y alude a la conjunción de estudios matemáticos, físicos, neurológicos, entre otros, que responden al análisis de los sistemas de control de seres vivos o máquinas, basados en las teorías de la información, algoritmos y autómatas; es decir, la cibernética trata de los mecanismos de control y comunicación en seres vivos y artificiales.

La realidad nos muestra que, desde sus orígenes a la actualidad, el ciberacoso ha ido en aumento, en el año 2019, UNICEF realizó un estudio internacional en más de 30 países en el que participaron 170.000 jóvenes de entre 13 y 24 años para encontrar datos acerca de la incidencia del acoso a través de las redes sociales. Los resultados fueron realmente alarmantes, ya que 1 de cada 3 jóvenes había sido víctima del ciberacoso en alguna de sus modalidades y 1 de cada 5 afirmó haber faltado a clases como consecuencia de esta agresión que sufrían a través de Internet.[3]

Es así que el ciberacoso se presenta como un problema de gran magnitud y constituye una de las grandes desventajas que trajo consigo el avance tecnológico, que permite utilizar las TIC para agredir aprovechando el anonimato en la red, configurando muchas veces conductas ilícitas. Esto nos lleva a preguntarnos cómo saber si existe el delito de ciberacoso, cuando las pruebas y el autor del delito pueden desaparecer con mucha facilidad, planteándonos la siguiente interrogante: ¿Cuáles son las dificultades ante el enemigo invisible en Perú, el ciberacoso sexual?

Precisamente, esto nos da como objetivo principal el determinar las dificultades ante el enemigo invisible en Perú, el ciberacoso sexual, modalidad delictiva que, a diferencia de otros tipos de acoso, se acerca en forma oculta y ataca sin dar la cara aprovechando el anonimato que le brindan las tecnologías de la información y la comunicación.

Concepto del ciberacoso

Cuando hablamos de ciberacoso, pensamos en aquellas acciones ideadas y plasmadas en forma negativa a través del internet con el fin de obtener un cierto tipo de satisfacción; en forma más precisa, Lucas et al (2016) nos dicen que el ciberacoso es una modalidad de acoso efectuado por un individuo o por parte de un grupo, los cuales hacen uso de las nuevas tecnologías de la información y la comunicación, para agredir intencional y reiteradamente a una persona vulnerable que va a ser incapaz de defenderse por sí misma, siendo uno de los medios para estos ataques las redes sociales. (p. 27)

En posición de Orozco (2020), "el ciberacoso es una emergente forma de hostigamiento" la cual se manifiesta por diversos medios que tienen acceso a

3 Se puede encontrar mayor información en las páginas web siguientes: https://www.unicef.org/es/buscar?force=0&query=ciberacoso&created%5Bmin%5D=&created%5Bmax%5D= y https://medicoplus.com/psicologia/tipos-ciberacoso

internet, como los celulares o smartphones. Se considera a este tipo de hostigamiento como aquel fenómeno que afecta negativamente a las víctimas quienes se ven directamente agredidas, alcanzando el impacto también a su entorno familiar. (p. 21)

Nos dice De la Serna (2017) que el "término ciberacoso, también conocido como ciberbullying, viene a ser una extensión del acoso en los medios tecnológicos, por teléfono o por internet, mediante el cual una persona (acosador) trata de minar o socavar la autoestima de otra (acosado)", esta afectación se hace a través de mensajes por e-mail o cualquier tipo de red social, que tienen contenidos muy variados, pero que de manera común van a encerrar frases amenazantes, que buscan intimidar al acosado o en su defecto chantajearlo. (p.10)

En ese orden de ideas, consideramos que el ciberacoso es un episodio agresivo llevado a cabo de manera repetitiva y constante por una persona sobre una víctima la cual se encuentra indefensa, este acoso es ocasionado mediante herramientas tecnológicas de la información. Sabemos que antes que evolucione el acoso a ciberacoso, los hechos se hacían sólo físicamente, es decir, mediante un careo, en el que existían los insultos, amenazas y burlas, donde probablemente acababa en agresiones físicas, el cual era el fin del acosador; sin embargo al desarrollar su forma tecnológica, o sea el ciberacoso, la agresiòn fìsica en muchos casos no se dan, màs el impacto psicológico suele ser mayor. Un concepto muy cercano es el de ciberbullying, que algunos lo diferencian del cibeeracoso en función a la edad de la víctima y el agresor, restringiendo el término de ciberbullying únicamente a los casos en el que el acoso se realice entre menores utilizando para ello los medios tecnológicos.

En resumen, nos parece adecuado lo señalado por Sánchez et al (2016, p. 2), respecto a que la figura del ciberacoso tiene un actuar doloso (intención), uso de las TIC (Tecnologías de la información y la comunicación) que en parte es realizada por mayores de edad y en otras por algunos menores, con la finalidad de insultar, hostigar, molestar, intimidar, humillar o amenazar a otra persona que puede ser un compañero o compañera de estudios. En ese orden de ideas el ciberacoso tiene una particularidad y es que se trata de una conducta impulsiva y deliberada (Dolo), perfeccionada a través de medios digitales por grupos o individuos que, de forma reiterada, envían mensajes subidos de tono u hostiles a otras personas con la intención de ofender. Esta postura consideramos se complementa con lo referido por González et al (2018, p. 16), quienes consideran que existe una relación entre cibervictimización y ciberacoso, relacionando a personas de distinta edad y género, siendo el primero consecuencia del segundo, el cual es definido como aquel comportamiento dañino o perjudicial para la víctima, la cual también utiliza medios informáticos o tecnológicos, dando lugar a que la víctima sea incapaz o no pueda defenderse oportunamente del agresor, quien ante estas circunstancias, va a tener una posición dominante frente a la persona agraviada.

Diferencias con otros tipos penales

Es importante destacar que, respecto al ciberacoso, a diferencia de otros delitos cibernéticos en los que el agresor o victimario trata en lo posible de ocultar

toda su información personal, o en todo caso, no dejar huellas ni antecedentes en los que se podría saber su ubicación, nombre propio, de familiares, y otros, como también su verdadera identidad, en la mayoría de veces, el ciberacoso a nivel escolar presenta un contacto directo con la persona real, pero es cierto también, que en otras tantas veces el acosador se mantiene en el anonimato, pero conoce en forma directa o física a su víctima.

Sánchez et al (2016, pp. 11-12) identifican varias diferencias entre el ciberacoso y el acoso escolar común, entre las cuales destacamos las siguientes:

- Identidad del agresor puede no ser conocida por la víctima.
- La agresión se realiza sin contacto físico y con mucha facilidad a través de las TIC.
- El acoso se propaga con gran rapidez.
- La audiencia que conoce el ciberacoso puede ser muy amplia, más aún si se viraliza a través de las redes sociales.
- La durabilidad del ciberacoso, que al difundirse por la red puede durar muchos años.
- El ámbito del ciberacoso, que excede los espacios escolares.
- El acceso del acosador a la víctima las 24 horas del día y todos los días del año.
- La invisibilidad de los agresores, no siendo consciente el agresor del daño real que propina a la víctima, lo que refuerza el poder del agresor.
- Es más difícil la detección por parte de los adultos.

Un punto clave en la evolución que ha ido sufriendo el ciberacoso al considerarlo como ciberdelito, es que el victimario o acosador mantiene el anonimato; sin embargo, esto no cambia tanto en la víctima, porque igual suele recibir la parte depresiva de todo ello, es decir, que recibe la agresión o peor parte del acosador, lo cual puede conllevar a que entre en depresión y ocasionalmente hasta el suicidio.

Ortega & Mora-Merchán (2007) destacan que si bien existen muchos estudios sobre el ciberacoso, todos coinciden en la facilidad de difusión al usarse los medios tecnológicos, lo cual incrementa la agresión, y que las diferencias entre los estudios obedecen principalmente a factores sociodemográficos (sociedades rurales, urbanas, marginales, etc.), grado de implantación de las nuevas tecnologías en la sociedad objeto de estudio, o de la metodología llevada a cabo para recoger los datos (por ejemplo, cuestionarios e ítems incluidos, encuestas telefónicas, autoinformes, etc.). (pp. 9-13)

Es de incidir que en los próximos años el incremento de los casos por ciberacoso aumentará y seguirá habiendo casos un importante porcentaje de casos en la oscuridad, esa cifra negra que no se llega a conocer en concreto porque no es denunciada y sólo se explora a través de los estudios, originando que no se pueda hacer notar el daño causado a las personas víctimas de ciberacoso.

Cabe precisar que la literatura se ha encargado de deslindar el fenómeno cyberbullying del bullying tradicional, otorgándole una entidad propia con unas particularidades diferentes, lo cierto es que existen otros muchos estudios que consideran que ambos fenómenos comparten muchos puntos en común que hacen posible la idea que uno pueda ser constitutivo del otro o al menos sea clave en su formación. (Li, 2005, p. 3)

Es así como, las conductas bullying y cyberbullying surgen del entramado de las relaciones interpersonales que se establecen entre aquellos escolares que comparten escenarios comunes y, a pesar de que ambos fenómenos son considerados como comportamientos que poco tienen que ver con conductas esporádicas o accidentales, pero mucho con el dominio y el abuso en unas relaciones en las que el desequilibrio de poder es básicamente visible, ambos son caracterizados de forma diferente.

Mientras el bullying tradicional es descrito como un estilo de relación interpersonal entre individuos envuelto por un desequilibrio de poder entre agresor y víctima que se mantiene en el tiempo (Ortega, 2010, p. 19), en el cyberbullying es puntualizado como un acto agresivo, intencional realizado por un grupo o individual, utilizando las formas electrónicas de contacto, repetida una y otra vez contra una víctima que no puede defenderse fácilmente. La principal diferencia radica por tanto en las propias características que las nuevas tecnologías aportan a la forma de relacionarse (anonimato, canal abierto 24 horas, inmediatez…). Pero, además, esta modalidad requiere de pericia tecnológica de aquellos que participan en dicho fenómeno.

A pesar de ello, existe un interesante cuerpo de la literatura que ha encontrado cierto solapamiento entre los participantes de ambos fenómenos. De hecho, algunos autores como Hinduja & Patchin (2010, p. 214) señalan una implicación de más del 60% entre aquellos que dicen participar en cyberbullying y a su vez en bullying tradicional. Además, los estudios destacan la fuerte conexión entre los involucrados como acosadores de ambos fenómenos y las víctimas de las dos vías.

También encontramos investigaciones que apuntan hacia la existencia de un intercambio de roles desde un fenómeno a otro, siendo que los agresores de bullying tradicional puedan volverse víctimas de cyberbullying y los cyberagresores víctimas de bullying tradicional. Posiblemente, entre las razones que justificarían las explicaciones causales de que los ciberagresores puedan ser víctimas de bullying tradicional estaría la concepción de las TIC como una forma de compensar lo que no pueden hacer cara a cara.

Por otro lado tenemos el término grooming, que suele ser un medio para la obtención de pornografía infantil y alude al delito de propuestas a niños, niñas o adolescentes, a través de internet con fines sexuales, el cual consideramos es una actividad delictiva de mayor gravosidad y complejidad que el ciberacoso sexual. En primer lugar, el grooming tiene como víctimas únicamente a menores de edad, pero su proceso que tiene como fin beneficios sexuales y económicos a partir de su venta o difusión, tiene una primera etapa de "enamoramiento", en que el agresor (que muchas veces se hace pasar por un niño o adolescente)

genera una relación de confianza con su víctima, lo cual le permite pasar a la segunda etapa de la "sexualización", en la que el delincuente recurre a la curiosidad natural del niño o niña – púber o adolescente hacia el tema sexual, llevando sus conversaciones hacia esa temática y explorar las experiencias que podía ya haber tenido, las cuales se van convirtiendo en morbosas a fin de lograr pasar a la tercera etapa de la "agresión", en la cual el ciber, delincuente logra gracias a la estimulación sexual producida en el menor, que muestre por la cámara sus zonas íntimas o se presente desnudo, lo cual es aprovechado para grabarlo y fotografiarlo, lo que le permite comenzar con la explotación obligando al menor bajo amenazas, a que continúe mostrándose desnudo, masturbándose, haciendo juegos sexuales con objetos y que en algunas oportunidades llega a concretarse en encuentros sexuales y violaciones.

Riesgos en la red

Como se pudo apreciar hasta el momento, estar conectado en redes del internet a través del uso de diferentes dispositivos digitales, aprovechando las tecnologías de la información y la comunicación, representa riesgos que pueden perjudicar y dañar a las demás personas, siendo una modalidad el ciberacoso, pero existiendo también otras como el ciberbulliyng, más estudiado desde un punto de vista psicológico y educativo y el grooming o child grooming centrado más en los estudios legales como una de las principales modalidades delictivas por medios informáticos.

Nos dice Hinduja & Patchin (2010, p. 207) que la omnipresencia, el tipo de funcionamiento, su trascendencia y, en definitiva, la potencialidad de las TIC, las convierten en unas poderosas herramientas que, utilizadas de forma malintencionada, pueden causar verdaderos estragos en la vida de las personas, y en especial, de los y las adolescentes por ser quienes principalmente las utilizan, y que ya podían venir presentándose en las relaciones directas que mantienen los jóvenes con los demás.

Esto nos quiere decir que se encuentra vinculado directamente como un tipo de bullying. Así, la mediación de los dispositivos digitales y los entornos virtuales en la sociedad actual no sólo ha modificado la naturaleza de las relaciones interpersonales mejorándolas, sino que también ha implicado la incorporación de problemas y conflictos que ya venían afectando la vida social de los escolares. En consecuencia, el uso de estos medios tecnológicos permite que los problemas escolares, o de la red de iguales, trascienda las barreras físicas del centro escolar o del lugar de residencia, para llegar a cualquier lugar del mundo donde exista un ordenador, un teléfono móvil, u otro dispositivo digital.

Las características propias de las TIC dotan al ciberacoso de unas particularidades que los distinguen del acoso tradicional, destacando las cuatro siguientes:

a) La agresión sucede en cualquier momento y en cualquier lugar, lo que la hace especialmente difícil para desconectarse o evitar la misma en los canales de

comunicación, que gracias a la magia de las tecnologías siempre están presentes y accesibles.

b) La agresión pueda ser difundida a una gran cantidad de personas y en forma indefinida.

c) Las víctimas muchas veces no llegan a conocer nunca a la persona que los agredió, debido al anonimato que le brindan las tecnologías.

d) Suele ser más difícil de detectar por padres y docentes. (Ortega et al, 2012, p. 57)

El cyberbullying se considera un tipo de bullying ya que se han hallado evidencias que muestran la tendencia de los sujetos envueltos en acoso tradicional a inmiscuirse también en problemas de ciberbullying. De esta forma, podría afirmarse que la tecnología dota a las y los agresores de una gran fuerza en cuanto a la frecuencia, duración y amplitud de escenarios y castiga a las personas víctimas con una dureza que podría ir más allá de lo que se puede observar en el bullying tradicional, permitiendo causar daños similares o que bien pueden ser mayores, produciendo las mismas consecuencias de las que podría causar el bullying existente por mucho más tiempo en nuestra sociedad, el cual si bien suele exceptuar la violencia física, genera una mayor afectación psicológica lo cual en ocasiones, hasta incluye desgraciadamente el suicidio. (Hinduja & Patchin, 2010, p. 211)

Pero el ciberbullying, esa suerte de agresión entre menores que no deja de encerrar una relación de dominación hacia la víctima, no es el único riesgo de violencia que posibilitan los nuevos entornos virtuales. Como lo enfatizamos, los chicos de menor edad encuentran muchos riesgos en la red, para cuya defensa no suelen estar debidamente preparados, por ejemplo, está presente una realidad delictiva que tiene efectos devastadores en su vida como es el grooming, cybergrooming o también denominado child grooming. En el ámbito jurídico se hace referencia a este comportamiento que se ha convertido en delito en el Perú desde el año 2013 con la promulgación de la Ley de Delitos Informáticos, como las acciones preconcebidas de una persona adulta a través de Internet para ganarse la confianza de un niño o adolescente, con la intención de establecer relaciones con el menor de edad, para conseguir un disfrute sexual personal mediante imágenes eróticas o pornográficas que consigue del menor, quién las entrega en un primer momento en forma voluntaria, pero posteriormente obligado por la amenaza de que sus padres, compañeros de escuela o amigos de barrio se enteren de sus fotos desnudo o semidesnudo, dejando al descubierto su intimidad, logrando con ello prolongar la agresión contra la libertad o indemnidad sexual de la víctima, pudiendo llegar incluso en ocasiones, a concertar un encuentro físico y abusar sexualmente de él. (Monge, 2010, p. 71) (Panizo, 2015, p. 24)

Legislación penal contra el ciberacoso sexual en Latinoamérica

En casi la totalidad de los países latinoamericanos, se ha incorporado legislación que sanciona el ciberacoso sexual, en algunos casos de manera explícita en las normas penales, en otros, se encuentra encubierta dentro de legislaciones

que protegen a la familia y los integrantes del grupo familiar, en otros tantos casos en normativas que sancionan delitos como la violencia contra la mujer y el feminismo, más encontramos legislaciones como la peruana, en los que sí se encuentra en forma explícita la tipificación del delito de ciberacoso sexual.

Como lo señala Temperini (2014, p. 9), existe en Latinoamérica una falta de homogeneización en las legislaciones sobre los delitos informáticos, a pesar de que existe la tendencia de tipificar una serie de conductas delictivas que pueden coincidir, siguiendo en cierta manera la línea establecida por la unión europea que comprendió la necesidad de la persecución colaborativa de los ciberdelincuentes, generando mecanismos y tipos penales similares a través del Convenio contra la Cibercriminalidad de Budapest, ratificado posteriormente por países de todo el mundo incluido el Perú en el año 2019.

En ese sentido, respecto al delito de ciberacoso sexual, en Argentina se incorporó el tipo penal con la Ley "Mica ortega" el año 2013, pero en otros países, lo que se sanciona es la difusión no consentida de imágenes de contenido sexual, como sucede en Brasil, Chile, Ecuador, Uruguay, Paraguay y México, en el caso de Perú, a partir del año 2018, mediante decreto legislativo 1410, se incorporó en el Art. 176B del Código Penal peruano, el delito de acoso sexual y ciberacoso, tipificando el primero como aquella persona que de cualquier forma, vigila, persigue, hostiga, asedia o busca establecer contacto o cercanía con una persona, sin el consentimiento de esta, para llevar a cabo actos de connotación sexual. El segundo párrafo del artículo es que agrega que el delito se puede cometer también a través de las tecnologías de la información y la comunicación, teniendo como sanción en ambos casos de 3 a 5 años de pena privativa de la libertad.

Respecto a este delito, al verificar su sistematización, observamos que presenta las siguientes características jurídicas:

- Sujeto activo: Puede ser ejercido por una persona adulta, hombre o mujer; aunque la figura penal también puede ser cometida por adolescentes, en este caso sería una infracción sancionada con una medida socioeducativa en la legislación peruana.
- Sujeto pasivo: Persona mujer u hombre, mayor o menor de edad que no acepta el acoso.
- Acción dolosa (Intención) evidente de querer generar un daño (Por ejemplo, publicación en alguna red social, afectación de la autoestima).
- El bien jurídico protegido: En este tipo de delitos informáticos el bien jurídico tutelado es la dignidad de la persona y en forma complementaria la libertad sexual.
- Agravantes: La víctima es un adulto mayor, tiene entre 14 a 18 años de edad, es gestante o persona con discapacidad. También si son cónyuges, convivientes o parientes, o existe una relación de dependencia entre agresor y víctima.
- Otros agravantes: El agresor reside en el mismo lugar que la víctima o el acoso se lleva a cabo en el marco de una relación laboral, educativa o formativa de la víctima.

- Existe la aparición de otro tipo de daños como la vulneración o el ataque a la intimidad y privacidad de la persona, por ejemplo, con la difusión de fotos o videos comprometidos de él sin su consentimiento.
- Existencia de desigualdad entre el agresor y la victima (relacionado a un desequilibrio de fuerza a nivel psicológico, social o físico).
- Son insultos u ofensas repetitivas a través de vigilancia de la víctima, persecución de esta, hostigamiento o asedio.

Análisis de la problemática

Volviendo a nuestra problemática planteada inicialmente con la interrogante ¿Cuáles son las dificultades ante el enemigo invisible en Perú, el ciberacoso sexual?, corresponde precisarlos en la situación actual de nuestro país, y para ello es necesario plantear en un primer momento cuáles son los mecanismos con que cuenta el Estado para enfrentar el ciberacoso.

En primer lugar, debemos mencionar que a nivel preventivo y como medio de orientación a las personas, el Ministerio de la Mujer y Poblaciones Vulnerables (MIMP) tiene desarrollados dos programas extendidos en todas las regiones del Perú. Uno de ellos son las Defensorías del Niño y Adolescente que pueden funcionar en una escuela, iglesia, club u organización vecinal, pero que obligatoriamente existen bajo el costo y administración de los gobiernos locales, es decir en las 1678 municipalidades distritales y 196 provinciales[4] con que cuenta el Perú, bajo la denominación de Defensoría Municipal del Niño y Adolescente (DEMUNA).

Las DEMUNA brindan un servicio gratuito de atención integral cuya finalidad es promover y proteger los derechos que la legislación reconoce a las niñas, niños, adolescentes y, por extensión, a sus familias. En ese sentido cuentan con personal especializado (psicológico, social y legal) para orientar a las personas que recurren a sus servicios, celebran conciliaciones, y canalizan las denuncias hacia el organismo investigador de delitos, que es el Ministerio Público, cuanto existen indicios de violaciones a la ley penal.

Un programa más reciente del MIMP son los Centros de Emergencia Mujer (CEM), que ya cuentan con más de 400 establecimientos distribuidos en todo el país, y que brindan servicios gratuitos y especializados de atención multidisciplinaria para personas afectadas por violencia familiar y sexual. En ese sentido proporcionan orientación legal, defensa judicial, consejería psicológica y apoyo social con personal especializado y voluntariado. Asimismo, realizan labor preventiva y promoción de los derechos de la mujer y campañas contra la violencia en sus diferentes modalidades, psicológica, física, sexual o patrimonial conforme lo establece la Ley 30364 "Ley de violencia contra la mujer y los integrantes del grupo familiar".

4 La información en detalle se encuentra en https://www.gob.pe/institucion/inei/informes-publicaciones/3313436-directorio-nacional-de-municipalidades-provinciales-distritales-y-de-centros-poblados-2022

Desde el año 2014 en que fueron creados los CEM, han incrementado la atención de casos que brindan superando los cien mil anuales en los últimos años, siendo más del 80% relacionados a violencia psicológica o física, lo cual demuestra la importancia en la prevención de la violencia que se está brindando en el país, como se puede apreciar en el gráfico siguiente actualizado al mes de mayo del 2021.

Ilustración 1: Casos atendidos en los CEM

Fuente: https://mimp.gob.pe/omep/estadisticas-violencia.php

No obstante, existe una gran cifra negra de casos que no se llegan a denunciar, ya sea por el temor de que se incremente la agresión, el riesgo de sentirse humillados por las autoridades, por la vergüenza de los agraviados de que su caso se conozca públicamente, o por la falta de confianza hacia las autoridades judiciales y policiales que brindan poca efectividad en sus acciones y después de varios años de proceso judicial, en el mejor de los casos concluyen con una sanción benigna por la comisión del delito de ciberacoso.

En cuanto al ciberbullying, que como hemos visto está bastante ligado al ciberacoso (que ya es la conducta delictiva), el Ministerio de Educación del Perú, ha implementado un aplicativo denominado "SiSeVe" (http://www.siseve.pe/web/app/index) que recibe 10 denuncias diarias de alguna variedad de agresión virtual; sin embargo, señalan que se tiene conocimiento que sólo el 10% de casos se denuncia, como lo revela un estudio de la Asociación Educativa Convivencia en la Escuela[5]

5 Se puede consultar mayor información en https://www.mercadonegro.pe/actualidad/9-de-cada-10-padres-peruanos-no-considera-posible-que-sus-hijos-ejerzan-bullying-pero-que-dicen-las-cifras/

El MIMP también es consciente de que la sanción del ciberacoso es mínima y la judicialización demora mucho y no brinda una protección adecuada a la víctima, por ello ha implementado diversos programas virtuales para denunciar casos de ciberacoso y de violencia virtual, como el de "No Al Acoso Virtual" (http://www.noalacosovirtual.pe/), que en los primeros cuatro meses del año 2021 recibió más de 500 denuncias, y a través del cual se ha podido establecer que la mayoría de agresiones se hace a través de las redes sociales, principalmente Facebook, WhastApp, Instagram y Tik Tok.[6]

Las iniciativas privadas frente al ciberacoso, también apuntan que es mejor la prevención y brindar el máximo de posibilidades a la víctima para denunciar su caso, en ese sentido, frente a todo tipo de agresión sexual, existe el canal de denuncias en línea de la "Red Peruana contra la Pornografía Infantil", denominado "Seguros en Internet" (https://www.seguroseninternet.org/es/#) que entre otros rubros incluye las denuncias por ciberacoso.

Lamentablemente el Ministerio Público, organismo responsable de investigar los delitos con la ayuda de la Policía Nacional del Perú, cuentan con mínimo personal especializado para la persecución de los delitos informáticos entre los cuáles, el ciberacoso no es el de mayor prioridad, lo que da lugar a que muchas veces las personas que inician un proceso judicial queden desprotegidas a merced de sus victimarios, situación que se extiende a lo largo de los años que puede durar el proceso judicial.

Hay que tener presente que este delito recién se incluyó en la legislación peruana el 12 de setiembre del año 2018, tipificando el Art. 151A del Código Penal el delito de ciberacoso, cometiéndolo la persona que haciendo uso de cualquier tecnología de la información o de la comunicación, vigila, persigue, hostiga, asedia o busca establecer contacto o cercanía con una persona sin su consentimiento, de modo que pueda alterar el normal desarrollo de su vida cotidiana, será reprimido con pena privativa de la libertad no menor de uno ni mayor de cuatro años e inhabilitación según corresponda, pudiendo incrementarse hasta siete años de privación de la libertad cuando la víctima es menor de edad.

Por su parte el ciberacoso sexual Art. 176B del Código Penal, tipifica el delito de la manera siguiente: El que, haciendo uso de las TIC, vigila, persigue, hostiga, asedia o busca establecer contacto o cercanía con una persona, sin el consentimiento de esta, para llevar a cabo actos de connotación sexual, será reprimido con pena privativa de la libertad no menor de tres ni mayor de cinco años e inhabilitación", que en caso concurra con algunas circunstancias agravantes podrá alcanzar una pena de 08 años de privación de la libertad.

La reciente incorporación de esos delitos al ordenamiento jurídico peruano, y el tiempo que demora un proceso judicial, no permite aún tener una estadística de casos sentenciados por los delitos de ciberacoso o ciberacoso sexual, además de que no se tiene programas efectivos de protección a las víctimas; lo que permite ratificar que la solución ante esta problemática no se encuentra en la sanción

6 Mayor información se puede encontrar en https://gestion.pe/peru/acoso-virtual-en-peru-se-concentraria-en-facebook-whatsapp-e-instagram-segun-denuncias-noticia/?ref=-gesr

al agresor, sino en la prevención y asesoramiento a las víctimas potenciales, así como fortalecer los mecanismos para lograr que acabe la agresión.

Conclusiones

1. La lucha contra el ciberacoso con propósito sexual debe realizarse en primer lugar desde una vertiente preventiva, porque es fundamental que los menores, padres y profesores sean conscientes de los riesgos de internet y del ciberacoso en particular. Pero, desgraciadamente, siempre va a haber una persona acosada, por lo que es necesario que este tipo de conductas tengan un encaje adecuado en la legislación penal y que jueces, fiscales y policías puedan contar con los instrumentos necesarios para investigar este tipo de conductas criminales, para lo que es imprescindible una buena formación, mejorar la colaboración internacional y poder utilizar con todas las garantías la figura del agente encubierto a lo largo de una investigación a través de internet.

2. Respondiendo al planteamiento del problema y al objetivo, vemos que en un 75% de casos del ciberacoso sexual, este no es denunciado por temor, el riesgo de sentirse humillados, o simplemente por vergüenza de los agraviados, además de la poca efectividad y sanción benigna por la comisión de este delito, sumado a que no hay suficientes mecanismos o instrumentos para obtener y salvaguardar los indicios o pruebas que apunten hacia el ciberacosador, y este pueda ser denunciado y a la vez reconocido e identificado.

Referencias

De la Serna, J. M. (2017). *CiberAcoso.* https://books.google.es/books?hl=es&lr=&id=TruYDwAAQBAJ&oi=fnd&pg=PT2&dq=Ciberacoso&ots=cVBxnoK6hY&sig=R_Bw6zVPhtbGuymbOupg6wPMpFE#v=onepage&q=Ciberacoso&f=false. (Fecha de consulta 05 de diciembre de 2022)

González, S., Varela, R., Gálvez, A., Ortega, T., & Gallego, C. (2018). *La Violencia en la Realidad Digital. Presencia y difusión en las redes sociales.* Egregius ediciones: ISBN 978-84-17270-62-9. https://idus.us.es/bitstream/handle/11441/88127/978-84-17270-62-9.pdf?sequence=1&isAllowed=y (Fecha de consulta 01 de diciembre de 2022)

Hinduja, S., & Patchin, J. W. (2010). *Bullying Ciberbullying and Suicide.* Archives of Suicide Research. doi:10.1080/13811118.2010.494133. (Fecha de consulta 02 de diciembre de 2022)

Li, Q. (2005). *Cyberbullying in schools: Nature and extent of adolescents' experience.* Montreal, Canadá: paper present at the Annual Educational Research Association Conference. https://www.researchgate.net/publication/234725126_Cyberbullying_in_Schools_Nature_and_Extent_of_Canadian_Adolescents'_Experience (Fecha de consulta 04 de diciembre de 2022)

Lucas, B., Pérez, A., & Gimenez, M. (2016). La evaluación del cyberbullying situación actual y retos futuros. *Papeles del Psicólogo,*(37), 27-35. https://www.redalyc.org/articulo.oa?id=77844204004 (Fecha de consulta 06 de diciembre de 2022)

Monge, A. (2010). *De los abusos y agresiones sexuales a menores de trece años tras la reforma penal de 2010*. Revista de Derecho y Ciencias Penales N ° 15. https://idus.us.es/bitstream/handle/11441/64084/EL%20MENOR%20ANTE%20LOS%20ABUSOS%20Y%20AGRESIONES%20SEXUALES.PDF?sequence=1&isAllowed=y (Fecha de consulta 06 de diciembre de 2022)

Olaya-Martínez, A. (2020). Rutas contra el silencio: análisis de los mecanismos para el manejo y prevención del acoso sexual al interior de la Universidad de Antioquia (Colombia). *El Ágora U.S.B.*, 20(1), 142-156. https://doi.org/10.21500/16578031.4137 (Fecha de consulta 04 de diciembre de 2022)

Orozco, M. (2020). *Influencia de los hogares disfuncionales en el ciberacoso.* Colombia: Universidad Pedagógica y Tecnológica de Colombia. https://repositorio.uptc.edu.co/bitstream/handle/001/3207/Ciberacoso.pdf;jsessionid=-2F04439A26CA479D7BCAF33311D0D2A8?sequence=1 (Fecha de consulta 03 de diciembre de 2022)

Ortega, R. (2010). *treinta años de investigación y prevención del bullying y la violencia escolar.* Madrid: En: Agresividad Injustificada. Bullying y violencia escolar. Alianza Editorial. https://docplayer.es/13901584-Treinta-anos-de-investigacion-y-prevencion-de-bullying-y-la-violencia-escolar.html (Fecha de consulta 05 de diciembre de 2022)

Ortega, R., & Mora-Merchán, J. T. (2007). *Acting against school bullying and violence.* Landau, Germany: Verlag Empirische Pädagogik. https://iamnotscared.pixel-online.org/data/database/publications/618_Acting_against_school_bullying_and_violence.pdf (Fecha de consulta 02 de diciembre de 2022)

Ortega, R., Del Rey, R., & Sánchez, V. (2012). *Nuevas dimensiones de la convivencia escolar y juvenil. Ciberconducta y relaciones en la Red: Ciberconvivencia.* Madrid: Ministerio de Cultura, Educación y Deporte. https://sede.educacion.gob.es/publiventa/d/15394/19/0 (Fecha de consulta 01 de diciembre de 2022)

Panizo Galence, V. (2015). *El Ciber-Acoso con intención sexual y el child-grooming.* https://dialnet.unirioja.es/servlet/articulo?codigo=3795512 (Fecha de consulta 07 de diciembre de 2022)

Sánchez, L., Crespo, G., Aguilar, R., Bueno, F., Aleixandre Benavent, R., & Valderrama, J. (2016). *Los adolescentes y el ciberacoso.* Unitat de Prevenció Comunitaria de Conductes Adictives (UPCCA-Valencia) ISBN: 978-84-9089-038-7. http://hdl.handle.net/10261/163035 (Fecha de consulta 05 de diciembre de 2022)

Téllez, F. R. (2016). Prefijo CIBER: arqueología de su presencia en la sociedad del conocimiento. *Investigación y Desarrollo, 24*(1), 142-162. https://www.

redalyc.org/pdf/268/26846686007.pdf (Fecha de consulta 02 de diciembre de 2022)

Temperini, M. (2014). *Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado.* Presentado en el 14 Simposio Argentino de Informática y Derecho. http://sedici.unlp.edu.ar/handle/10915/42145 (Fecha de consulta 05 de diciembre de 2022)

INFORMÁTICA Y DERECHO

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO
(SEGUNDA ÉPOCA)

FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES
DE DERECHO E INFORMÁTICA

ISSN 2530-4496 – N.º 13, 2023, PP. 45-56

LA "META" ES UN UNI "VERSO" CON PERSPECTIVA DE GÉNERO

THE "META" IS A UNI "VERSE"
WITH A GENDER PERSPECTIVE

Paola Consuelo Ramos Martínez[1]

Claudia Bibiana Ruiz[2]

1 Doctoranda en Estudios de Género y Políticas de Igualdad de la Universidad de Salamanca, España. Docente de la Facultad de Derecho de la Universidad Santo Tomás Villavicencio, Colombia. paolaramosm@usantotomas.edu.co

2 Doctoranda en Ciencias Humanas y Sociales de la Universidad Nacional de Colombia en la línea brecha digital de género e interseccionalidad. Docente de la Universidad Santo Tomás Villavicencio, Colombia. claudiabruiz@usantotomas.edu.co

Resumen

El metaverso se ha convertido en un entorno prometedor que ha canalizado la ilusión de una realidad paralela a través de las nuevas tecnologías. No obstante, la reproducción de nuestras acciones en un mundo digital alterno repercute en la construcción de comportamientos que pueden continuar vulnerando el derecho de las mujeres a una vida libre de violencias basadas en género. Identificar los desafíos del metaverso en materia de la incorporación de una perspectiva de género es una tarea esencial para trabajar en la erradicación y prevención de situaciones que afecten al grupo poblacional femenino en todas sus aristas, así como para promover espacios seguros para todas, en donde se reconozcan las consecuencias de las acciones llevadas a cabo en entornos digitales como afectaciones directas al mundo real.

Palabras clave

metaverso, perspectiva de género, violencias basadas en género, mujeres.

Abstract

The metaverse has become a promising environment that has channeled the illusion of a parallel reality through new technologies. However, the reproduction of our actions in an alternate digital world has repercussions on the construction of behaviors that can continue to violate women's right to a life free of gender-based violence. Identifying the challenges of the metaverse in terms of incorporating a gender perspective is an essential task to work on the eradication and prevention of situations that affect the female population group in all its aspects, as well as to promote safe spaces for all, where the consequences of actions carried out in digital environments are recognized as direct effects on the real world.

Keywords

Metaverse, Gender Perspective, Gender-Based Violence, Women.

El metaverso: la metáfora del mundo real

El cyborg es un organismo cibernético,
un híbrido de máquina y carne,
una criatura de realidad social
y también de ficción

Donna Haraway

Hacia una conceptualización del Metaverso

El concepto de Metaverso deriva de la combinación del prefijo "meta" (que implica trascender) con la palabra "universo", la cual describe un entorno hipotético vinculado al mundo físico. El origen de la palabra "metaverso" se remonta

a su primer uso en una pieza de ficción especulativa llamada "Snow Crash", escrita por Neal Stephenson en 1992. En esta novela, el autor define el metaverso como "un entorno virtual masivo paralelo al mundo físico, en el que los usuarios interactúan a través de avatares digitales." (Joshua, 2017)

Desde este primer uso, el concepto de metaverso como un universo generado por computadora ha tenido múltiples definiciones con similitud en el factor paralelo de lo digital y lo real, no obstante, diversos autores/as lo han considerado bajo expresiones como: el metaverso como el fiel registro de vida, como un espacio colectivo en la virtualidad, como Internet encarnado/Internet espacial, así como un mundo espejo y hasta un omniverso: un lugar de simulación y colaboración.

No obstante, la definición establecida por Lee, L. H., Braud, T., Zhou, P., Wang, L., Xu, D., Lin, Z., ... & Hui, P. (2021, p.1) en donde el metaverso puede ser entendido como "un entorno virtual que combina lo físico y lo digital, facilitado por la convergencia entre Internet y las tecnologías Web, y la Realidad Extendida (XR)" es precisa al identificar los elementos esenciales que convergen para su construcción.

Los autores expresan que dicha dualidad realidad-virtualidad se ha venido integrando en varios grados: como realidad aumentada, realidad mixta y la realidad virtual. Un ejemplo de ello puede identificarse en "Snow Crash" cuando se proyecta la dualidad del mundo real y una copia del mismo en los entornos digitales.

Para (Álvarez & Carrasco, 2022) un metaverso "es en esencia un mundo virtual 3D, una infraestructura canalizada a través de una red inteligente que mediante un sistema de inteligencia artificial (IA) recapta y genera datos a tiempo real de cada usuario conectado." Desde un punto de vista jurídico, un metaverso es una infraestructura de red que cursa respecto de sus contenidos como una plataforma, con una estructura dominical centralizada y una relación usuario-proveedor.

Si bien el concepto de metaverso no es nuevo, puesto que desde hace tiempo existen buen número de ellos, principalmente en el sector de los videojuegos, el reciente auge de distintas tecnologías ha venido generando expectativas colectivas sobre las oportunidades de entretenimiento, desarrollo de negocios, forma de relacionarnos con otras personas, entre otras, que podrían ir más allá de las limitaciones del mundo real. Incluso, se provee que en su grado de desarrollo más alto el metaverso es una realidad alternativa a la natural que ofrece la posibilidad de sustituir la realidad natural por otra distinta, en palabras de (Álvarez & Carrasco, 2022) «la creación de sociedades- Estado virtuales bajo un ámbito privado basadas en un sistema económico criptográfico».

Características del Metaverso

Si bien no existe un único modelo de metaverso, es posible identificar en la multiplicidad, particularidades básicas que los componen, entre ellas:

- Funcionan continuamente con independencia de que haya o no gente conectada a ellos y simulan las leyes temporales del mundo real.

- Permiten el acceso mediante dispositivos de realidad virtual, que ofrecen más opciones de interacción entre las personas.
- Cada usuario/a tiene asociado/a un avatar, que es la representación gráfica de la identidad virtual del usuario.

De acuerdo con (Álvarez & Carrasco, 2022), lo que realmente marca la complejidad jurídica del metaverso es la estructura de la organización que les da soporte, diferenciándose entre los siguientes:

- Centralizados: en ellos una única empresa gestiona todos los aspectos del metaverso; es la propietaria de todos los datos generados por los usuarios y controla cualquier tipo de intercambio económico que se efectúe dentro de él. Este tipo engloba todas las plataformas de videojuegos que llevan operando desde hace años, tales como Roblox, Minecraft o Fortnite.
- Abiertos: son aquellos que, en lugar de haber una única empresa que controle centralizadamente todos los datos y operaciones, se descentralizan varias funciones mediante el uso de tecnología de cadena de bloques (*blockchain*). En ellos se destacan las siguientes características:
  - Disponen de un sistema de identidad digital que identifica unívocamente a cada usuario (sin necesidad de revelar su identidad en el mundo real) mediante un monedero digital (*wallet*) y un inventario de propiedades digitales asociado a ese monedero digital mediante *tokens* (vales) no fungibles (NFT).
  - Llevan aparejado un sistema de economía digital, generalmente soportado por su propio *token* o criptomoneda, que es utilizada para la compra y venta de bienes y servicios en el mundo virtual.
  - La gobernanza del mundo virtual se rige a través de una organización autónoma descentralizada mediante la cual los propios usuarios son los que de forma democrática actualizan las políticas que determinan el comportamiento y reglas del metaverso.

Acerca del Avatar

El concepto de avatar se ha asociado a la representación gráfica de la identidad virtual del/a usuario/usuaria. Podría interpretarse como una extensión de la identidad del individuo en un entorno digital. El avatar únicamente está presente en el metaverso cuando quien lo controla está conectado/a y, por tanto, desaparece en el momento en que se efectúa la desconexión.

El concepto de avatar intenta simular a la persona que representa, por tanto, la personalización del mismo se encuentra anclada a la idea de la creación de una apariencia que individualiza al sujeto digital. La libertad y un amplio abanico de opciones de selección que permitan construir esa particularidad o esencia misma de la persona, son indispensables para el desarrollo de la experiencia digital-real. El avance en ello ha conseguido que, mediante la lectura de una foto normal, se cree automáticamente una representación gráfica 3D similar al individuo de la imagen, pero como alternativa, se han facilitado las opciones

para que el/la usuario/a diseñe su propia representación ficticia mediante un programa diseñado para ello.

La forma en la que se lleva a cabo el control del avatar va a definir el grado de inmersión en dicha virtualidad. Para (Álvarez & Carrasco, 2022) el control del avatar se puede realizar desde diversos tipos de controladores básicos (como un teclado, un ratón o un mando) que permiten un control limitado, o bien mediante unas gafas de realidad virtual, que, gracias a un conjunto de cámaras y sensores integrados, posibilitan al avatar imitar todos los movimientos y gestos que el/a usuario/a realiza en el mundo real.

Etapas de desarrollo del Metaverso

El metaverso combina una dualidad en la que se representa lo real en un entorno digital, como una alternativa para el individuo de experimentar la vida (su vida) en la virtualidad metafórica. Esta dualidad comienza incluso desde la creación del "usuario" puesto que representa a través de avatares el ser físico del individuo, se lleva a cabo una duplicidad de la identidad o una extensión de la identidad, en donde igualmente trasciende nuestro concepto de persona como sujeto de derechos.

Para conseguir dicha dualidad, es necesario que el metaverso pueda superar tres etapas, las cuales definen Lee, L. H., Braud, T., Zhou, P., Wang, L., Xu, D., Lin, Z., ... & Hui, P. (2021, p.2) así: (I) gemelos digitales, (II) nativos digitales y, finalmente, (III) la coexistencia de la realidad física-virtual o la surrealidad.

Es posible establecerlo como se presenta a continuación:

Tabla 1. Etapas de desarrollo del Metaverso

Primera etapa	Segunda etapa	Tercera etapa
Gemelos Digitales	Nativos Digitales	Coexistencia realidad física - virtual
Objetivo: Copia digital de la realidad física. - Modelos y entidades digitales a gran escala y de alta fidelidad duplicados en entornos virtuales. - Reflejan las propiedades de sus contrapartes físicas, incluidos los movimientos del objeto, la temperatura e incluso la función. - La conexión entre los gemelos virtuales y físicos está vinculada por sus datos. Ejemplos: Diseño asistido por computadora para el diseño de productos y arquitecturas de edificios: planificación urbana inteligente, sistemas industriales asistidos por IA; operaciones de riesgo asistidas por robots.	Objetivo: Creación de contenido nativo - Creadores de contenido, a través de los avatares, se involucran en creaciones digitales dentro de los mundos digitales. - Las creaciones digitales pueden estar vinculadas a sus contrapartes físicas, o incluso solo existir en el mundo digital. - Los ecosistemas conectados son análogos a las normas y regulaciones existentes en la sociedad del mundo real, y respaldan la producción de bienes físicos y contenidos intangibles. - Se centra en el primer punto de contacto con los usuarios, como las técnicas de entrada y el sistema de autoría para la creación de contenido	Objetivo: un mundo virtual persistente y autosuficiente que coexiste e interactúa con el mundo físico con un alto nivel de independencia. - Los avatares que representan a usuarios humanos en el mundo físico pueden experimentar actividades heterogéneas en tiempo real caracterizadas por un número ilimitado de usuarios concurrentes en múltiples mundos virtuales. - El metaverso puede permitir la interoperabilidad entre plataformas que representan diferentes mundos virtuales, es decir, permitir a los usuarios crear contenidos y distribuirlos ampliamente a través de mundos virtuales.

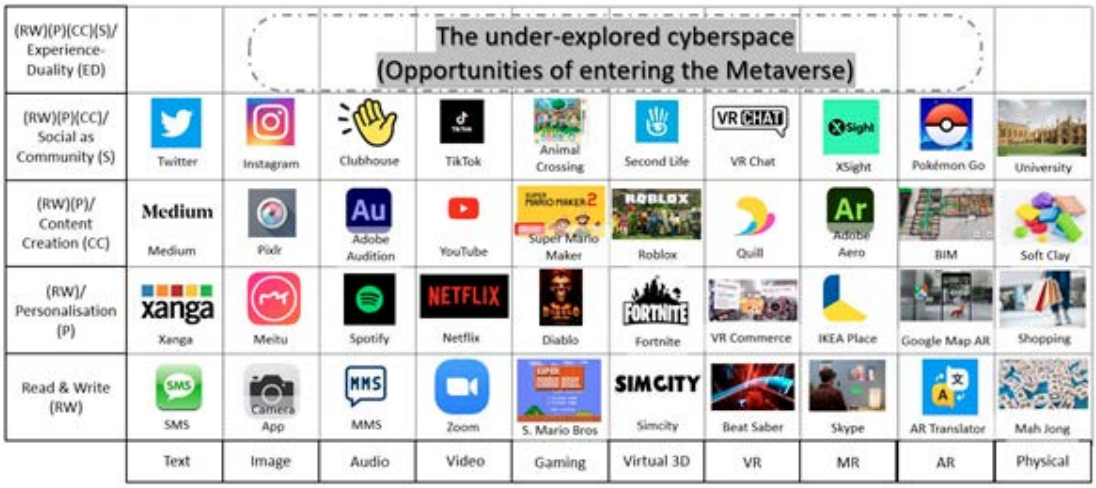
Fuente: elaboración propia.

Estas tres etapas de desarrollo tienen a los gemelos digitales como un punto de partida, puesto que es allí donde los entornos físicos se digitalizan y, por lo tanto, poseen la capacidad de reflejar cambios periódicamente en sus contrapartes virtuales. De acuerdo con el mundo físico, los gemelos digitales buscan crea - FIADI r copias digitales de los entornos físicos como "muchos" mundos virtuales, y los usuarios humanos con sus avatares trabajan en nuevas creaciones en dichos mundos virtuales, como nativos digitales. Es importante tener en cuenta que tales mundos virtuales sufrirán inicialmente una conectividad limitada entre sí y con el mundo físico. Finalmente, los mundos físico y virtual digitalizados eventualmente se fusionarán, representando la etapa final de la coexistencia de la realidad física-virtual similar a la surrealidad.

De acuerdo con los conceptos diversificados de universo(s) mediados por computadora mencionados anteriormente, se puede argumentar que ya estamos situados en el metaverso. Por ejemplo, el mapa 3D de la Tierra ofrece marcos de imágenes del mundo real, pero carece de otras propiedades físicas además de la información del GPS, mientras que las redes sociales permiten a los usuarios crear contenidos, pero se limitan a textos, fotos y videos con opciones limitadas de participación de los usuarios. Por otro lado, los videojuegos son cada vez más realistas e impresionantes. Es posible experimentar a través de ellos gráficos sobresalientes con física en el juego, por ejemplo, Call of Duty: Black Ops Cold War, que brinda una sensación de realismo que se asemeja al mundo real en gran detalle. Sin embargo, los videojuegos aún carecen de interoperabilidad entre ellos.

Actualmente, como lo indican Lee, L. H., Braud, T., Zhou, P., Wang, L., Xu, D., Lin, Z., ... & Hui, P. (2021, p.2), el panorama del ciberespacio puede construirse desde las aplicaciones que se utilizan en la vida real, donde existen relaciones de superación en la teoría de la riqueza de la información (de izquierda a derecha), así como en la dimensión de transitoriedad y permanencia (de abajo a arriba), así:

Figura 1. Panorama del ciberespacio de las aplicaciones de la vida real



Fuente: Lee, L. H., Braud, T., Zhou, P., Wang, L., Xu, D., Lin, Z., ... & Hui, P. (2021, p.2)

El metaverso ha experimentado cuatro transiciones desde juegos interactivos basados en texto, mundos abiertos virtuales, juegos masivos multijugador en línea (MMOG), entornos virtuales inmersivos en dispositivos portátiles y móviles inteligentes, hasta el estado actual del metaverso. Cada transición está impulsada por la aparición de nuevas tecnologías, como el nacimiento de Internet, los gráficos en 3D, el uso de Internet a gran escala y el hiperlibro. Claramente las tecnologías han servido como catalizadores para impulsar tales transiciones de los ciberespacios.

Las nuevas tecnologías podrían potencialmente desbloquear características adicionales del metaverso e impulsar los entornos virtuales hacia un universo virtual percibido.

Desafíos con perspectiva de género en el metaverso

El metaverso es un mundo virtual tridimensional, interactivo, inmersivo y colaborativo donde diferentes multitudes de personas pueden compartir y tener cada vez más interacciones en línea (Kim, 2021). No son pocos los autores que señalan su inherencia en la cotidianidad del mundo contemporáneo en donde la interacción exponencial y continua de mundos virtuales y físicos sostienen una delgada línea que los divide, y a su vez, les mezcla a tal punto que no se sabe dónde empieza uno y donde termina el otro (Hacker et al., 2020; Srivastava y Chandra, 2018; Zhang et al., 2020). En este sentido, los desafíos cotidianos del metaverso atraviesan todos los escenarios (la educación, la cultura, el trabajo, la política etc) en el mundo contemporáneo. Por ende, debería ser observado y analizado bajo la perspectiva de género, ya que, desde allí, es donde se pueden considerar a todas las personas y sus experiencias.

El Metaverso para las mujeres desde la academia hasta el trabajo

Las formas de aprender han cambiado de manera ostensible. Incluir actividades donde las Tecnologías de la Información y de la Comunicación (TIC) deban ser las protagonistas y estén alineadas junto con la motivación, emoción y contenidos educativos, parecen ser el mantra de los nuevos tiempos académicos en la mayoría de los niveles. Mientras la tecnología sigue avanzando y adhiriéndose a la piel de las clases, (sin importar su modalidad: híbrida, remota, presencial, en línea, por nombrar algunas), nuevos mundos inmersivos e imaginarios aparecen para crear nuevas oportunidades, pero también reproduciendo desigualdades y generando riesgos, que pueden ser observados tanto dentro como fuera del contexto del metaverso, es decir, en la realidad de la vida cotidiana de las personas.

A manera de oportunidad, entornos de creación de contenidos como Minecraft. Las tecnologías de realidad extendida (XR), y de realidad aumentada (AR), realidad virtual VR, han permitido explorar otras formas de conocimiento donde la curiosidad, imaginación y disciplina, guían el diseño de las experiencias educativas, impactando a usuarios de diferentes edades.

De este modo, la mayoría de los avatares de manera simultánea estudian, juegan, chatean y crean, mientras al mismo tiempo, otros avatares (personas), realizan de manera indiscriminada actos inapropiados, nocivos y lesivos. Sí antes del Metaverso se escuchaba con insistencia sobre el acoso, docentes de todas las áreas y niveles deben preguntarse ¿qué y cómo hacer para proteger a los estudiantes del abuso digital? mientras se sumergen en la interacción en primera persona por medio de avatares, incorporando y utilizando prácticas educativas en el metaverso.

A diario, millones de niñas, niños y jóvenes se conectan en diferentes juegos como Minecraft, Roblox, Fortnite, entre otros, con diferentes dispositivos de

realidad virtual, pero también muchos otros apenas tienen si acaso un computador, o un teléfono inteligente. Lo cual reproduce y fortalece la brecha digital tanto en su uso, como calidad e infraestructura. Así, en este nuevo universo, factores clave como la seguridad, el respeto, el diseño de hardware, el uso de los datos y la privacidad son asuntos no menores a revisar bajo el lente de la perspectiva de género.

Lo anterior, considerando que la propia naturaleza del Metaverso, según Di Pietro y Cresci (2021), desafía de manera incremental la privacidad personal, donde las identidades son fácilmente replicadas o inclusive invisibilizadas. Adicionalmente, según el libro blanco de Common Sense Media (2020), las dudas sobre el desarrollo de metaversos educativos siguen en incremento, ya que los peligros que conllevan pueden listarse en cinco momentos como sigue:

1. Peligros fisiológicos. Navegar por el metaverso a través de la realidad virtual puede inducir náuseas, fatiga visual y otras formas de "ciberenfermedad" entre las niñas, niños y jóvenes. Y los auriculares VR pueden cegar a los usuarios ante los obstáculos del mundo real. Dentro de estas ciberenfermedades, se encuentra por ejemplo el mareo cibernético o ciber náusea, (es decir, el mareo por movimiento asociado con la realidad virtual), que se vincula directamente al uso de visores de realidad virtual y donde las niñas y mujeres son más afectadas en comparación con los hombres, debido a la menor compatibilidad física que ellas tienen con los parámetros y dispositivos que se utilizan.

Así lo señalan, algunos autores como Parkman et al., 1996; Stanney et al., 2003; Klosterhalfen et al., 2005. Aunado a lo anterior, los factores individuales fisiológicos que pueden contribuir a diferencias de género tienen que ver con el ciclo hormonal femenino, niveles de susceptibilidad, etnicidad, aptitud aeróbica, índice de masa corporal, entre otras, las cuales son diferentes de los hombres y aún siguen sin ser consideradas en los entornos inmersivos y solo bajo algunas variables en las investigaciones.

2. Peligros de violación a privacidad. Debido al registro biométrico permanente y sensible, considerando que la recopilación de datos en línea inicia desde movimientos faciales y oculares, los cuales dan cuenta de un gran insumo de datos no verbales. Estos, pueden luego ser explotados con fines comerciales, dando acceso a las empresas de publicidad usar reacciones físicas involuntarias para rastrear y orientar sus deseos internos. Riesgos de privacidad,

3. Peligros de infoxicación y manipulación. El Metaverso facilita el acceso libre y abierto donde malos actores pueden persuadir, engañar y manipular. Hechos contemporáneos en aumento como los "deepfakes" y las realidades alteradas por la realidad aumentada dan cuenta de ello, sin poder discernir con claridad quién es el responsable.

4. Riesgos de contenido y abuso sexual. Ya que, en el metaverso para tener una experiencia inmersiva de cuerpo entero, los usuarios más jóvenes pueden encontrarse regularmente con clubes de striptease virtuales, preparación sexual, actos sexuales simulados y amenazas de violación. Este tipo de abusos en línea, tienen el potencial de ser aún más traumáticos. Estudios recientes como el de Oultaw (2022), han demostrado que muchos usuarios del Metaverso han

sufrido acoso sexual en las plataformas de realidad virtual, donde nuevamente las mujeres son más afectadas con una representación del 49%, en contraste con un 36 % de hombres para ser más específicos.

5. Riesgos psicológicos. Los cuales establecen su relación entre las tecnologías de realidad virtual que subyacen al metaverso y adicción, aumento de la agresión y disociación de la realidad.

Así mismo, al hablar de los desafíos del Metaverso en el trabajo, desde la perspectiva de género, queda en evidencia que no importa el contexto, la edad, la etnia, entre otras. El miedo al acoso representa un gran reto por superar, especialmente para las mujeres. Otros riesgos a considerar tienen que ver con la imagen propia y dismorfia corporal, ya que al igual que en diferentes videojuegos, en los que los personajes femeninos están hipersexualizados, los avatares de realidad virtual para mujeres podrían presentar problemas similares que generarían problemas de salud mental para las mujeres.

En esta misma línea, cabe recordar que el nacimiento de la realidad virtual proviene en gran medida de la industria de los videojuegos, la cual ha sido históricamente representada por hombres. Por ende, existe un gran riesgo de que estos legados se reproduzcan en el metaverso y lo conviertan en un espacio no inclusivo.

Así, la ausencia de mujeres en el diseño de hardware las deja físicamente incompatibles con los dispositivos creados por hombres para el Metaverso. Todo lo anterior sugiere que la protección de las niñas, niños y comunidad en general en el Metaverso, requieren de una fuerte implementación de medidas de seguridad.

Por eso y como ya lo han señalado diferentes entes gubernamentales como la ONU Mujeres (2019), el rápido desarrollo tecnológico y la innovación presentan nuevas oportunidades y nuevos desafíos. Sabiendo que la innovación y la tecnología no benefician automáticamente a todos por igual, los siguientes propósitos se hacen prioritarios:

- Crear conciencia de mercado, inversión y acciones en toda la industria para hacer crecer un mercado de innovación que promueva la igualdad de género y el empoderamiento de mujeres y niñas.
- Desarrollar herramientas y metodologías con socios de la industria para adoptar un enfoque de innovación sensible al género;
- Promoción de la mujer como innovadora y empresarial;
- Invertir en innovaciones y tecnologías que satisfagan las necesidades de las mujeres.

Adicionalmente, los problemas de desigualdad actuales, como la brecha de género, la brecha digital y la brecha digital de género se están extendiendo del mundo físico al mundo virtual. De este modo, en los contextos de trabajo del siglo XXI, problemas heredados de falta de inclusión, preocupaciones de seguridad y reproducción del patriarcado siguen a la orden del día. Los riesgos legales del Metaverso deben abordar estos asuntos y más.

Por todo lo anterior, y en línea con lo que propone Masia (2021), se deben encontrar soluciones de inclusión, a partir de cambios culturales como la inclusión de más mujeres tanto en la creación de hardware y software, como también de algoritmos. Porque, mientras abordemos la tecnología desde un determinado ángulo, seguiremos creando productos que parecen perfectos en la fase de pruebas, pero que una vez lanzados al mercado se convierten en promotores de la discriminación, puesto que

> El mismo hombre blanco adulto que desarrolla los algoritmos y prueba la eficacia de los prototipos en sí mismo, en sus propios ojos. El mismo hombre blanco adulto que decide que el producto está listo para ser lanzado al mercado, cuando no tiene más episodios de cybersickness en la fase de pruebas. (Masia, 2021)

Conclusiones

Las mismas características que hacen del Metaverso una gran oportunidad de transformación, participación, trabajo colaborativo y evolución para todas las personas en sus diversos escenarios cotidianos (trabajo, estudio, entretenimiento etc), son las mismas que le hacen potencialmente peligroso. La inmediatez, el anonimato, las otredades y sus reacciones en línea trascienden de lo humano en este entorno inmersivo apalancado principalmente por la realidad virtual y la realidad aumentada.

Realidades que pueden ser muy ajenas al entorno físico, teniendo consecuencias en ambos mundos sin separar al uno del otro, ya que las emociones, sensaciones y recuerdos prevalecen. Lo anterior, debido a que los gestos, reacciones, estados de ánimo y otros procesos biológicos podrían empezar a ser rastreados y clasificados, sin discriminar edades o género, para procurar una publicidad más invasiva que en últimas, juega una suerte de "control inconsciente mental". Está podría ser una "meta

Lo anterior debería ser no solo impensable sino imposible a la hora de alcanzar la "meta" de un uni-"verso" con perspectiva de género, donde se construya un mundo que verdaderamente represente a todas las personas, sin sesgos o limitaciones, o condiciones de consumo.

Por ende, la meta, debe considerar la generación permanente de espacios seguros, visibles, accesibles y participativos sin importar el espacio virtual o físico, la tecnología y sus bondades debería ayudar a asegurar y propiciar la satisfacción de necesidades, deseos y cierre de brechas sin restricciones ni condiciones.

Referencias

Di Pietro, R., and Cresci, S. (2021), "Metaverse: Security and Privacy Issues", The Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications, December 13-15, 2021.

Hacker, J., vom Brocke, .J., Handali, J., Otto, M., and Schneider, J. (2020), "Virtually in this together–how web-conferencing systems enabled a new

virtual togetherness during the COVID-19 crisis", European Journal of Information Systems, Vol. 29 No.5, pp.563-584.

Judy Joshua. Information Bodies: Computational Anxiety in Neal Stephenson's Snow Crash. *Interdisciplinary Literary Studies*, 19(1):17– 47, 2017. Publisher: Penn State University Press.

Kim, J. (2021), "Advertising in the Metaverse: Research Agenda", Journal of Interactive Advertising, Vol. 21 No. 3, pp. 141-144.

Klosterhalfen, S., Pan, F., Kellermann, S., and Enck, P. (2006). Gender and race as determinants of nausea induced by circular vection. Gend. Med. 3, 236–242. doi: 10.1016/S1550-8579(06)80211-1

Lederer, L. G., and Kidera, G. J. (1954). Passenger comfort in commercial air travel with reference to motion sickness. Int. Rec. Med. Gen. Pract. Clin. 167, 661–668

Lee, L. H., Braud, T., Zhou, P., Wang, L., Xu, D., Lin, Z., ... & Hui, P. (2021). All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda. *arXiv preprint arXiv:2110.05352*.

Masia, E. (2021). Cybersickness en las mujeres: el último síntoma del sesgo de género en la tecnología | Spindox. Retrieved 13 July 2022, from https://www.spindox.it/es/blog/cybersickness-en-las-mujeres-el-ultimo-sintoma-del-sesgo-de-genero-en-la-tecnologia/#gref

Parkman, H. P., Harris, A., Miller, M. A., and Fisher, R. S. (1996). Influence of age, gender, and menstrual cycle on the normal electrogastrogram. Am. J. Gastroenterol. 91, 127–133.

Stanney, K. M., Kingdon, K., Nahmens, I., and Kennedy, R. S. (2003). What to expect from immersive virtual environment exposure: Influences of gender, body mass index, and past experience. Hum. Factors 45, 504–522. doi: 10.1518/hfes.45.3.504.27254

Srivastava, S. C., and Chandra, S. (2018), "Social presence in virtual world collaboration: An uncertainty reduction perspective using a mixed methods approach", MIS Quarterly, Vol. 42 No.3, pp. 779-804.

Women, U. (2019). Innovation For Gender Equality. https://www.unwomen.org/sites/default/files/Headquarters/Attachments/Sections/Library/Publications/2019/Innovation-for-gender-equality-en.pdf

Zhang, Y. G., Dang, M. Y., and Chen, H. (2020), "An explorative study on the virtual world: Investigating the avatar gender and avatar age differences in their social interactions for help-seeking", Information Systems Frontiers, Vol. 22 No. 4, pp. 911-925.

INFORMÁTICA Y DERECHO

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO
(SEGUNDA ÉPOCA)

FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES
DE DERECHO E INFORMÁTICA

ISSN 2530-4496 – N.º 13, 2023, PP. 57-72

CIBERDELITOS Y CRIMINALIDAD INFORMÁTICA

Rol de la prevención en la expansión de la ciberdelincuencia

ROLE OF PREVENTION IN THE EXPANSION OF CYBERCRIME

Daniel Ernesto Peña Labrin[1]

1 Abogado & Sociólogo, Maestro en Derecho Penal por la Universidad Nacional Federico Villarreal. Segunda Especialidad en Derecho Informático (UIGV). Profesor de Derecho Penal y Derecho Informático; del Curso de Especialización en Derecho Informático y Programa de Especialización en Ciberseguridad de la Universidad Continental (Grado y Posgrado) – Huancayo/Lima- Perú; Miembro del Comité Científico Internacional del Instituto Iberoamericano de Criminología Aplicada IBERCRIMA-España; Miembro Honorario de la Sociedad Peruana de Criminología y Política Criminal y Vicepresidente de la Comisión de Estudio de Criminología y Ejecución Penal del Ilustre Colegio de Abogados de Lima (2022-2024). Email: dpena@continental.edu.pe

Resumen

Con el advenimiento de la disruptiva transformación digital post Covid-19 a nivel global, las nuevas tecnologías de información y comunicación gobiernan el mundo y con ello se han incrementado las vulnerabilidades de los sistemas informáticos por ciberdelincuentes, aprovechándose de las brechas de ciberseguridad y seguridad informática producidas, por el volumen, la velocidad y la sofisticación de las amenazas vigentes y se exige que éstas sean capaces de responder en tiempo real no solamente a nivel de personas y el Estado, sino también a nivel de las organizaciones y empresas, incidiendo en la maximización de la producción y la imagen empresarial, relacionado a la protección de datos personales e información privilegiada. La ciberdelincuencia, que ya ha destacado frente a la delincuencia tradicional en el mundo físico, posee sui generis fortalezas en el mercado delictivo para nivelar la oferta y la demanda criminógena, tiene sus propias barreras de entrada, su amplia y variada oferta de servicios y su especialización laboral, con roles profesionistas específicos. En tal sentido, urge mayor concientización de protección tecnológica y consecuentemente "evangelización" a los cibernautas en seguridad informática y ciberseguridad, reconociendo que el factor humano es la pieza del rompecabezas más fácil de atacar, de allí el fortalecimiento de la cultura de prevención a nivel de personas organizaciones y el propio Estado que debe cumplir el rol proactivo y proyectarnos a una cruzada global que consolide este esfuerzo en el control de la ciberdelincuencia.

Palabras clave

ciberdelincuencia, prevención, nuevas tecnologías de información y comunicación; criminología y derecho penal.

Abstract

With the advent of the disruptive post-Covid-19 digital transformation at a global level, new information and communication technologies rule the world and with this, the vulnerabilities of computer systems by cybercriminals have increased, taking advantage of cybersecurity and information security gaps. produced, due to the volume, speed and sophistication of current threats and it is required that these be capable of responding in real time not only at the level of individuals and the State, but also at the level of organizations and companies, influencing the maximization of production and business image, related to the protection of personal data and privileged information. Cybercrime, which has already stood out against traditional crime in the physical world, has sui generis strengths in the criminal market to balance criminogenic supply and demand, has its own entry barriers, its wide and varied offer of services and its labor specialization, with specific professional roles. In this sense, there is an urgent need for greater awareness of technological protection and consequently "evangelization" of netizens in information security and cybersecurity, recognizing that the human factor is the piece of the puzzle that is easiest to attack, hence the strengthening of the culture of prevention at the national level. of people, organizations and the State itself that must play a proactive role and project ourselves into a global crusade that consolidates this effort in the control of cybercrime.

Keywords

Cybercrime, Prevention, New Information and Communication Technologies, Criminology and Criminal Law.

Introducción

Los años 2020-2022 (pandemia y postpandemia), fueron sin duda años insólitos y aterradores en muchos aspectos. Las economías del planeta fueron arrasadas por el Covid-19, las personas, organizaciones, empresas y los entes gubernamentales tuvieron inexorablemente que digitalizarse a un ritmo extraordinario, lo que provocó un gran avance en los sectores económicos, sociales y culturales, sin embargo, trajo consigo un inminente caldo de cultivo para la ciberdelincuencia, forjándose en el ciberespacio un nuevo lugar para la actuación de distintos ataques a bienes jurídicos tan importantes como la privacidad, la fe pública, el patrimonio, la libertad sexual, los sistemas informáticos y la información contenida en soportes electromagnéticos[2]

Aunque la mayoría de estos comportamientos explica Ortiz, no son en esencia, algo nuevo en sí mismas, respecto a la extraordinaria particularidad del medio con el que se cometen, o sobre el que actúan, y otorgan a estas conductas una especial configuración que obliga a romper los esquemas clásicos para su incidencia en el circuito delictivo: tradicional y tecnológico. Ya sea por jactancia, por error o por ignorancia del modo de funcionamiento de los diversos dispositivos electrónicos que manipulamos cotidianamente, nos hemos convertido en la versión moderna de "Hansel y Gretel", y vamos dejando incesantemente migas de pan, en muy diversos formatos, de qué hemos hecho, dónde hemos estado y con quién hemos interactuado.[3]

Si bien, las nuevas tecnologías de la información y comunicación (NTIC), son aquellas que permiten la adquisición, almacenamiento, procesamiento, evaluación, transmisión, distribución y difusión de la información. Las NTIC sean desarrollado a través de la convergencia de la informática, las telecomunicaciones, la electrónica y la microelectrónica. Las NTIC constituyen un nuevo sistema tecnológico con un amplio terreno de aplicación, especialmente en campos en los cuales: se requiere procesar metadatos e integrar multiplicidad de actividades industriales y de servicios.[4]

2 RAYÓN BALLESTEROS M. y GÓMEZ, J., "Cibercrimen: Particularidades en su Investigación y Enjuiciamiento". *En Anuario Jurídico y Económico Escurialense, XLVIII, La Rioja*,2014. p.01 y "disponible en sitio web: https://dialnet.unirioja.es/servlet/articulo?codigo=4639646 (Fecha de consulta: 10 de enero de 2023)".

3 ORTIZ PRADILLO, J., "Geolocalización y Comunicaciones Electrónicas. Un salto cualitativo en la investigación criminal". *Ciberdelincuencia: Nuevas amenazas, nuevas respuestas. Actas del XVº Congreso Internacional Internet, Derecho y Política. Universitat Oberta de Catalunya*, Barcelona, 1-2 de julio de 2020, p.158 y "disponible en sitio web:https://es.scribd.com/document/578128087/Geolocalizacion-y-Comunicciones-Electronicas (Fecha de consulta: 11 de enero de 2023)".

4 SÁNCHEZ-TORRES, J., González Zabala, M. y M, Sánchez Muñoz, "La Sociedad de la Información: Génesis, Iniciativa, Concepto y su Relación con las TIC". IUS INNERAS: *Revista Electrónica de la Facultad de Ingenierías y Fisicomecánias*, Bogotá, 2012, p.121

El auge de la ciberdelincuencia está estrechamente ligada al desarrollo tecnológico informático, según la ONU (2019), las tecnologías de información y comunicación crearon oportunidades para los malhechores y dieron lugar al aumento de la tasa y la diversidad de los delitos cometidos en el mundo digital y a través de él. Si bien no se cuentan con cifras oficiales que reflejen las consecuencias de este delito, la OEA, estima que la ciberdelincuencia ocasiona costos de aproximadamente 575 millones de dólares al año, suma que llega a representar el 0.5 % del producto bruto interno mundial y considera que América Latina y el Caribe estos costos son de aproximadamente 90 millones de dólares anuales.[5]

De otro lado, añade Miro Linares, se suele utilizar como sinónimo de ciberespacio el concepto de "espacio virtual", como incompatible al espacio "real". La coincidencia, la unicidad de momentos, puede llevar a la impresión de que el ciberespacio es la ausencia de espacio, quizás fruto del equívoco de asimilar la idea de espacio a la de distancia real. Ciertamente, el ciberespacio es real en el sentido de que existe, pero se trata de una "especie nueva" de espacio, invisible cognoscitivamente y en el que las coordenadas espacio-tiempo adquieren otro significado y ven redefinidos su trayectoria y límites. El ciberespacio supone la contracción total del espacio (de las distancias) y, a la vez, la dilatación de las opciones en el ámbito de las telecomunicaciones en tiempo real. La red ha contraído el mundo fáctico acercando a un mismo lugar interactivo a personas que pueden estar en coordenadas espaciales separadas por miles de kilómetros y comunicarnos a una latencia de milisegundo, el espacio se contrae, la intercomunicación se expande.[6]

Así pues, la creación de internet implicó la aparición de nuevos paradigmas en materia de procesos de comunicación masiva y como consecuencia de tal hito, el derecho tuvo que readecuar sus instituciones a los fines de describir, predecir y regular las conductas sociales materializadas en los mencionados procesos, a través de herramientas que permitan reglamentar aquellas conductas que puedan resultar penalmente reprochables [7]. En palabras de Bauman y Chul Han,

y "disponible en sitio web: https://www.redalyc.org/pdf/5537/553756873001.pdf (Fecha de consulta: 12 de enero de 2023)".

5 INFORME DE ANÁLISIS: "Ciberdelincuencia en el Perú: Pautas para una investigación Fiscal Especializada". *Editado por el Ministerio Publico y la Oficina de Análisis Estratégico contra la Criminalidad*, Lima,2021, p.05 y "disponible en sitio web: https://cdn.www.gob.pe/uploads/document/file/1669400/CIBERDELINCUENCIA%20EN%20EL%20PERU%CC%81%20-%20PAUTAS%20PARA%20SU%20INVESTIGACIO%CC%81N%20FISCAL%20ESPECIALIZADA%20-%2015%20FEBRERO%202021.pdf (Fecha de consulta: 13 de enero de 2023)".

6 MIRO LINARES, F., "La Oportunidad Criminal en el Ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del Cibercrimen", *Revista Electrónica de Ciencia Penal y Criminología*, 2011, Granada, p.06 y "disponible en sitio web: https://dialnet.unirioja.es/servlet/articulo?codigo=4396388 (Fecha de consulta: 13 de enero de 2023)".

7 PARADA, R. Y ERRECABORDE J., (coords) "Cybercrimen y Delitos Informáticos": Los Nuevos Tipos Penales en la Era de Internet*, 1a ed. Ciudad Autónoma de Buenos Aires: Erreius*, 2018, p.03 y "disponible en sitio web: https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf (Fecha de consulta: 14 de enero de 2023)".

advierte Suerio: "Estamos ante un flamante "panóptico digital", a través de la vigilancia electrónica que pulula en el ciberespacio".[8]

Sobre esta base, se sustenta que los delincuentes online buscan explotar las debilidades de las tecnologías (libertad y de seguridad), la falta de concientización de los usuarios, así como el alcance global de internet y su rápida expansión, factores sin duda facilitan la comisión de viejos delitos o actos ilícitos con nuevas herramientas que nos trae la posmodernidad, aprovechando la situación para propagar ciberdelitos, obstaculizar las operaciones, cultivar dudas y ganar dinero ágilmente, estiman Parada y Errecaborde.[9]

Sin embargo, la persecución penal será eficaz si el Estado capacita a los operadores jurídicos sobre los aspectos dogmáticos y doctrinarios de estos nuevos tipos penales, garantizando el debido proceso y el equilibrio entre los intereses de la sociedad y la ley penal bajo el irrestricto respeto de los derechos humanos reconocidos y tutelados por la carta fundamental y leyes especiales, así como por diversas declaraciones y tratados universales de derechos humanos y sobre todo se genere conciencia informática en el tejido social , sobre los peligros y bondades del uso masivo del internet y su vinculación transversal con la protección de datos personales. Los ciberdelincuentes se encuentran siempre al acecho de nuevas formas con las que atacarnos a los usuarios aprovechándose de su desconocimiento y/o vulnerabilidades en nuestras defensas, sus objetivos son cuantiosos y pueden tener distintas consecuencias para los usuarios.[10]

Problemática criminógena

Como nos recuerda Posada Maya, a partir de finales de los años setenta de siglo XX, con el nacimiento de la ciberdelincuencia (daños informáticos, trasferencias no consentidas de activos, obstaculización de datos e infraestructuras informáticas, etc.), ha demostrado la existencia de una serie de factores dogmáticos y político criminales que obligan a repensar e incluso replantear varias de las nociones y categorías dogmáticas tradicionales.[11] Esta reformulación indica Morón, permitiría enfrentar lo que sin duda constituye un nuevo paradigma delictivo caracterizado por su virtualidad y por el empleo de medios tecnológicos avanzados en una sociedad modificada digitalmente. Son delitos que lesionan o ponen en peligro efectivo la confiabilidad (confidencialidad), la integridad y

8 SUERIO, C. "El Derecho Penal en la Era Digital", *AC Ediciones*, Lima,2018, p.209

9 PRANDINI, P. y MAGGIORE, M., "Ciberdelito en América Latina y el Caribe". Una Visión desde la Sociedad Civil. *Proyecto Amparo. Sección Estudios. Coordinación: Carlos Martínez, 2013*, México, p.20

10 INSTITUTO NACIONAL DE CIBERSEGURIDAD -INCIBE., (2020) "Guía de Ciberataques. Todo lo que debe debes saber a nivel Usuario". *Oficina de Seguridad del Internauta*. Madrid, p.03 y "disponible en sitio web: https://www.incibe.es/sala-prensa/notas-prensa/incibe-lanza-guia-ciberataques-usuarios-no-tecnicos (Fecha de consulta: 15 de enero de 2023)".

11 POSADA MAYA, R., "El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad físicas a una realidad virtual". *Revista Nuevo Foro Penal.Vol.13, N°88, enero-junio, Universidad EAFIT*, Medellín, 2017, p.72 y "disponible en sitio web: https://dialnet.unirioja.es/servlet/articulo?codigo=6074006 (Fecha de consulta: 16 de enero de 2023)".

la disponibilidad de los datos, los sistemas y las infraestructuras informáticas necesarias para el adecuado funcionamiento social.[12]

En tal sentido, la ciberdelincuencia, constituye una acción delictiva que perturba o vulnera una computadora, una red informática o un dispositivo en red. Mayormente el ciberdelito, lo perpetran cibercriminales o crackers por fines lucrativos. Sin embargo, la ciberdelincuencia lo realizan también personas y organizaciones. Algunos cibercriminales están organizados en empresas criminales, y utilizan avanzadas técnicas de ingeniería social y cuentan según sea el caso con básicas y especializadas destrezas informáticas.

A su vez, el "delito informático" en su acepción amplia, comprende situaciones en que el elemento informático se encuentra en el objeto de la conducta penada (verbigracia: acceso ilícito a bases de datos), y aquellas en que dicho elemento es el medio para realizar un fin ilícito. De esta manera, el concepto de ciberdelincuencia abarcaría, en sentido amplio, tanto delitos comunes que se ejecutan a través de medios informáticos, como nuevos delitos, cuya ejecución sólo es posible gracias a la existencia de dichos medios. Y dentro de este término genérico identifica Cavada, los delitos informáticos serían aquellas conductas delictuales en que se atacan bienes informáticos en sí mismos, no como medio, por ejemplo, dañar el Software mediante la intromisión de un virus y los delitos computacionales contrario sensu cuando la informática constituye un medio para cometer un fin, por ejemplo, la suplantación de identidad, el grooming, entre otros. En raras ocasiones, el ciberdelito tiene como objetivo dañar las computadoras por motivos distintos a la obtención de dinero. Estos pueden ser políticos o personales.[13]

Empero, el universo electrónico mueve anualmente billones de dólares. En suma, la ciberdelincuencia está entre las actividades ilícitas más rentables y que más ganancias de dinero agita en el planeta anualmente. Ya que habitualmente se perpetran ciberataques en diferentes partes del mundo generalmente a Bancos, grandes empresas, infraestructuras críticas y personas naturales, pagándose ingentes cantidades de dinero por Malware, suplantación de identidad, ransomware| y phishing, etc.

Tendencias delictógenas

Desde finales del siglo XX, con el surgimiento del internet que ha penetrado en la vida de todas las personas, empresas, organizaciones, etc., esto ha provocado la posibilidad de interconexión e intercambio de información entre todo tipo

12 MORÓN LERMA, E., "Nuevas tecnologías e instrumentos internacionales: Consecuencias Penales". *En Derecho Penal y nuevas tecnologías*, Bogotá, Universidad Sergio Arboleda, 2016, p.39

13 CAVADA HERRERA, J., "Cibercrimen y el Delito Informático: Definiciones en la Legislación Internacional, nacional y extranjera". *Editado: Biblioteca del Congreso Nacional de Chile/BCN. Asesoría Técnica Parlamentaría*, Santiago de Chile, 2020, p.01 y "disponible en sitio web: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/29012/2/Definicion_y_regulacion_de_cibercrimen_y_delito_informatico_JPC_edit.pdf (Fecha de consulta: 16 de enero de 2023)".

de personas a nivel global. En la actualidad con el acelerado incremento de las nuevas tecnologías de la información y comunicación, se ha generalizado el uso de éstas, mayormente por móviles educativos, económicos, sociales y culturales. En consecuencia, argumentan Prada y Vásquez, a través de distintos dispositivos y plataformas digitales se puede tener acceso a ese "cosmos digital" con el que se interactúa cotidianamente.[14]

Si bien descartar totalmente el peligro de ser víctima de la ciberdelincuencia, es algo improbable hoy en día. Sin embargo, existen comportamientos preventivos que nos pueden ayudar a coadyuvar el riesgo o evitar ser sujeto pasivo de la criminalidad informática. ¿Cuál es el talón de Aquiles?

Estudios de ciberseguridad y seguridad informática, arrojan que el factor humano incide preponderantemente en la victimación, el desconocimiento y falta de cultura de seguridad informática nos hace vulnerables. Podemos indicar situaciones recurrentes que vitalizan nuestra fragilidad ante la ciberdelincuencia la misma que se dedica a intentar burlar la ciberseguridad de los sistemas de diferentes organizaciones. Como vemos, la galaxia de internet en general ha supuesto un huracán de cambios disruptivos en el 2020- 2022 pero, lastimosamente, la ciberdelincuencia, también ha abierto puertas a la criminalidad cibernética, como fenómeno punible sin precedentes.

Por su parte, Hikal, Ramos y Pérez, sintetizan que el estudio del fenómeno de la ciberdelincuencia corresponde a la denominada parte especial de la ciencia criminológica, donde se ubican las llamadas "criminologías específicas", referido al estudio de una determinada sección de la realidad y su relación con la criminalidad, las tipologías delictivas, se trata de especializaciones por razón de la materia dentro del objeto de estudio de la criminología.[15]

El término cibercriminología o criminología informática es relativamente reciente y no está exento de cierta polémica doctrinal respecto al alcance de su significado, constituye el enfoque multidisciplinario que no proporciona comprender la naturaleza del delito en la red y nos orienta sobre cómo debemos mitigar el comportamiento de la ciberdelincuencia, son varios los autores que han tratado de definir esta especialización. Sin embargo, algunos de los temas particulares que atañen a nuestra ciencia se han venido desarrollando de manera lenta pero continua, conocidas como líneas de investigación, tanto a niveles

14 PRADA H. y VÁSQUEZ RÍOS, J., "Cibercrimen: Tendencias y Mecanismos de Protección". *Revista CIES. Volumen 7, N°1, Dirección de Investigaciones-Institución Universitaria Escolme*. Medellín, 2016, p.35 y "disponible en sitio web: https://docplayer.es/94188538-Cibercrimen-tendencias-y-mecanismos-de-proteccion.html (Fecha de consulta: 17 de enero de 2023)".

15 HIKAL CARREÓN, W., RAMOS EROSA R., Y PEREZ TOLENTINO J., "Nacimiento, sistematización y evolución de las criminologías especificas en México". *Revista Archivos de Criminología, Seguridad Privada y Criminalística. Año 6, Volumen XI, agosto-diciembre*,2018, p.01 y "disponible en sitio web: https://p.calameoassets.com/200425030643-c2ee2b08425b65d1a67d5ad771226796/p1.jpg (Fecha de consulta: 18 de enero de 2023)".

de tesis académicas de grado y posgrado, como en estudios de carácter especializado en América Latina.[16]

El término original se atribuye a Jaishankar, "padre fundador" de la cibercriminología, quien lo considera, con carácter general, un nuevo campo académico; una subdisciplina de la criminología, como una materia multidisciplinar que abarca diversos campos, tales como la criminología, la victimología, la sociología, la ciencia de internet y las ciencias de la computación. En sus publicaciones ha definido la cibercriminología como el estudio de la causa de los delitos que ocurren en el ciberespacio y su impacto en el espacio físico. [17]

En esencia, la cibercriminología implica el examen del comportamiento criminal y la victimización en el ciberespacio desde una perspectiva teórica y criminológica. Según Cámara, la elección del término y su utilización se debe dos razones: primero, el cuerpo de conocimiento que se ocupa de los delitos por computadoras, no debe confundirse con la investigación de los mismos y fusionarse con la ciencia forense cibernética en segundo lugar, debe haber una disciplina independiente para estudiar y explorar los delitos tecnológicos desde la perspectiva de las ciencias sociales.[18] Además, aclara Choi y Toro, la cibercriminología permite aplicar metodologías de estudio con el fin de identificar patrones, factores y causas de las desviaciones punibles y no punibles en el ciberespacio. De esta manera los académicos pueden hacer sugerencias de política y contrarrestar la inseguridad en el ciberespacio, indagando y buscar estudiar las causas, factores y escenarios que permiten la materialización de la ciberdelincuencia, destacando la problemática de la victimación digital: proposición conocida como la teoría de las actividades cotidianas en el ciberespacio o ciber TAC.[19]

En el plano iberoamericano Pérez, acuña el termino criminología cyborg. Una nueva criminología que entiende el profundo impacto que han supuesto las nuevas tecnologías en nuestro hábitat, trata de acercarse desde diversos vértices: antropológico, sociológico, psicológico, etc. La criminología cyborg, entiende el delito como inherente a la fusión/conversión cyborg y trata de ayudar (como un techno matrona desde las ciencias sociales) a comprender, prevenir y tratar aquellas cuestiones que afectan nuestra humanidad.[20]

16 GARCÍA LUNA J. y PEÑA LABRIN, D., "Cibercriminalidad y Posmodernidad". La Cibercriminología, como respuesta al escenario contemporáneo. *En Actualidad Penal, Editado Instituto Pacífico*, Lima,2017, p.349

17 JAISHANKAR, K., "Space Transition Theory of cyber crimes". *In Schmallager, F. & Pittaro, M. (Eds.), Crimes of the Internet*, 2008, p.01 y "disponible en sitio web: https://www.cybercrimejournal.com/pdf/Editoriaijccjuly.pdf (Fecha de consulta: 19 de enero de 2023)".

18 CÁMARA ARROYO, S., "Estudios Criminológicos Contemporáneos (IX): La Cibercriminología y el Perfil del Delincuente". *Revista Derecho y Cambio Social, N°60, abril-junio,2020*, p.472 y "disponible en sitio web: https://dialnet.unirioja.es/servlet/articulo?codigo=7524987 (Fecha de consulta: 20 de enero de 2023)".

19 CHOI, K.S y TORO-ÁLVAREZ, M., "Cibercriminología: Guía para la investigación del cibercrimen y mejores prácticas en seguridad digital". *Fondo Editorial UAN*, 2017, p.01, Bogotá y "disponible en sitio web: https://biblioteca.ucatolica.edu.co/cgi-bin/koha/opac-detail.pl?biblionumber=78948 (Fecha de consulta: 21 de enero de 2023)".

20 PÉREZ SUÁREZ, J., "We Are Cyborgs". *Grupo Editorial Criminología y Justicia*, Palma de Mallorca, 2017.

Sin embargo, en el estudio de la legislación supranacional, indica Vega y Arévalo, se ha podido observar que se viene legislando aceleradamente, con el propósito de combatir la ciberdelincuencia, verbigracia, en países europeos: Alemania, España, Francia, Portugal y Austria, han agregado en sus respectivos catálogos penales a estos delitos de nueva data y países como Inglaterra y Holanda han promulgado leyes especiales contra la ciberdelincuencia. Igualmente, los países americanos como Argentina, Colombia, Costa Rica, Chile y México han incluido en sus respetivos códigos penales a la delincuencia informática y países como Estados Unidos de América y Venezuela, han optado por crear leyes especiales para hacer frente al flagelo del siglo XXI: la ciberdelincuencia.[21]

Perspectivas de prevención

La prevención de la delincuencia y de la conducta antisocial es la finalidad de la criminología. En efecto, con la aceleración de la transformación digital sufrida por el Covid-19 y la migración estrepitosa y la dependencia de todos los sectores de la vida social a procesos dominados por la informática y la inteligencia artificial, han creado una esfera de vulnerabilidad de los sistemas informáticos e infraestructuras críticas, si bien es cierto la tecnología nos ha traído indiscutibles bondades no es menos cierto que las nuevas tecnologías de información y comunicación, nos han proporcionado nuevos riesgos y ocasiones para la realización de hechos ilícitos al ser un novísimo campo, existe desconocimiento de ciberseguridad lo que facilita un campo fértil de impunidad, poniendo en riesgo además nuestra seguridad y privacidad. Sin duda, reconocemos que no existe ningún campo de la dinámica del ser humano en el que la seguridad esté resguardada absolutamente, unido a los conflictos de investigación y juzgamiento respecto al anonimato, la ubicuidad y sus modus operandi son sin duda, el elemento criminógeno de mayor relevancia, es por ello que la prevención resulta clave en el morigeramiento de la ciberdelincuencia.

Por consiguiente, una de las características más relevantes del ciberespacio detalla Flores, consiste en su posibilidad de interactuación constante con el espacio real. En esta posibilidad de fenómeno social, estriba en buena medida la fuerza de las redes informáticas y de ella deriva, también, su potencialidad ofensiva sobre bienes jurídicos protegidos en el espacio real, pero vulnerables a ataques con modernas conductas procedentes de un espacio nuevo y con enorme proyección futura. Por lo cual, cabe afirmar que el ciberespacio ha generado la aparición de nuevas conductas delictivas vinculadas a las nuevas tecnologías de la comunicación y la información, al tiempo que ha aumentado considerablemente la vulnerabilidad de determinados bienes jurídicos, como la información en bases de datos y los relacionados con la intimidad, el honor, la propiedad, la autodeterminación informática, la libertad sexual, y la seguridad del mercado o del consumo entre otros. La complejidad de las nuevas tecnologías informáticas y la variedad de conductas y posibilidades de afectación de bienes jurídicos a

21 VEGA AGUILAR, J y AREVALO MINCHOLA, M., "Ciberdelitos. Análisis en el Sistema Penal, *Editorial IUSTITIA*, Lima 2022, p.495

través de las mismas dificultan enormemente la tarea de delimitar y de designar con precisión estas nuevas formas de delincuencia.[22]

No obstante, diferentes estudios, informes y artículos de los líderes del mercado, han extraído las cinco estrategias de seguridad y tecnología que son los protagonistas en el panorama de la ciberseguridad.[23]

Ciberseguridad en la educación: Recordemos que aproximadamente 1.5 mil millones de estudiantes de todos los niveles a nivel mundial, se vieron forzados a emprender clases de forma remota tras la pandemia. Los docentes tuvieron que familiarizarse de forma muy acelerada a algunas plataformas como Zoom o Google Classroom, entre otros; siendo el tema de mayor preocupación lo vinculado a la privacidad, sobre todo cuando el principal mercado es la población infantil, quienes pueden tener acceso no controlado a contenidos no aptos para su edad o, por otro lado, pueden acceder a sitios que pongan en riesgo el bienestar de su formación. Un inicial reto fue la capacitación de los profesores, para que, de forma responsable y segura, hagan uso de estas y otras plataformas custodiando la información y de sus propios datos personales de sus alumnos.

Ciberseguridad en la salud: Se proyectaron ciberataques para los desarrolladores de las vacunas, en un cuadro de espionaje industrial que secuestraron y paralizaron las operaciones de salud en hospitales y poniendo en riesgo la vida de los pacientes.

Al mismo tiempo, la vulneración de información con datos personales y datos sensibles de pacientes, que se encontraban en la nube, aumentaron los ataques de phishing utilizando el anzuelo basado en información sanitaria. El elemento "ciber psicológico" y humano fue clave para el éxito de los ataques de suplantación de identidad, y su incremento se dedujo en un alto riesgo.

Ciberseguridad en lo industrial: Esta modalidad de ciberataques, a menudo suelen ser al azar, es decir, el aprendizaje que los cibercriminales desarrollan al atacar redes específicas y más localizadas, con móviles crematísticos, donde la preocupación principal es la falta de soporte y actualización para los sistemas Windows 7 y Windows Server ICS, así como la filtración del código de Windows XP que son ya obsoletos y habituales. Esto, combinado con la falta de inversión en seguridad de TI y la reducción en el personal, puede ser detonante para la explosión de innumerables vulnerabilidades que afectaron el desarrollo durante los últimos años.

Ciberseguridad en el trabajo a distancia: El trabajo remoto sin duda llegó para quedarse. Y, en consecuencia, hoy se entiende que la seguridad siga a los datos. En relación a los proveedores de servicios, convendrán en suministrar seguridad y protección de datos en la trazabilidad de sus operaciones.

22 FLORES PRADA, I., "Prevención y solución de conflictos internacionales de jurisdicción en materia de Ciberdelincuencia". *Revista Electrónica de Ciencia Penal y Criminología, 2015*, núm. 17-21,2015, p.05 y "disponible en sitio web: https://dialnet.unirioja.es/servlet/articulo?codigo=5354905 (Fecha de consulta: 21 de enero de 2023)".

23 INFOSECURITI-México, "Tendencias en Ciberseguridad", 06 y 07 octubre 2021 y "disponible en el sitio web: https://www.infosecuritymexico.com/es/blog/tendencias-de-ciberseguridad-2021.html (Fecha de consulta: 22 de enero de 2023)".

Destacando que las soluciones de autenticación remota se han desarrollado y seguirán aumentando aceleradamente, puesto que es necesario saber en todo momento quién y cuándo ha accedido a la información de la empresa, y en las organizaciones, así como trabajar en la "nube" por sus incalculables fortalezas, verbigracia: el trabajo colaborativo, motivo por el cual, las entidades de seguridad informática, orientan sus energías en escrutar soluciones, calculadas en proteger la transferencia y almacenamiento de información, unida con el posicionamiento de la importancia de la privacidad de los datos.

Ciberseguridad financiera: Si comparamos las amenazas del 2020 y su recurrencia en 2021-2022, destacamos: la crisis económica encauzada por la pandemia Covid-19, en la que se pronosticaron fuertes rezagos e incluso el colapso de algunas economías, generando una oleada de ciberdelitos; el aumento en la combinación de ataques DDoS y Ransomware, el primero para distraer a los equipos de TI de la presencia de un malware en su sistema, cuya finalidad es encriptar o robar información y posteriormente extorsionar a sus víctimas.

Sin duda, los problemas de seguridad de la red seguirán aumentando, a medida que aumenta la conectividad, la movilidad y el uso de "cloud". Dicha problemática ha afectado a grandes empresas y organizaciones y son una clara evidencia de que las reglas están cambiando. Dados los recortes de presupuesto en sinnúmero de instituciones y dada la falta de personal idóneo en ciberseguridad, es crítico implementar un plan de respuesta a incidentes que permita prevenir cualquier brecha o vulnerabilidad posible. Las políticas de ciberseguridad son fundamentales para salvaguardar los derechos de los ciudadanos en el ámbito digital, tales como la privacidad, la propiedad, así como aumentar la confianza de los ciudadanos en las tecnologías digitales y que estos puedan sentirse cómodos accediendo a las mismas.[24]

En suma, la prevención es el primer paso para la planeación exitosa, peor que ser víctima de un ciberataque es ser víctima y saber que se podrían haber tomado medidas para prevenirlo o para contener el daño. En cuanto a los recursos normativos, Perú está suscrito desde el año 2019 al convenio de Budapest-Hungría, del 23 de noviembre del 2001 y aprobado a través de Resolución Legislativa N°30913 del 12/02/2019 y ratificado por Decreto Supremo N°010-2019-RE, del 09/03/2019 y vigente a partir del 01/12/2019. Respectivamente[25]

Si bien cierto el resto de los países de la región no se adhirieron inicialmente al tratado internacional, hoy lo han suscrito ya 68 países (2023). Sin embargo, el no ser parte éstos del Consejo de Europa, nada frenó que en la región:

24 CIBERSEGURIDAD., "Riesgos, avances y el camino a seguir en América Latina y el Caribe". *Reporte de Ciberseguridad BID-OEA*,2020, p.10 y "disponible en sitio web: https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe (Fecha de consulta: 23 de enero de 2023)".

25 CONSEJO NACIONAL DE POLÍTICA CRIMINAL., "Diagnóstico Situacional Multisectorial sobre la Ciberdelincuencia en el Perú". *Ministerio de Justicia y DD. HH y el Observatorio Nacional de Política Criminal*, 2020, p.27 y "disponible en sitio web: https://cdn.www.gob.pe/uploads/document/file/1616607/Diagn%C3%B3stico%20Situacional%20Multisectorial%20sobre%20la%20Ciberdelincuencia%20%20en%20el%20Per%C3%BA.pdf (Fecha de consulta: 24 de enero de 2023)".

Argentina, Chile, Costa Rica, Paraguay, República dominicana, Colombia, Panamá y Perú, hayan ratificado el Convenio de Budapest. El cual indica las directrices que deben seguir los países miembros para incorporar a su legislación los recursos normativos necesarios para combatir la ciberdelincuencia. Además de ello, tenemos la Ley N°30096 (2013); modificada por la Ley N.°30171 (2014) y Ley N°30838 (2018); también se cuenta con una serie de normas legales, tales como la Ley N°30999 Ley de Ciberdefensa y el, Equipo de respuesta ante Incidentes de Seguridad Digital del Perú (PECERT: RM N.°360-2009) y a través del D.U.N°007-2020 (artículo 7); el Centro Nacional de Seguridad Digital incorpora al Equipo de Respuesta ante Incidentes de Seguridad Digital Nacional, con la responsabilidades de gestionar la respuesta y/o recuperación ante incidentes de seguridad digital en el ámbito nacional; y de coordinar y articular acciones con otros equipos de similar naturaleza nacionales e internacionales para atender los incidentes de seguridad digital); N°29733 Ley de Protección de Datos Personales y su Reglamento D.S.003-2013(modificado por el D.Leg N°1353 y fe de erratas:D.S.N°019-2017); Resolución N°504-2021: Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, esta última entró en vigor el 01 de julio del 2021 y la Estrategia nacional de inteligencia artificial (documento de trabajo para la participación de la ciudadana:2021-2026),elaborado por la Secretaría de gobierno y transformación digital de la Presidencia del Consejo de Ministros-Perú.

Conclusiones

Con el advenimiento de la disruptiva transformación digital post Covid 19, a nivel global las nuevas tecnologías de información y comunicación gobierna el mundo y con ello igualmente se han incrementado las vulnerabilidades de sistemas electrónicos por la ciberdelincuencia, aprovechándose de las brechas de ciberseguridad producidas; el volumen, la velocidad y la sofisticación de las amenazas vigentes exigiendo ser capaces de responder en tiempo real no solamente a nivel de personas y el Estado, sino también a nivel de las organizaciones y empresas, incidiendo en la maximización de la producción y la imagen empresarial, relacionado a la protección de información privilegiada. La ciberdelincuencia, que ya ha destacado frente a la delincuencia no convencional en el mundo físico, posee sui generis fortalezas en el mercado para nivelar la oferta y la demanda delictiva, tiene sus propias barreras de entrada, su amplia y variada oferta de servicios y su especialización laboral, con roles profesionistas específicos. Sin embargo, otra situación que está cambiando, fruto de esta industrialización de la ciberdelincuencia, están relacionados a la exploración de acciones delictivas que impliquen bajo riesgo, máximo beneficio y gran escala.

Es incuestionable que el proceso de transformación digital, ha cambiado nuestra cotidianidad en todos los aspectos de la vida humana; reduciendo trayectos y agilizando procesos. Por lo tanto, cada vez que se navega por internet o se interactúa por redes sociales se exponen datos personales y/o sensibles, que puede ser usada maliciosamente por personas con habilidades técnicas en seguridad informática, llamados “hackers” y/o “crackers”. Un ciberataque es una

sucesión de operaciones que se realizan contra los sistemas de informáticos, realizados con el fin de alterarlos, bloquearlos o destruirlos. Un cibercrimen puede ir dirigido a sistemas de información como bases de datos, archivos etc., o contra redes, servicios o sistemas operativos.

En este panorama, hoy en día las instituciones, gobiernos, empresas y personas están conectados en el ciberespacio, y a través de la web, comparten información inapreciable, estadísticas y otros datos. En consecuencia, los delincuentes online, buscan traspasar las estructuras digitales para su propio beneficio, constituyendo un fenómeno que se conoce actualmente como «ciberdelincuencia».

En consecuencia, urge mayor concientización de protección digital e inexorablemente "evangelización a los cibernautas en ciberseguridad", reconociendo que el factor humano es la pieza del rompecabezas más fácil de atacar, de allí la sensibilización y el fortalecimiento de la prevención a nivel de personas, organizaciones y el propio Estado que debe cumplir el rol preventivo y una cruzada igualmente global que consolide este esfuerzo en el control de la criminalidad informática que no se ralentiza sino que se sofistica al azotar el planeta, y hoy con la fortaleza digital de la inteligencia artificial en la dinámica de los delitos en la red. A todo ello se une los grandes recursos económicos de los que disponen para perpetrarlos en la década del veinte y se basaran sin duda alguna en la: Cloud security (seguridad en la nube); zero trust (confianza cero) y passwordless (seguridad sin contraseñas); inteligencia artificial y automatización; cifrado avanzado e integridad de los datos; blockchain; big data; evolución de la ingeniería social; valorización de la privacidad de datos y nuevas regulaciones nacionales y globales: Edge computing & IoT (internet de las cosas); nuevos ataques de ransomware; la socialización de la seguridad informática y ciberseguridad como servicio.

Finalmente, la ciberdelincuencia se dilata al compás que lo hace el uso masivo de las nuevas tecnologías de información y comunicación (NTICs) y el desplazamiento de diversas relaciones sociales y económicas al internet. Ante esta nueva realidad criminógena, es indiscutible el desafío que poseen las instituciones y las organizaciones, e igualmente las personas, para prevenir los ataques delictivos a los bienes jurídicos tutelados por la ley, que están en riesgo, y la necesidad que las acciones preventivas estén fundadas en un conocimiento basado en los resultados de la investigación empírica, requisito indispensable para poder mitigarlos.

Referencias

Cámara Arroyo, S. (2020). Estudios Criminológicos Contemporáneos (IX): La Cibercriminología y el Perfil del Delincuente. *Revista Derecho y Cambio Social, N°60, abril-junio*,2020, p.472. https://dialnet.unirioja.es/servlet/articulo?codigo=7524987

Cavada Herrera, J. (2020). Cibercrimen y el Delito Informático: Definiciones en la Legislación Internacional, nacional y extranjera. *Editado: Biblioteca del Congreso Nacional de Chile/BCN. Asesoría Técnica Parlamentaría*, Santiago de Chile, 2020, p.01 https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/29012/2/

Definicion_y_regulacion_de_cibercrimen_y_delito_informatico_JPC_edit.pdf

Choi, K. S. Y Toro-Álvarez, M. (2017). Cibercriminología: Guía para la investigación del cibercrimen y mejores prácticas en seguridad digital. *Fondo Editorial UAN*, 2017, p.01, Bogotá. https://biblioteca.ucatolica.edu.co/cgi-bin/koha/opac-detail.pl?biblionumber=78948

Ciberseguridad. (2020). Riesgos, avances y el camino a seguir en América Latina y el Caribe. *Reporte de Ciberseguridad BID-OEA*,2020, p.10. https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

Consejo Nacional de Política Criminal (2020). Diagnóstico Situacional Multisectorial sobre la Ciberdelincuencia en el Perú. *Ministerio de Justicia y DD. HH y el Observatorio Nacional de Política Criminal*, 2020, p.27. https://cdn.www.gob.pe/uploads/document/file/1616607/Diagn%C3%B3stico%20Situacional%20Multisectorial%20sobre%20la%20Ciberdelincuencia%20%20en%20el%20Per%C3%BA.pdf

Flores Prada, I. (2015). Prevención y solución de conflictos internacionales de jurisdicción en materia de Ciberdelincuencia. *Revista Electrónica de Ciencia Penal y Criminología*, 2015, núm. 17-21,2015, p.05. https://dialnet.unirioja.es/servlet/articulo?codigo=5354905

García Luna J. y Peña Labrin, D. (2017). Cibercriminalidad y Posmodernidad. La Cibercriminología, como respuesta al escenario contemporáneo. *En Actualidad Penal*, *Editado Instituto Pacífico*, Lima.

Hikal Carreón, W., Ramos Erosa R., y Pérez Tolentino J. (2018). Nacimiento, sistematización y evolución de las criminologías especificas en México. *Revista Archivos de Criminología, Seguridad Privada y Criminalística. Año 6, Volumen XI, agosto-diciembre*,2018, p.01. https://p.calameoassets.com/200425030643-c2ee2b08425b65d1a67d5ad771226796/p1.jpg

Informe de análisis (2021). Ciberdelincuencia en el Perú: Pautas para una investigación Fiscal Especializada. *Editado por el Ministerio Publico y la Oficina de Análisis Estratégico contra la Criminalidad*, Lima,2021, p.05. https://cdn.www.gob.pe/uploads/document/file/1669400/CIBERDELINCUENCIA%20EN%20EL%20PERU%CC%81%20-%20PAUTAS%20PARA%20SU%20INVESTIGACIO%CC%81N%20FISCAL%20ESPECIALIZADA%20-%2015%20FEBRERO%202021.pdf

Infosecuriti-México (2021). Tendencias en Ciberseguridad, 06 y 07 octubre 2021 y "disponible en el sitio web: https://www.infosecuritymexico.com/es/blog/tendencias-de-ciberseguridad-2021.html

Instituto Nacional de Ciberseguridad -Incibe. (2020). Guía de Ciberataques. Todo lo que debe debes saber a nivel Usuario. *Oficina de Seguridad del Internauta*. Madrid, p.03. https://www.incibe.es/sala-prensa/notas-prensa/incibe-lanza-guia-ciberataques-usuarios-no-tecnicos

Jaishankar, K. (2008). Space Transition Theory of cyber crimes. *In Schmallager, F. & Pittaro, M. (Eds.), Crimes of the Internet*, 2008, p. 01. https://www.cybercrimejournal.com/pdf/Editoriaijccjuly.pdf

Miro Linares, F. (2011). La Oportunidad Criminal en el Ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del Cibercrime *Revista Electrónica de Ciencia Penal y Criminología*, 2011, Granada, p. 06. https://dialnet.unirioja.es/servlet/articulo?codigo=4396388

Morón Lerma, E. (2016). Nuevas tecnologías e instrumentos internacionales: Consecuencias Penales. *En Derecho Penal y nuevas tecnologías*, Bogotá, Universidad Sergio Arboleda.

Pérez Suárez, J. (2017). We Are Cyborgs. *Grupo Editorial Criminología y Justicia*, Palma de Mallorca.

Prada H. y Vásquez Ríos, J. (2016). Cibercrimen: Tendencias y Mecanismos de Protección. *Revista CIES. Volumen 7, N.°1, Dirección de Investigaciones-Institución Universitaria Escolme*. Medellín, 2016, p.35. https://docplayer.es/94188538-Cibercrimen-tendencias-y-mecanismos-de-proteccion.html

Prandini, P. y Maggiore, M. (2013). Ciberdelito en América Latina y el Caribe". *Una Visión desde la Sociedad Civil. Proyecto Amparo. Sección Estudios. Coordinación: Carlos Martínez*, México.

Posada Maya, R. (2017). El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad físicas a una realidad virtual. *Revista Nuevo Foro Penal. Vol.13, N°88, enero-junio, Universidad EAFIT*, Medellín, 2017, p.72. https://dialnet.unirioja.es/servlet/articulo?codigo=6074006

Ortiz Pradillo, J. (2020). Geolocalización y Comunicaciones Electrónicas. Un salto cualitativo en la investigación criminal. Ciberdelincuencia: Nuevas amenazas, nuevas respuestas. *Actas del XV Congreso Internacional Internet, Derecho y Política. Universitat Oberta de Catalunya*, Barcelona, 1-2 de julio de 2020, p.158. https://es.scribd.com/document/578128087/Geolocalizacion-y-Comunicciones-Electronicas

Rayón Ballesteros M. y Gómez, J. (2014). Cibercrimen: Particularidades en su Investigación y Enjuiciamiento. *En Anuario Jurídico y Económico Escurialense, XLVIII*, La Rioja, 2014. p. 01. https://dialnet.unirioja.es/servlet/articulo?codigo=4639646

Sánchez-torres, J., González Zabala, M. y Sánchez Muñoz, M. (2012). La Sociedad de la Información: Génesis, Iniciativa, Concepto y su Relación con las TIC. IUS INNERAS: *Revista Electrónica de la Facultad de Ingenierías y Fisicomecánias*, Bogotá, 2012, p.121 https://www.redalyc.org/pdf/5537/553756873001.pdf

Suerio, C. (2018). *El Derecho Penal en la Era Digital*, AC Ediciones, Lima.

Vega Aguilar, J y Arévalo Minchola, M. (2022). Ciberdelitos. Análisis en el Sistema Penal, *Editorial IUSTITIA*, Lima.

INFORMÁTICA Y DERECHO

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO
(SEGUNDA ÉPOCA)

FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES
DE DERECHO E INFORMÁTICA

ISSN 2530-4496 – N.º 13, 2023, PP. 73-84

LOS CIBERDELITOS Y LA CIBERSEGURIDAD: UNA CUESTIÓN DE GÉNERO

Claudia Bibiana Ruiz[1]

Rodrigo Cortés Borrero[2]

1 Decano de la Facultad de Derecho de la Universidad Santo Tomás, Sede Villavicencio, Colombia; Doctorando en Derecho Privado de la Universidad de Salamanca, Magíster en Derecho Contractual Público y Privado, Especialista en Derecho Administrativo y Abogado Universidad Santo Tomás.

2 Doctora (C) en Ciencias Humanas y Sociales de la Universidad Nacional de Colombia en la línea brecha digital de género e interseccionalidad. Magister en docencia e investigación Universitaria con enfoque TIC. Mentora Minciencias OEI Programa + mujer + Ciencia + Equidad y Miembro de las comunidades mujeres TIC y más mujeres en Apps de Alianza Inn Colombia y MinTic con el reto Ciberseguridad Hacker Girls. Formadora de formadores en el campo de Herramientas digitales para la Innovación educativa y transformación digital, ciberfeminismo.

Introducción

Los ciberdelitos son una amenaza cada vez más común en el mundo digital actual, y la ciberseguridad es un tema crucial para protegerse contra ellos. Estos delitos incluyen desde el ciberacoso y el ciberstalking hasta el robo de identidad y la piratería informática. La ciberseguridad es un tema crucial para protegerse contra estos delitos y mantener la seguridad en línea. Sin embargo, existen diferencias de género en cuanto a la exposición y vulnerabilidad a estos delitos. Las mujeres a menudo son más propensas a ser víctimas de ciberacoso y otros delitos en línea, mientras que los hombres tienden a ser más propensos a cometer delitos cibernéticos. Además, también existe una brecha de género en la industria de la ciberseguridad en sí, donde las mujeres a menudo están subrepresentadas.

Esto puede deberse a varios factores, incluyendo diferencias en la forma en que los hombres y las mujeres usan internet y en la forma en que son percibidos por otros en línea. Además, también existe una brecha de género en la industria de la ciberseguridad en sí, donde las mujeres a menudo están subrepresentadas. Esto puede contribuir a la desproporción en la exposición y vulnerabilidad a los ciberdelitos, ya que las mujeres pueden tener menos acceso a las herramientas y recursos necesarios para protegerse. Es importante abordar estas desigualdades de género en la ciberseguridad y los ciberdelitos. Esto puede incluir promover la igualdad de oportunidades en la industria de la ciberseguridad, proporcionar recursos y educación a las mujeres para protegerse contra los ciberdelitos y tomar medidas para prevenir y responder a estos delitos. Al hacerlo, podemos crear un entorno en línea más seguro y justo para todos.

En este artículo, se reflexiona en torno a cuatro momentos: En primer lugar a manera de génesis: los ciberdelitos y la ciberseguridad. En segundo lugar, ciberseguridad y ciberdefensa. En tercer lugar, se presentan algunos retos de la ciberseguridad en la era digital para las mujeres y por último algunas reflexiones en torno a la Ciberseguridad y Género: entre la Vulnerabilidad y la Oportunidad.

A manera de génesis: los ciberdelitos y la ciberseguridad

Los ciberdelitos son actividades ilegales que se llevan a cabo a través de internet o de otras redes informáticas. La ciberseguridad es el conjunto de medidas y técnicas que se utilizan para proteger a las personas, empresas y organizaciones de estos delitos. La historia de los ciberdelitos tiene sus orígenes en la década de 1940, cuando se desarrollaron las primeras redes informáticas. En ese momento, los ciberdelitos eran principalmente actividades realizadas por aficionados a la informática con el objetivo de demostrar su habilidad técnica. Sin embargo, a medida que la tecnología y la conectividad a internet se volvieron más comunes y accesibles, los ciberdelitos también se volvieron más sofisticados y peligrosos.

Para la década de los 50s, surge lo que se conoce como "phone phreaking", con el cual se buscaba secuestrar los protocolos que permitían realizar llamadas gratuitas y evitar los peajes debido a las largas distancias a recorrer. Fue solo hasta

finales de la década de los 80s cuando esta práctica finalmente se extinguió. Fue a mediados de la década de los 60s, que las computadoras eran enormes alojadas en cuartos seguros con control de temperatura. Sus costos elevados y su limitado acceso inclusive para los programadores, sugería una alta seguridad.

Sin embargo, las incursiones de piratería no se hicieron esperar, especialmente lideradas por estudiantes que buscaban mejorar los sistemas existentes haciéndolos funcionar más rápido y de manera más eficiente. Hasta ese momento, los ataques surgían por curiosidad y travesura más que por beneficios comerciales o geopolíticos. Inspirados por esta realidad, hacia el año 1967, IBM recurre a estudiantes en edad escolar a "explorar" su nueva computadora, y de esta manera desarrollar una mentalidad defensiva, que es esencial para lo programadores de hoy en día, dando origen a lo que se conoce como hacking ético[3].

Uno de los primeros ejemplos de ciberdelitos fue el "Creeper", el primer malware de la historia que fue creado en 1971 por el ingeniero informático Bob Thomas. El Creeper se replicaba a sí mismo a través de la red de ordenadores ARPAnet [4](la predecesora de internet) y mostraba el mensaje "I'm the creeper, catch me if you can!" (Soy el Creeper, ¡cápturenme si pueden!) en la pantalla de los ordenadores infectados. El Creeper fue eliminado por otro virus informático llamado "Reaper", creado por el mismo Bob Thomas para eliminar el Creeper.

Figura 1

Fuente: Core War https://corewar.co.uk/creeper.htm

3 Este es una persona (hacker ético o hacker blanco), no destruye la seguridad en los sistemas, evaluando e identificando la seguridad y vulnerabilidades en sistemas, redes o infraestructura de sistemas. Esto implica encontrar y explotar algunas vulnerabilidades para determinar cuándo hay acceso sin autorización u otras actividades maliciosas.

4 La ARPAnet (advanced research projects agency network) o Red de Agencias de Proyectos de Investigación Avanzada en español, era una red de computadoras construida en 1969 como un medio resistente para enviar datos militares y conectar principales grupos de investigación a través de los Estados Unidos. ARPAnet ejecutó NCP (network control protocol/protocolo de control de red) y subsequentemente la primera versión del protocolo de Internet o la suite TCP/IP, teniendo la ARPAnet una descatada parte en la naciente Internet. ARPAnet finalizó a comienzos de 1990. https://developer.mozilla.org/es/docs/Glossary/Arpanet

Así se da inicio a la ciberseguridad. Creeper podía moverse a través de la red de ARPAnet, dejando un rastro de *migas de pan* donde quiera que fuera. Así que Ray Tomlinson, el inventor del correo electrónico, escribió el programa Reaper, que perseguía y eliminaba a Creeper, lo que lo convirtió en el primer gusano informático.

A medida que la tecnología avanzó, las computadoras empiezan a reducir su tamaño, costo y accesibilidad, los ciberdelitos también se volvieron más sofisticados y comenzaron a tener un impacto real en la vida de las personas. El 19 de enero de 1986, se lanzó el primer virus informático con fines de lucro, por los hermanos Basit y Amjad Farooq Alvi, dos desarrolladores de software provenientes de Pakistán: "Brain". Este virus se distribuía a través de disquetes y se instalaba en los ordenadores infectados sin el conocimiento de los usuarios. Una vez instalado, el virus mostraba un mensaje solicitando un pago para eliminarlo.

Posteriormente, en la década de 1990, el mundo se conecta a Internet. Allí, surgieron nuevas formas de ciberdelitos, como el spamming (el envío masivo de correos electrónicos no solicitados), el phishing (el intento de obtener información confidencial a través de correos electrónicos falsos) y el malware (software dañino que se instala en los ordenadores sin el conocimiento de los usuarios). En la actualidad, los ciberdelitos son un problema global y son cada vez más sofisticados y peligrosos. Algunos ejemplos de ciberdelitos comunes incluyen:

Hacking: Es el acto de acceder ilegalmente a un sistema informático o a una cuenta de usuario sin autorización. Los hackers pueden utilizar técnicas sofisticadas para burlar la seguridad de los sistemas y obtener acceso a información confidencial o para realizar actividades ilegales.

Ataques de ransomware: Es un tipo de malware que cifra los archivos del usuario y solicita un rescate para desbloquearlos. Los ataques de ransomware son cada vez más comunes y pueden causar grandes daños a las empresas y organizaciones.

Robo de identidad: Es el acto de utilizar la información personal de otra persona (como su nombre, dirección o número de seguridad social) para obtener beneficios o realizar actividades ilegales en su nombre.

Phishing: Es el acto de enviar correos electrónicos falsos que parecen legítimos con el objetivo de obtener información confidencial de los usuarios (como contraseñas o datos bancarios).

Ya para la época del años 2000, con la proliferación de amenazas cibernéticas, el nacimiento de nuevos virus y organizaciones criminales en línea, el fortalecimiento de la ciberseguridad también tuvo que seguir incrementando. Actualmente el ransomware es una de las amenazas más comunes y requiere de acciones preventivas y correctivas con urgencia pues se prevé que siga aumentando.

En resumen, la historia de los ciberdelitos y la ciberseguridad es larga y complicada, y seguirá evolucionando junto con el desarrollo de la tecnología. Los ciberdelitos son un problema global que afecta a todos, desde las personas hasta empresas y organizaciones. Es importante estar siempre alerta y tomar medidas

adecuadas para protegerse de estos delitos, y una forma de protección es la educación a lo largo de la vida sobre estos asuntos.

Ciberseguridad y ciberdefensa

El advenimiento en las últimas cuatro décadas del desarrollo de las comunicaciones y de las tecnologías ha presentado un reto para las naciones, pues han surgido nuevas problemáticas en cuanto al uso de estas, representadas en amenazas desde la seguridad nacional hasta la economía del ciudadano de a pie. Este no es un fenómeno aislado de países sub- desarrollados, pues se han evidenciado vulneraciones a la seguridad nacional y a la economía en distintas latitudes del globo, que han forzado la creación y fortalecimiento de políticas públicas en materia de ciberseguridad y ciberdefensa por parte de los distintos gobiernos a nivel mundial.(Cortes ,2015).

La ciberseguridad y la ciberdefensa son dos conceptos clave en la era digital actual. Entendiendo por ciberseguridad como lo define (Kaspersk,2022) como la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil, y puede dividirse en algunas categorías comunes. Por otro lado, la ciberdefensa se refiere a las políticas y medidas implementadas por los gobiernos para proteger la soberanía nacional y la seguridad cibernética de un país.

Haciendo la diferenciación en que la ciberseguridad se dirige más hacia el sector de los particulares, alejándose de las nociones clásicas de ciberdefensa (relacionada con la soberanía nacional); se han implementando múltiples herramientas y estrategias que han fortalecido la seguridad de la información; no obstante en esa sensación de seguridad e hipervigilancia tecnológica, emerge la problemática de los límites y posibles sesgos que se construyen y se ocultan en la panacéa de hacer un mundo más seguro, pero que en últimas terminan germinando segregación, discriminación e inequidad. Por lo tanto, es prioritario que la ciberseguridad y la ciberdefensa sean permeadas por la inclusión y el género, ya que estos aspectos pueden tener un impacto significativo en la forma en que se abordan estos temas.

Para ello, el vertiginoso avance tecnológico, la conquista y reivindicación de los derechos de las Mujeres empieza a destacarse en el mundo contemporáneo, sabiendo articular la tecnología para su fortalecimiento y uso, llevando el mensaje de construcción de una sociedad paritaria en los escenarios como redes sociales, acceso a la información, particpaicón politica y ciberactivismo; no obstante, pareciese que el escenario digital en ocasiones se ha tornado en contra ambientando escenarios de violencia digital, ciberacoso, censura, sobre exposición, chantaje y extorsión. Siendo menester que la ciberseguridad debe ser permeada por la inclusión y el género, el cual será el desafío constante del avance tecnológico.

Retos de la ciberseguridad en la era digital para las mujeres

La ciberseguridad en la era digital presenta retos tanto para las mujeres como para el conjunto de la sociedad. El feminismo, representado por diferentes teorías de corte social dentro de un marco político, se define como la defensa de los derechos de las mujeres para conseguir la igualdad económica, social y en materia de derechos y política con respecto a los hombres. Hoy en día, este movimiento tiene más fuerza que nunca, debido a la tecnología, que facilita la incorporación de la mujer en todos los ámbitos de la sociedad. Sin embargo, el ciberespacio es un lugar oscuro para las mujeres, dado que pueden sufrir ciberdelitos, que van desde comentarios sexistas, misóginos, discriminatorios, abusivos, ofensivos y perjudiciales hacia mujeres y niñas a través de las Tecnologías de la Información y de la Comunicación – TIC, hasta la distribución de imágenes y videos sexualmente explícitos (Abissath, 2018), lo que crea un entorno hostil en línea. Dichos ciberdelitos deben ser enfrentados por medio de herramientas y estrategias de ciberseguridad. Estos escenarios se caracterizan por una mayor representación masculina, razón por la cual vale la pena preguntarse: ¿Tienen género los ciberdelitos? Especialmentge cuando algunos de los retos a los que se enfrentan las mujeres en el ciberespacio son:

1. Violencia digital: Las mujeres a menudo son víctimas de ciberviolencias, como: cybermobs o ciberturbas, creepshot, cyberflashing, discriminación por razón de género, dowblousing, doccing o doxing, grooming o ciberengaño pederasta, hackeo, packs, pornovenganza, sexting o sexteo, sextorsión, sluthhaming, troleo de género, upskirting.
2. Desigualdades de género: Las mujeres a menudo tienen menos acceso a la tecnología y a la formación en ciberseguridad, lo que limita su capacidad para protegerse y defenderse en línea.
3. Representación y visibilidad: Las mujeres a menudo son menos visibles y menos representadas en el sector de la ciberseguridad, lo que puede dificultar su participación y liderazgo en el campo.

Con relación al ciberespacio, es necesario reconocer ontológicamente el concepto espacio, que según Qvortrup (2002), tiene tres enfoques: primero, desde el positivismo, el cual declara que "la mente humana es una copia de la realidad y el espacio con sus propiedades existe en sí mismo" (Qvortrup, 2002, p. 12). En segundo lugar, dualista, tomando en cuenta lo siguiente:

> El espacio no es sólo lo que permiten átomos y movimiento, sino la existencia de la identidad y simultaneidad como tal. Y en tercer lugar, fenomenológico, pues se trata de una constitución de espacio que depende primariamente de nuestros atributos prácticos y cognitivos. (Qvortrup, 2002, p. 17)

Aunque estas discusiones no son definitivas, si queda en evidencia que "el ciberespacio va mucho más allá de ser un espacio de recolección y producción de datos, a un espacio de permanente comunicación e interacción social" (Wertheim, 1999, p. 232). Es justo en esa interacción y práctica de relacionamiento virtual donde las mujeres, al igual que en los espacios no digitales, están siendo más vulneradas.

En cuanto a los ciberdelitos, de acuerdo con la RAE (Real Academia Española) (2014) son "delitos que se cometen a través de internet" (párr. 1). Además, pueden producirse contra individuos o grupos de personas y los problemas que traen consigo son variados, como la difamación, la violación de la intimidad o el robo de datos, como el ciberacoso, el sexteo, etc. No obstante, es necesario resaltar que no todos los ciberdelitos son cometidos por hombres, unos pocos son cometidos por mujeres. La relación entre género y la ciberdelincuencia es un tema aún en exploración, de modo que es importante abordarla de una manera más holística, abarcando sus relaciones y representaciones sociales, los roles de cada quien en el ciberespacio a la hora de cometer el ciberdelito, los cuales podrían ayudar a responder si los ciberdelitos tienen género.

Lo anterior bajo el entendido de que las mujeres son hasta un 51 % más ciberacosadas que los hombres, en concordancia con los resultados del más reciente estudio de Microsoft (2020). Así también lo identificó Pantallas Amigas (2018), al manifestar que "más allá del ciberacoso sexual y otras formas de violencia sexual digital, la victimización de las mujeres online cobra especial relevancia impulsada por dos características" (párr. 2): la facilidad para hacer daño en línea, puesto que cualquier actuación en el ciberespacio puede quedar impune, en medio de innumerables dificultades para mantener la privacidad; y el control que puede ejercer el victimario a través del contacto permanente con la víctima, a través de los diferentes dispositivos y redes sociales como Facebook, Instagram, TikTok, Twitter, entre otras (Pantallas Amigas, 2018).

En este sentido, el ciberacoso implica, necesariamente, el uso de las TIC para perpetrar más de un incidente con la intención de hostigar, molestar, atacar, amenazar, asustar y/o abusar verbalmente, de manera reiterada, de las personas (Oficina de las Naciones Unidas contra la Droga y el Delito [UNODC], 2015). Esta forma de acoso puede ser especialmente perjudicial para las víctimas, pues, como se había dicho, permite al agresor permanecer en el anonimato y evitar ser descubierto.

Probablemente, todas las personas están familiarizadas con el término "acoso", el cual tiene una connotación negativa, e implica que alguien está sufriendo actos delictivos cometidos por extraños o por personas que se conocen entre sí. Por ejemplo, Torres et al. (2014) aseveraron:

> [Que] las mujeres jóvenes son más vulnerables al daño del ciberacoso por la desigualdad en la consideración y valoración social a la que se someten los comportamientos y las imágenes de las mujeres en la relación de pareja, por lo que su vivencia es muy traumática. Los estereotipos tradicionales que siguen existiendo en las relaciones sociales entre hombres y mujeres, con valores sexistas, se siguen proyectando en la violencia de género ejercida en el mundo de internet y las redes sociales. (p. 5)

Aunado a lo anterior, según una encuesta realizada por Amnistía Internacional (2017), más de 3500 mujeres encuestadas en España, Reino Unido, Estados Unidos, Suecia, Italia, Dinamarca y Polonia sufrieron algún tipo de abuso en línea, al menos una vez; por ejemplo, acoso cibernético. Adicionalmente, el 41 % de estas mujeres temieron por su seguridad personal debido a este tipo de acoso,

al haber recibido mensajes intimidatorios, imágenes, videos sexualmente explícitos y amenazas de violencia en redes sociales y otras plataformas en línea. En el contexto latinoamericano, el panorama no deja de ser impactante. Según la Organización de los Estados Americanos – OEA (2019) como se citó en Rodríguez (2022), "el 60% de niñas y adolescentes que tienen acceso a internet en todo el planeta, han sido víctimas de ciberacoso por lo menos una vez" (párr. 4). Asimismo, de acuerdo con un estudio de la Universidad de Valencia en España (2018) como se citó en Rodríguez (2022), Colombia tiene uno de los índices de ciberacoso más altos de la región, situación que se intensificó debido a la repentina llegada de la pandemia del COVID-19.

Bajo este escenario, las leyes de ciberacoso varían mucho de un país a otro, dado que algunas solo requieren que la víctima sienta miedo, intimidación o angustia emocional, para ser consideradas un delito, mientras que otras exigen que cualquier comunicación electrónica vaya acompañada de una amenaza física. Por ejemplo, como lo estableció la Biblioteca del Congreso Nacional de Chile (2018), en países como Corea del Sur, donde el ciberacoso es un grave problema, a tal punto de llegar a clasificar los suicidios que este ciberdelito ha causado como "asesinatos sociales", crearon la Ley de Desprecio Cibernético, con la cual se iniciaron casos criminales sin necesidad de una denuncia formal por parte de la víctima. En la India, existe la Ley de Información Tecnológica del año 2000, que busca respaldar a las víctimas que demuestran haber sufrido ofensas y daño a la moral, con lo cual se puede generar desde una multa hasta enviar al victimario a prisión por cinco años.

En esta misma línea, en Filipinas existe la Ley contra el Acoso Escolar, con la cual se establecieron las normas para proteger a las víctimas, mientras se creaba un marco legal que regulara el comportamiento de todas las edades en las plataformas en línea. De esa forma, se especifican seis tipos de actos ofensivos a realizar en el ciberespacio (Biblioteca del Congreso Nacional de Chile, 2018):

1. Enviar mensajes repetitivos con insultos
2. Difundir información denigrante sobre la víctima
3. Enviar fotos ofensivas de la víctima, sean alteradas o no, con o sin consentimiento, con la intención de humillar y avergonzar a la víctima
4. Intervenir el email o redes sociales con el fin de enviar, subir o distribuir material a otras personas
5. Compartir información de la víctima que revelen detalles de su vida personal
6. Envío repetido de mensajes que incluyan amenazas, daños o convocatorias de activismo para generar miedo e inseguridad en las víctimas. (Biblioteca del Congreso Nacional de Chile, 2018, párr. 18-23)

Para el caso de América Latina, por ejemplo, en Chile se publicó se publicó una reforma a la Ley General de Enseñanza que busca reglamentar y "prevenir toda forma de violencia física o psicológica, agresiones u hostigamientos" (Borghello, 2012, párr. 5). Para el caso Colombia, existe el Proyecto de Ley 201 de 2012 que define el ciberbullying como el "uso deliberado de tecnologías de

información (Internet, redes sociales virtuales, telefonía móvil y videojuegos online) para ejercer maltrato psicológico y continuado entre iguales" (Borghello, 2012, párr. 13).

Ciberseguridad y género: entre la vulnerabilidad y la oportunidad

Los constructos sociales del género en los entornos digitales siguen asociándose a los hombres y la masculinidad, al operar como una suerte de estructura social jerárquica. Esto a menudo, pero no siempre, significa que las actividades y los conceptos relacionados con la masculinidad –como la experiencia técnica–, se valoran sobre los asociados con la feminidad, tales como experiencia en políticas o igualdad y diversidad iniciativas. Igualmente, las vulnerabilidades que afectan a las mujeres en el ciberespacio también pueden ser descritas desde otras brechas, además de la de género. Por ejemplo, la brecha digital[5] que afecta a personas de diferentes edades y culturas, especialmente a las mujeres, con un 52 % de representación en el mundo. Esto acarrea la brecha digital de género[6], que pone nuevamente en desventaja la participación femenina en lo que se conoce como la Cuarta Revolución Industrial (4RI).

> Además, características como el género, la raza, la edad, la situación socioeconómica y la ubicación del hogar de residencia intersectan entre sí generando múltiples desventajas para las mujeres. Específicamente, aquellas con un bajo nivel educativo que viven en áreas rurales y que constituyen el grupo menos "conectado", lo que se destaca como un área importante para intervenir mediante políticas. Por lo tanto, abordar estas desigualdades es una oportunidad para mejorar el acceso de las mujeres rurales a este recurso y promover su empoderamiento económico y político. (Rotondi et al., 2020, p. 7)

En este sentido, las mujeres son doblemente vulneradas tanto por la manera en que se crean los ciberespacios, con una mayoritaria representación masculina, como por el uso que se les da. A medida que el mundo se va moviendo cada vez más en línea, los delitos contra las mujeres siguen aumentando; por lo tanto, la definición de ciberseguridad tiene implicaciones de género, de modo que el pilar de diseño de la ciberseguridad también debe incluir mujeres en cada una de sus fases, a fin de reducir sus vulnerabilidades en el ciberespacio. Como lo indicó Ruiz (2021), "esto está sucediendo en este preciso momento, de este modo que es obligatorio contar con nuevos enfoques y metodologías que empezaran a dar cuenta de una sociedad de la información incluyente, democrática y con justicia de género" (p. 31). De tal forma, también se fortalece el escenario de la

5 Según van Dijk (2017), la brecha digital se refería a la desigualdad entre aquellos que tenían o no tenían acceso físico a las TIC. Según Norris (2001), existen tres distintos tipos de brecha: la brecha social, que es la diferencia en el acceso a la información entre los pobres y ricos en cada país; la brecha global, que se refiere a la diferencia entre países desarrollados y en desarrollo en cuanto al uso de TIC; y la brecha democrática, que significa la diferencia entre quienes utilizan las TIC para movilizarse y participar en la esfera pública.

6 Este término hace alusión a las desigualdades existentes entre hombres y mujeres en cuanto al acceso y el uso de las nuevas tecnologías.

ciberseguridad con representación femenina en la investigación de sistemas de ciberdefensa con perspectiva de género.

Ahora bien, más allá del contexto específico de la ciberseguridad, en la automatización del diseño prevalece la omisión de género, la cual lleva a malinterpretar y consolidar datos, al discriminar o privilegiar prácticas que estereotipan la feminidad de maneras problemáticas. Estos aspectos de género tienen un impacto directo en la ciberseguridad, donde según Millar et al. (2021):

> El diseño y la experiencia del usuario hasta ahora refuerzan estereotipos de género como por ejemplo en la elección de la voz femenina para teléfonos y parlantes inteligentes. Así mismo, los prototipos de realidad virtual, que como muchas tecnologías, han omitido a las mujeres casi en su totalidad como sus usuarios previstos. Y por si fuera poco el diseño de dispositivos domésticos inteligentes no ha incluido adecuadamente violencia de género[7] en la fase de diseño de "modelado de amenazas", lo que significa que los dispositivos inteligentes supuestamente seguros aumentan los riesgos de género. (p. 18)

En ese orden de ideas, hay brechas de género en la investigación académica y la industria sobre tecnología, en cada una de sus etapas se producen nuevos sesgos. En consideración del auge que el campo de la ciberseguridad tiene en el mundo contemporáneo, su influencia y prestigio, depende de la participación de las mujeres como una cuestión de igualdad y equidad que se traduce en oportunidades de éxito, reconocimiento y potencial de ingresos para las mujeres.

Algunas de las oportunidades de la ciberseguridad en la era digital para las mujeres son:

1. Empoderamiento femenino: A través de la formación y el aprendizaje en ciberseguridad, las mujeres pueden adquirir habilidades y conocimientos que les permiten protegerse y defenderse en línea, y participar plenamente en la vida digital.
2. Participación y liderazgo: La ciberseguridad es un campo en constante evolución y necesita una amplia variedad de perspectivas y enfoques para abordar adecuadamente los desafíos actuales y futuros. Las mujeres pueden aportar una gran cantidad de valor y contribuir al desarrollo de soluciones innovadoras.

7 "Violencia que se dirige contra una mujer por ser mujer o que afecta a las mujeres de manera desproporcionada" (Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 1992), incluye daño físico, sexual y/o emocional (o psicológico) y se ha cometido tanto fuera de línea como en línea. Con respecto a la violencia de género en línea, Powell y Henry (2017) utilizan el término "violencia sexual facilitada por la tecnología para describir el uso de las tecnologías de la información y la comunicación (TIC), para facilitar o extender el daño sexual y de género a las víctimas, incluyendo agresión sexual facilitada por la tecnología;... abuso sexual basado en imágenes;... ciberacoso y acoso criminal;... acoso sexual en línea; y... acoso basado en el género y discurso de odio" (p. 205).

3. Inclusión y diversidad: La ciberseguridad es un campo en el que se valora y se necesita la inclusión y la diversidad. Al fomentar la participación y el liderazgo de las mujeres, se puede lograr una mayor inclusión y diversidad en el sector, lo que beneficiará tanto a las mujeres como a la sociedad en general.

Por lo anterior, para enfrentar y disminuir los ciberdelitos, más allá del género, se requieren políticas que promuevan la inclusión, la participación y la capacitación de mujeres en el escenario de las nuevas tecnologías, como la ciberseguridad para reducir el acoso y la discriminación. Asimismo, es imprescindible el fomento de la transformación organizacional y cultural, con el propósito de valorar un variedad de actividades y capacidades, incluidas las que suelen estar más asociadas con la feminidad. Así pues, generar espacios de participación en el desarrollo de una nueva cultura de respeto a los derechos de la mujer tanto en la vida real como en el ciberespacio.

Referencias

Abissath, M. K. (2018). *All Rights Matter, Women's Rights Online in Ghana Matter*. https://allafrica.com/stories/201802211035.html

Amnistía Internacional. (2017). *Amnistía revela alarmante impacto de los abusos contra las mujeres en Internet*. https://www.amnesty.org/es/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/

Biblioteca del Congreso Nacional de Chile. (2018). *Sepa cómo tres países del Asia controlan prácticas de cyberbullying*. https://www.bcn.cl/observatorio/asiapacifico/noticias/paises-asia-pacifico-controlan-cyberbullying

Borghello, C. F. (2012). *119 - Países con leyes de Ciberbullying - 16/12/2012*. https://www.segu-info.com.ar/articulos/119-paises-leyes-cyberbullying

Cortés Borrero, R., & Facultad de Derecho, Universidad de los Andes. (2015). Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia. *Revista de Derecho Comunicaciones y Nuevas Tecnologías*, *14*, 1–17. https://doi.org/10.15425/redecom.14.2015.06

Congreso de la República de Colombia. (2012). Proyecto de Ley 201 de 2012. [Por el cual se crea el Sistema Nacional de Convivencia Escolar y Formación para el Ejercicio de los Derechos Humanos, Sexuales y Reproductivos y la Prevención y Mitigación de la Violencia Escolar]. Bogotá, D. C., Colombia.

Congreso Nacional de Chile. (2011). Ley 20536 de 2011. [Sobre violencia escolar]. Santiago, Chile.

Henry, N., & Powell, A. (2017). *Sexual Violence in a Digital Age*. Palgrave Macmillan.

Kaspersky. *¿Qué es la ciberseguridad?* (2021, diciembre 1). latam.kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Microsoft. (2020). *Civility, Safety & Interaction Online*. Microsoft.

Millar, K., Shires, J., & Tropina, T. (2021). *Gender approaches to cybersecurity: design, defence and response.* United Nations Institute for Disarmament Research.

Norris, P. (2001). *Digital Divide, Civic Engagement, Information Poverty and the Internet Worldwide.* Cambridge University Press.

Oficina de las Naciones Unidas contra la Droga y el Delito [UNODC]. (2015). *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children* . Naciones Unidas.

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (1992). *Redomendación General.* Comité para la Eliminación de la Discriminación contra la Mujer.

Pantallas Amigas. (2018). *Ciberviolencia de género.* https://www.pantallasamigas.net/ciberviolencia-de-genero/

Qvortrup, L. (2002). Cyberspace as Representation of Space Experience: In defence of a Phenomenological Approach. In L. Qvortrup, *Virtual Space: Spatiality in Virtual Inhabited 3D Worlds* (pp. 5-24). Springer-Verlag London.

Real Academia Española [RAE]. (2014). *Definición de ciberdelito.* https://dle.rae.es/ciberdelito

Rodríguez, L. S. (2022). *Why are women more victims of cybercrime than men?* https://impactotic.co/en/Why-are-women-more-victims-of-cybercrime-than-men%3F/

Rotondi, V., Billari, F., Pesando, L. M., & Kashyap, R. (2020). *Desigualdad digital de género en América Latina y el Caribe.* Instituto Interamericano de Cooperación para la Agricultura (IICA) - Banco Interamericano de Desarrolllo (BID) - Universidad de Oxford - Fondo Internacional de Desarrollo Agrícola (FIDA).

Ruiz, C. B. (2021). Mujeres en la educación: desigualdades sociales más allá del género. *Análisis, 53*(98), 1-42. https://doi.org/10.15332/21459169.6237

Torres, C., Robles, J. M., & de Marco, S. (2014). *El ciberacoso como forma de ejercer la violencia de género en la juventud: un riesgo en la sociedad de la información y del conocimiento.* Ministerio de Sanidad, Servicios Sociales e Igualdad de España.

van Dijk, J. (2017). Digital divide: impact of access. In P. Rössler, C. A. Hoffner, & L. van Zoonen, *The International Encyclopedia of Media Effects* (pp. 1-11). John Wiley y Sons.

Wertheim, M. (1999). *The pearly gates of cyberspace. From Dante to Internet.* W.E. Norton & Company.

INFORMÁTICA Y DERECHO

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO
(SEGUNDA ÉPOCA)

FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES
DE DERECHO E INFORMÁTICA

ISSN 2530-4496 – N.º 13, 2023, PP. 85-90

ESFUERZOS DENTRO DEL ESTADO DE CHIHUAHUA, MÉXICO EN MATERIA DE CIBERSEGURIDAD

CYBERSECURITY EFFORTS WITHIN THE STATE OF CHIHUAHUA, MEXICO

Ricardo Ramón Torres Knight[1]

Osiris Abril Méndez Morales[2]

1 Ingeniero y Profesor en la Facultad de Ingeniería de la Universidad Autónoma de Chihuahua.
rtorres@uach.mx

2 Abogada y Profesora en la Facultad de Derecho de la Universidad Autónoma de Chihuahua. omendez@uach.mx

Resumen

La ciberseguridad son los esfuerzos que se hacen para proteger los sistemas informáticos, lo cual incluye, pero no limita a equipos físicos, redes, software, sistemas operativos, datos, entre otros contra cualquier tipo de ataque malicioso o incidentes de seguridad. Es esencial en la actualidad ya que cualquier ente privado o público depende funcionalmente de sistemas informáticos para su operación. Es común que las Entidades Federativas, así como los Gobiernos Federales trabajen en foros e iniciativas para combatir los nuevos delitos que puedan ir apareciendo. Aquí estaremos haciendo una revisión de los trabajos que se hacen en el Estado de Chihuahua para mejorar la seguridad en línea y evitar delitos cibernéticos para mejorar la lucha contra la ciberdelincuencia. De la misma manera daremos una revisión dentro de las Instituciones Educativas del Estado de Chihuahua para saber de qué forma están colaborando ante estos nuevos desafíos.

Palabras Clave

ciberseguridad, delitos cibernéticos, opiniones legales.

Abstract

Cybersecurity is the efforts made to protect computer systems, including but not limited to physical equipment, networks, software, operating systems, data, among others against any type of malicious attack or security incident. It is essential nowadays since any private or public entity depends functionally on computer systems for its operation. It is common that the Federal Entities, as well as the Federal Governments work in forums and initiatives to combat new crimes that may appear. Here we will be reviewing the work being done in the State of Chihuahua to improve online security and prevent cybercrime to improve the fight against cybercrime. In the same way, we will be reviewing the educational institutions in the State of Chihuahua to know how they are collaborating to face these new challenges.

Keywords

Cybersecurity, Cybercrime, Legal Opinions.

Introducción

La ciberseguridad es un tema que vemos más frecuentemente en todos los medios de información, aunado a esto después de la pandemia por COVID se observó un incremento de tramites bancarios, gubernamentales y empresariales de modo virtual, es decir infraestructura ya hecha para hacer tramites se vio aumentada en su demanda, así como la realización de nuevos mecanismos digitales para reemplazar los tramites presenciales a virtuales. Esto ha abierto la puerta para el incremento de ataques a la ciberseguridad en todo este espectro de tramites. Según cita el Financiero solamente de 2019 donde hubo un registro de 300.3 millones de ataques a 120 mil millones de intentos en el 2021, un crecimiento de casi 400 veces, lo que coloco a México en el país más atacado en América Latina.[3]

Se puede observar que en algunas regiones los ingresos por este tipo de crímenes han ido reemplazado a los ingresos por el narcotráfico. De acuerdo con el Foro Económico Mundial (WEF), este tipo de delincuentes logran obtener 600,000 millones de dólares a nivel mundial de gobiernos, empresas e individuos. En el caso del narcotráfico los recursos que generan están en el orden de 320,000 millones de dólares anuales.[4]

Chihuahua en la ciberseguridad

El Estado de Chihuahua, según el último censo del Instituto Nacional de Información, Estadística e Informática en el 2020 tenía una población de 3, 741,869 personas[5], de los cuales 1,043,000 eran menores de 15 años, por lo que poco más del 72 % de la población es susceptible de delitos financieros actualmente. Por lo mismo los temas de ciberseguridad para el estado de Chihuahua tienen que estar presentes y con alta prioridad. Además, Chihuahua cuenta con un gran número de industria con alta tecnología y un incremento de dispositivos electrónicos en la sociedad, por lo que se deben de tener mejores regulaciones y contar con nuevas leyes e instituciones.

La Fiscalía General del Estado de Chihuahua cuenta con La Dirección de Análisis de Evidencia Digital e Informática Forense que es parte de la Dirección General del Centro Estatal de Información Análisis y Estadística Criminal tiene como objetivo contribuir, a través del desarrollo efectivo y organizado en las funciones sustantivas, la de recabar y analizar información a través de medios electrónicos y de telecomunicaciones para elaboración de informes técnico/forenses

3 Calderón, C. (2022, 9 junio). *México 'clientazo' de los ciberataques: crecen 42% amenazas por internet*. El Financiero. https://www.elfinanciero.com.mx/empresas/2022/06/09/aumentan-42-los-ciberataques-con-85-mil-millones-de-intentos-en-mexico/ (Fecha de consulta 22 de diciembre del 2022)

4 Barboza, C. (2021, 27 agosto). *Los ciberataques ya superan al narcotráfico y dañan más a empresas*. Business Insider México | Noticias pensadas para ti. https://businessinsider.mx/recursos-de-ciberataques-superan-narcotrafico-ademas-representan-mayor-impacto-economico-empresas/ (Fecha de consulta 22 de diciembre del 2022)

5 *Número de habitantes. Chihuahua.* (s. f.). https://cuentame.inegi.org.mx/monografias/informacion/chih/poblacion/ (Fecha de consulta 28 de diciembre del 2022)

con el fin de establecer vínculos y coadyuvar con las autoridades competentes a la resolución de investigaciones, esto en los términos de las disposiciones legales aplicables establecidas en el Reglamento Interior de la Fiscalía General.[6]

Esta dirección está compuesta por los departamentos de Informática Forense, Análisis Delictivo e Información Cibernética, los cuales en conjunto conforman la Policía Cibernética basadas en el modelo de policía cibernética federal. Esta policía es constantemente capacitada por agencias de seguridad como el FBI, la DEA entre otras.

Dentro del Plan Estatal de Seguridad Ciudadana y Procuración de Justicia 2022-2027[7] publicado en el Periódico Oficial del Estado de Chihuahua el 7 de mayo del 2022, se cuentan con las estrategias y acciones:

2.1.4.5. Coordinar como miembro de del Comité de Seguridad Nacional, la regulación y homologación de las Policías Cibernéticas de los municipios del Estado, logrando ser el primer contacto con la ciudadanía para delitos cibernéticos y brindar tanto asesoría como difusión de estrategias preventivas.

6.1.2. Generar productos de análisis de información estadística delictiva; además de información de resultados institucionales; y de aquellos generados por la Inteligencia y análisis criminal, que identifique estructuras delincuenciales y objetivos prioritarios generadores de violencia, además de productos de análisis criminal que tengan fundamentación metodológica y científica derivada del uso de las nuevas tecnologías de la información y comunicación, de la actividad cibernética en Internet, de los análisis de informática forense, y los análisis de contexto criminal, e informes sustentables que abonen al combate de la impunidad, manteniendo una cercanía comunitaria con la policía preventiva.

6.1.2.6. Potenciar las Áreas con un enfoque de modernidad y vanguardia a contar con mayores capacidades en materia de Ciberseguridad y en una mejor y mayor atención del área de Evidencia Digital y e Informática Forense hacia las Fiscalías Regionales y Especializadas.

6.1.2.8. Generar informes técnicos y productos de análisis criminal que tengan fundamentación metodológica y científica obtenida del uso y ventajas de las nuevas tecnologías de la información y comunicación, de la actividad cibernética en Internet, de los hallazgos y análisis de informática forense, y los análisis de contexto criminal, plasmada en informes sustentables que abonen en las investigaciones criminales y al combate de la impunidad.

6 *Dirección del Centro Estatal de Información, Análisis y Estadística Criminal*. (2022, 11 julio). Fiscalía General del Estado de Chihuahua. http://fiscalia.chihuahua.gob.mx/direccion-del-centro-estatal-de-informacion-analisis-y-estadistica-criminal/ https://cuentame.inegi.org.mx/monografias/informacion/chih/poblacion/ (Fecha de consulta 2 de enero del 2023)

7 *Plan Estatal de Seguridad Ciudadana y Procuración de Justicia 2022-2027*. (s. f.) https://chihuahua.gob.mx/sites/default/atach2/periodico-oficial/anexos/2022-05/ANEXO%2037-2022%20PLAN%20ESTATAL%20DE%20SEGURIDAD%20CIUDADANA%20Y%20PROCURACION%20DE%20JUSTICIA%202022-2027%20.pdf (Fecha de consulta 3 de enero del 2023)

6.1.3.10. Suscribir convenios de colaboración y cooperación nacionales e internacionales, en materia de combate al crimen organizado trasnacional, y de mecanismos de prevención e investigación en actividades de ciberseguridad, tráfico de personas, tráfico y consumo de drogas ilícitas en la entidad.

6.1.4.6. Contrarrestar la incidencia delictiva cibernética en todo el estado mediante productos de inteligencia e investigación, con el uso de inteligencia artificial y tecnología especializada en informática forense, rastreo de datos descentralizados en internet e indicadores de impacto generados por los sistemas de plataforma centinela, capacitar a empresas, escuelas y sector público y privado para el conocimiento de ciber seguridad, métodos de hackeo e ingeniería social defensiva, brindar a cada una de las instituciones lineamientos en cultura cibernética y seguridad social en el internet.

Instituciones de Educación Superior y Ciberseguridad Chihuahua

La Universidad Autónoma de Chihuahua firmo un convenio el 25 de octubre del 2017[8] con la Fiscalía General del Estado de Chihuahua para reforzar el vínculo cooperativo entre instituciones en carácter de seguridad informática, en beneficio de los chihuahuenses. El convenio establece la colaboración de ambas organizaciones en el desarrollo de un programa formativo específico, así como la organización, participación o colaboración conjunta en cursos y seminarios. Asimismo, se promueven también otras áreas de cooperación entre la Fiscalía General del Estado de Chihuahua y la Coordinación General de Tecnologías de Información, entre las que destacan el intercambio de información relativa a incidentes de seguridad y el desarrollo de proyectos tecnológicos. Esta línea de trabajo busca crear sinergias entre diferentes organizaciones, fomenta la búsqueda del talento y mejora la capacitación profesional de los alumnos en materia de ciberseguridad.

Uno de los resultados que se han tenido posterior a la firma de este convenio es el portal Ciberseguridad Chihuahua que se puede visitar en https://ciberseguridad.uach.mx/, el cual contiene recursos, guías y herramientas especializadas, así como información acerca de los ciberdelitos, de la misma manera ilustra y apoya para documentar y denunciar estos tipos de delitos, así como asesoría en caso de ser víctima de uno de ellos y dar un acompañamiento total. Aunado a eso cuenta con información y recomendaciones para tener una navegación segura por internet, así como guías para cuidar privacidad, cifrar información, etc.

Otra aportación por parte de la Universidad Autónoma de Chihuahua es el Diplomado de Seguridad Informática[9] que imparte en conjunto con la Asociación Nacional de Universidades e Instituciones de Educación Superior (ANUIES),

8 *Convenio de colaboración en materia de colaboración en seguridad informática entre la Universidad Autónoma de Chihuahua y la Fiscalía General del Estado de Chihuahua octubre del 2017*. (s. f.). http://transparencia.uach.mx/articulo_77/fraccion_xxxiii/CONTRATOS_Y_CONVENIOS_2018/COLAB-SEGURIDAD%20INFORMATICA-FISCALIA-25%20OCTUBRE%202017.pdf (Fecha de consulta 6 de enero del 2023)

9 *Diplomado de Seguridad Informática*. (s. f.). https://diplomadoanuies.uach.mx (Fecha de consulta 10 de enero del 2023)

que contiene los temas más actuales en ciberseguridad, con módulos que incluyen introducción a la seguridad informática, hacking ético, controles técnicos de seguridad, gestión de la seguridad de la información y marco regulatorio.

Conclusiones

Como se ha estado escribiendo, el incremento tanto de dispositivos digitales, como de servicios digitales crece de manera vertiginosa y por lo tanto los delitos cibernéticos tienen un mayor espectro donde pueden efectuar sus delitos. También se observa que las ganancias de los delincuentes son muy lucrativas a nivel mundial, incluso al estar en muchos países por arriba de las ganancias por narcotráfico. Por eso estaremos viendo que constantemente se estarán abriendo nuevas oportunidades y formas de delitos informáticos por lo que tenemos que estar monitoreando iniciativas como la página de ciberseguridad de la Universidad Autónoma de Chihuahua y de la Fiscalía del Estado de Chihuahua, donde constantemente actualizan información de nuevas formas de delito y de actualizaciones de seguridad en equipos físicos. Aunado a eso estamos conscientes de que la delincuencia estará aportando un gran volumen de recursos financieros y técnicos para le realización de delitos de manera que será difícil de competir por las instituciones si no se realizan alianzas estratégicas, por lo que se insta a los responsables de seguridad a buscar estos vínculos.

Referencias

Calderón, C. (2022, 9 junio). México 'clientazo' de los ciberataques: crecen 42% amenazas por internet. El Financiero. https://www.elfinanciero.com.mx/empresas/2022/06/09/aumentan-42-los-ciberataques-con-85-mil-millones-de-intentos-en-mexico/

Barboza, C. (2021, 27 agosto). Los ciberataques ya superan al narcotráfico y dañan más a empresas. Business Insider México | Noticias pensadas para ti. https://businessinsider.mx/recursos-de-ciberataques-superan-narcotrafico-ademas-representan-mayor-impacto-economico-empresas/

Número de habitantes. Chihuahua. (s. f.). https://cuentame.inegi.org.mx/monografias/informacion/chih/poblacion/

Dirección del Centro Estatal de Información, Análisis y Estadística Criminal. (2022, 11 julio). Fiscalía General del Estado de Chihuahua. http://fiscalia.chihuahua.gob.mx/direccion-del-centro-estatal-de-informacion-analisis-y-estadistica-criminal/ https://cuentame.inegi.org.mx/monografias/informacion/chih/poblacion/

Plan Estatal de Seguridad Ciudadana y Procuración de Justicia 2022-2027. (s. f.) https://chihuahua.gob.mx/sites/default/atach2/periodico-oficial/anexos/2022-05/ANEXO%2037-2022%20PLAN%20ESTATAL%20DE%20SEGURIDAD%20CIUDADANA%20Y%20PROCURACION%20DE%20JUSTICIA%202022-2027%20.pdf

Convenio de colaboración en materia de colaboración en seguridad informática entre la Universidad Autónoma de Chihuahua y la Fiscalía General del Estado de Chihuahua octubre del 2017. (s. f.).

INFORMÁTICA Y DERECHO

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO
(SEGUNDA ÉPOCA)

FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES
DE DERECHO E INFORMÁTICA

ISSN 2530-4496 – N.º 13, 2023, PP. 91-104

ESCENARIOS DE ATENCIÓN DIGITAL Y CONTEMPLACIONES DE CIBERSEGURIDAD MX

DIGITAL CARE SCENARIOS AND CYBERSECURITY CONTEMPLATIONS MX

Carlos Ramírez Castañeda[1]
Doctor. Universidad Anáhuac Online

1 Doctor en administración y políticas públicas. Universidad Anáhuac Online.

Resumen

El objetivo de esta publicación es analizar tres escenarios de impacto relacionados a la ciberseguridad bajo el ejemplo de México, partiendo con una escala en donde la información e integridad del usuario desde su navegación podría tener afectaciones, en el segundo escenario el patrimonio e instituciones financieras se convierten en el objetivo ante temas delictivos y para finalizar una reflexión sobre el escenario de acción nacional interno que requiere miras mucho más robustas en pro de la prevención.

Si el usuario tiene un parámetro de conocimiento sobre cómo operan los escenarios digitales donde la ciberseguridad se hace presente, tendremos un impacto preventivo y sobre todo una concientización que ayudaría a reducir los impactos directos e indirectos.

La ciberseguridad debe contemplar diversos escenarios, jurídicos, técnicos, políticas públicas, e incluso pedagógicas para llevar a un punto donde el usuario evita ser víctima, no por sentido común, sino por conocimiento.

Palabras clave

Wifi, Carding, Defacement, DDoS, Ransomware.

Abstract

The objective of this publication is to analyze three impact scenarios related to cybersecurity using the example of Mexico, starting with a scale where the information and integrity of the user from browsing could be affected, in the second scenario the assets and financial institutions are become the objective in criminal matters and to conclude a reflection on the internal national action scenario that requires much more robust views in favor of prevention.

If the user has a parameter of knowledge about how digital scenarios where cybersecurity is present operate, we will have a preventive impact and, above all, an awareness that would help reduce direct and indirect impacts.

Cybersecurity must consider various legal, technical, public policy, and even pedagogical scenarios to reach a point where the user avoids being a victim, not out of common sense, but out of knowledge.

Keywords

Wifi, Carding, Defacement, DDoS, Ransomware

Introducción

Nos encontramos en una época donde la conexión masificada a internet e interconexión entre usuarios y dispositivos nos lleva a vivir una realidad que pende de un hilo, con la delgadez entre lo digital y lo material, una realidad en la que convergemos a través de hilos invisibles que nos permiten la realización de diversas tareas cotidianas, algunas especializadas, otras más de ocio y recreación, al final del día nos encontramos virtual y presencialmente en actividad.

Con la premisa anterior debemos reconocer e identificar todos los posibles escenarios digitales, gestados a través de las tecnologías de la información y comunicación (TIC), con ello tener miras a las contemplaciones relacionadas intrínsecamente a la ciberseguridad, reconociendo a esta última como un pilar fundamental para el resguardo no solamente de información en alguna de las categorizaciones relacionadas, si no también pasando transversalmente y con influencia directa hacia usuarios, software, hardware, lineamientos jurídicos, pedagógicos, políticas públicas, políticas internas, empresas y gobiernos, todos siendo parte de un ecosistema digital que requiere resguardo preventivo.

Para todo lo anterior la ciberseguridad requiere un entendimiento primordial para los usuarios y así reconocer los múltiples escenarios, conociendo como es que opera un ciberdelincuente, y operando en la realidad con casos reales que nos servirán de punto de partida.

El mundo digital muchas veces supera a la ficción y nuestra modernidad y la cotidianeidad imperan un énfasis profundo para dar a conocer al usuario gran parte de lo que debe resguardarse y así no ser víctima de un ciberataque, una vulnerabilidad, malware, entre muchas otras categorías que desentrañaremos en este artículo.

Cabe resaltar que muchos de los escenarios de acción de la ciberseguridad son fluctuantes y están en un constante movimiento y actualización, por lo cual se hace una identificación generalizada y las posibles afectaciones con base a casos acontecidos.

Escenario inalámbrico (WIFI)

La versatilidad que permiten los dispositivos portátiles es amplia, involucrando una gama diversa de hardware como móviles, laptops, vestibles y demás dispositivos relacionados al internet de las cosas, también conocido como IoT por sus siglas “Internet of things”, todos los anteriores tienen un común denominador, un estándar y tecnología de conexión que permite estar conectados a internet de manera inalámbrica, superando a los avances que se tenían hace un par de décadas con conexiones alámbricas dependientes.

El crecimiento de usuarios de internet y la penetración del espectro en los hogares mexicanos ha tenido un incremento en los últimos años, la llegada pandémica y aislamiento fueron factores propicios para migrar a un escenario digital, muchas veces obligado, en el cual los usuarios llegaron a la utilización bajo

un aprendizaje empírico, lo cual los deja expuestos ante factores de inseguridad digital.

En 2022, se estimó que aproximadamente 98,6 millones de personas en México tenían acceso a internet, lo que supone un incremento de alrededor de 16 millones con respecto al número de usuarios registrados en 2021. Se pronostica que para 2026 alrededor de 118,2 millones de mexicanos tengan acceso a la red.[2]

Si hacemos un contraste con el número de usuarios de portátiles, encontraremos un amplio porcentaje poblacional, lo cual nos lleva al uso de un espectro de comunicación Wifi.

Wifi es una tecnología de red inalámbrica a través de la cual los dispositivos, como computadoras (portátiles y de escritorio), dispositivos móviles (teléfonos inteligentes y accesorios) y otros equipos (impresoras y videocámaras), pueden interactuar con Internet. Permite que estos dispositivos, entre tantos otros, intercambien información entre sí y establezcan, de esta manera, una red.

La conectividad a Internet se logra a través de un router inalámbrico. Cuando accede a wifi, se conecta a un router inalámbrico que permite que los dispositivos que admiten wifi interactúen con Internet.[3]

Sin entrar en mayores detalles técnicos sobre las diversas frecuencias, la nomenclatura jurídica relacionada a espectros de comunicación inalámbrica requiere una actualización y homologación con estándares internacionales en pro de la prevención y seguridad de los usuarios, por mencionar únicamente a la NMX-I-1362-NYCE-2021[4] con relación a los dispositivos IoT, pero dejando de lado los portátiles, móviles por mencionar algunos. ¿Pero por qué dejar todo a una normativa? Los usuarios requieren en un primer momento conocimiento sobre la tecnología que están utilizando y sobre todo énfasis en los riesgos que derivan de la tecnología inalámbrica.

Aquí mencionaremos a uno de los primeros ataques relacionados a la tecnología inalámbrica, los "Evil Twin" los cuales consisten en que el atacante genera un punto de acceso Wifi clonado, con el mismo nombre que el original, esperando que el usuario víctima haga un enlace buscando conectividad, aquí usualmente los puntos falsos tienen un portal cautivo el cual muchas veces suplanta el panel de inicio de algún sitio de redes sociales o correo electrónico, al emular con alta similitud al real los usuarios inexpertos caen y con ello ceden sus accesos a los atacantes.

Los ataques Evil Twin se pueden detectar en un segundo momento, cuando el usuario tiene la conexión Wifi-encendida en automático se hará un enlace a la red con el nombre guardado, aquí es donde el usuario debe corroborar que tiene

2 Statista. Número de usuarios de internet en México de 2015 a 2025. Disponible en https://es.statista.com/estadisticas/1171866/usuarios-de-internet-mexico/ (Fecha de consulta 8 de enero del 2023)

3 Cisco. ¿Qué es Wi-Fi?. Disponible en https://www.cisco.com/c/es_mx/products/wireless/what-is-wifi.html (Fecha de consulta 8 de enero del 2023).

4 DOF. DECLARATORIA de vigencia de la Norma Mexicana NMX-I-1362-NYCE-2021.Disponible en https://www.dof.gob.mx/nota_detalle.php?codigo=5642167&fecha=08/02/2022#gsc.tab=0 (Fecha de consulta 8 de enero del 2023)

conexión inmediata y no a través de un panel de inicio de sesión, de igual manera revisando el url del portal cautivo.

A través de los puntos de acceso falso o suplantado para este ataque descrito, los atacantes también pueden interceptar todos los datos que circulan a través del enlace, muchas veces permitiendo otro tipo de ataques, como el secuestro de sesiones a través de cookies, la visibilidad de texto plano de accesos a sitios, etc.

El escenario preventivo para el usuario es simple, no dejar su conexión Wifi encendida todo el tiempo, apagarla cuando no esté en uso, de igual manera revisar antes de conectar los nombres de las redes y si existiese duplicidad, verificar la conectividad sin algún tipo de panel de acceso que solicite usuario y contraseña, está de sobra reiterar evitar utilizar redes Wifi públicas y solo en caso de emergencia utilizarlas y evitar hacer algún tipo de inicio de sesión, en correo electrónico, redes sociales, banca en línea, y otros accesos que imperen información relativa al usuario en la esfera de lo privado.

Escenario financiero

El sector financiero no es ajeno al contexto digital, en la actualidad la mayoría de las instituciones bancarias ofrecen a sus clientes el servicio de banca en línea, por medio de la cual se pueden realizar múltiples operaciones bancarias a través de los dispositivos móviles de los usuarios, de esta forma es posible consultar estados de cuenta, hacer transferencias y hasta pagar servicios por medio de los teléfonos celulares, lo cual simplifica muchos temas de movilidad y tiempos reducidos.

De acuerdo con la base de datos Global Findex, para el año de 2021 se registró que el 76 % de los adultos a nivel mundial contaban con una cuenta en un banco, otra institución financiera o por medio de un proveedor de dinero móvil, también registraron, en sus datos más recientes, que dos terceras partes de los adultos de todo el mundo realizan o reciben pagos digitales, además el 83 % de las personas que recibieron pagos digitales también usaron sus cuentas para realizar pagos digitales[5].

Con estos datos podemos ver que un gran porcentaje de la población mundial hace uso de este tipo de servicios bancarios en línea, dichos servicios tuvieron un crecimiento considerable durante la pandemia de SARS-CoV-2[6], pues resultado de las medidas de aislamiento aplicadas en gran parte del mundo, muchas personas optaron por realizar sus transacciones bancarias por medio de los servicios digitales que sus respectivos bancos ofrecían sin la necesidad de salir de sus hogares, este hecho también fue registrado por la base de datos Global Findex,

5 Banco Mundial. La COVID-19 incrementa el uso de los pagos digitales a nivel mundial. Disponible en: https://www.bancomundial.org/es/news/press-release/2022/06/29/covid-19-drives-global-surge-in-use-of-digital-payments (Fecha de consulta 09 de enero de 2023)

6 SARS-CoV-2: Virus que causa una enfermedad respiratoria llamada enfermedad por coronavirus de 2019 (COVID-19). El SARS-CoV-2 es un virus de la gran familia de los coronavirus. Disponible en https://www.cancer.gov/espanol/publicaciones/diccionarios/diccionario-cancer/def/sars-cov-2 (Fecha de consulta 9 de enero del 2023)

durante la pandemia más del 40 %[7] de personas adultas que realizaron pagos a comercios minoristas o compras en línea, utilizaron por primera vez métodos de pago como tarjeta, un teléfono o internet; estos datos fueron tomados exceptuando a el caso de China, esto ameritaría un análisis aparte, cosa que no es pertinente a nuestro caso.

Dentro de los datos expuestos podemos notar otro de los ejemplos del escenario digital financiero, y es el caso del comercio electrónico junto con las soluciones digitales relacionadas, los cuales gracias al crecimiento marcado se pusieron en miras de los atacantes al ser soluciones de uso masificado.

El comercio electrónico o e-commerce, como también se le conoce, tal como su nombre lo indica es el comercio de bienes y/o servicios por medio de plataformas digitales, un tema que cobró también importancia relevante en el contexto pandémico y está estrechamente relacionado con el escenario financiero.

La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) en México, reporto que en el primer trimestre del 2021 las compras registradas de comercio electrónico efectuadas por medio de tarjetas de crédito y débito llegaron a ser de 176 millones de operaciones por un monto de 101 mil 015 millones de pesos, pese a que la situación financiera no era de las mejores en todo el mundo, la preferencia por el uso de fondos propios para compras por internet en contraste al mismo periodo del 2020[8].

Para 2022 la Condusef reporto que en México para el primer trimestre de ese año alrededor de 1,019 millones de pagos con tarjetas en comercios tradicionales y en comercios electrónicos; de los cuales el 21.3% del total de pagos representan los pagos realizados al comercio electrónico[9].

Cuando un producto o servicio comienza a ser más utilizado, mayor interés habrá por parte de la delincuencia, para este caso ciberdelincuencia, para así poder obtener algún tipo de lucro o beneficios de manera ilícita, es por ello que durante el primer trimestre de 2022, la Condusef registró que de 217 millones de operaciones autorizadas por parte de la institución emisora de la tarjeta (producto del comercio electrónico), el 0.41% resulto en un contracargo o reclamación por parte del titular de la tarjeta, al no reconocer la operación o el monto de esta[10].

Tomando como referencia las cifras anteriores podemos mencionar de manera directa la usurpación de datos financieros; el Banco de México describe tres

7 Banco Mundial, *Op. Cit.,* Pág 1

8 CONDUSEF. La CONDUSEF informa sobre las compras en comercio electrónico durante el primer trimestre de 2021. Disponible en : https://www.condusef.gob.mx/?p=contenido&idc=1750&idcat=1#:~:text=En%20el%20primer%20trimestre%20del,decir%2C%20177%20millones%20de%20operaciones (Fecha de consulta 9 de enero del 2023)

9 CONDUSEF. CONDUSEF informa sobre las compras en comercio electrónico, durante el primer trimestre de 2022. Disponible en: https://www.condusef.gob.mx/?p=contenido&idc=2028&idcat=1#:~:text=%C2%B7%20En%20el%20primer%20trimestre%20del,mil%20913%20millones%20de%20pesos. (Fecha de consulta 9 de enero del 2023)

10 CONDUSEF, *Op.cit.,* p. 2

tipos de riesgos a los que se pueden enfrentar las instituciones financieras ante los ciberataques:

1. *Disrupciones de las tecnologías de la información que utilizan y la consecuente indisponibilidad de sus servicios*
2. *Afectación a la integridad, confidencialidad y disponibilidad de la información que gestiona la institución, incluida la de sus clientes*
3. *Pérdidas económicas a las propias instituciones o a sus clientes*[11].

La información de los usuarios suele ser un blanco recurrente para los atacantes, a continuación, se abordarán algunos de los riesgos más comunes dirigidos a la información financiera de los usuarios. Particularmente los accesos y los números para realizar compras en línea como los dígitos frontales de la tarjeta, fecha de vencimiento y números de verificación (CVV) son los blancos primordiales que resultan para realizar "carding" relacionado a la clonación de tarjetas.

Este delito consiste en el robo de la información que se encuentra en los plásticos de las tarjetas, una vez que el delincuente tiene en su poder la tarjeta, transfiere los datos a una tarjeta vacía con ayuda de un dispositivo electrónico llamados "skimmer", incluso algunos más accesibles como lectores/escritores en sim y banda magnética; para realizar dicha acción no es necesario que despojen de sus pertenencias a los usuarios, simplemente basta con que los delincuentes tengan por unos momentos la tarjeta en su poder y fuera de la vista del usuario para que puedan obtener los datos, en otros casos el colocar los datos de acceso en un portal web, para este último caso hablamos de carding puro.

Los datos de las tarjetas también pueden ser adquiridos al fotografiar la parte delantera y trasera de los plásticos, obteniendo así los 16 dígitos y los dígitos verificadores; el nombre del usuario puede ser adquirido de la misma forma o bien pueden hacerlo de alguna otra manera, incluso cayendo en la suplantación/usurpación de identidad o generando una aleatoria.

Cuando los usuarios son víctimas de este delito suelen percatarse hasta que revisan sus cuentas y encuentran cargos que no reconocen de compras o servicios que no hicieron o consumieron.

Muchos bancos proporcionan herramientas para prevenir este tipo de situaciones, por ejemplo, limitar el monto máximo para las compras con la tarjeta, así como la notificación a la banca en línea de cada movimiento que se realiza en las cuentas, etc.

Los dos escenarios anteriores, carding en parte digital y clonación de tarjetas en parte física son riesgos implícitos que sin un control del usuario y revisión periódica de recursos como banca en línea se convierten en potenciales peligros, ahora mencionemos un escenario de la ciberseguridad que involucra ambos mundos, desde el engaño hasta la consumación y afectación al patrimonio.

A través del "phishing" los atacantes obtienen información de sus víctimas haciéndolas caer en el error por medio del uso de trucos de ingeniería social, una

11 Banco de México. Ciberseguridad en Banco de México. Disponible en: https://www.banxico.org.mx/sistema-financiero/seguridad-informacion-banco.html (fecha de consulta 09 de enero de 2023)

técnica que consiste en la inducción al error o engaño, logrando así que sus víctimas revelen sus datos confidenciales, entre ellos también los datos financieros.

Este tipo de ataques puede realizarse por correo electrónico, mensajes de texto SMS, redes sociales, etc., pero en todos los casos la base es la misma, el atacante inicia una comunicación con la victima para persuadirla para que acceda a un enlace para que esta envíe la información solicitada o descargue un documento adjunto, o en ocasiones hasta para que realice un pago; previamente el atacante pudo haber estudiado a la víctima, por medio de su actividad en redes sociales y de esta forma entender que es lo que se le hace más atractivo o creíble para que la víctima caiga en el engaño, algunos van desde un simple mensaje spam hasta notificaciones "bancarias" muy bien trabajadas y estructuradas para que los usuarios caigan en el engaño, actualmente los atacantes más experimentados utilizan voz obtenida a través de grabaciones oficiales de los bancos para que sea más creíble y contactan a través de plataformas de mensajería instantánea.

La compañía Kaspersky realizo una investigación sobre el aumento de los ataques financieros en América Latina y con respecto al phishing revela que durante los meses de enero a agosto de 2022 esta empresa logro bloquear 38 millones de accesos a enlaces fraudulentos y se enlistaron los países latinoamericanos con más ciberataques, en donde encontramos a Brasil a la cabeza de la lista en primer lugar y Ecuador en segundo[12].

De manera global los países latinoamericanos que son más asediados por ataques de phishing bancario son Brasil con el sexto lugar global, ecuador con el segundo, 33°Perú, 37º Colombia, 48º Chile, 51° Panamá, 61º Guatemala, 65º Paraguay y México en el lugar 71[13].

Este estudio también revela los principales objetivos de este tipo de ataques, en primer lugar, con un 27% se encuentran las credenciales de banca por Internet/móvil, 22% credenciales de redes sociales, 18% credenciales de servicios en línea (tiendas online, streaming, etc.), el 9% dirigido a la utilización de temas de servicios financieros para robar contraseñas y el 7% quiere datos de pago (tarjeta de crédito)[14].

Hay medidas que se deben tener en cuenta para poder proteger los datos financieros y lo relacionado ante estos tipos de ataques y cualquier otro relacionado, si bien las instituciones bancarias tienen la responsabilidad de resguardar nuestros datos y dinero en el entorno digital, también es responsabilidad del usuario llevar a cabo ciertas acciones para resguardar sus datos, a continuación, mencionamos algunas recomendaciones para reducir el riesgo de los escenarios comentados:

12 Kaspersky. Los ataques financieros crecen en América Latina y aumenta la preocupación por el uso de la piratería. Disponible en: https://latam.kaspersky.com/blog/panorama-amenazas-latam-2022/25509/ (Fecha de consulta 09 de enero de 2023)

13 Ibidem. p. 3

14 Ibidem. Pag 3

a) Configuración de servicios de banca en línea con opciones de notificación ante cualquier actividad, así como el monitoreo constante y continuo de la misma, manteniendo una actualización de contraseñas y limitando si es el caso los montos máximos para operaciones.
b) Estar al tanto de las tendencias de ciberseguridad y recomendaciones financieras, esto muchos bancos mexicanos lo realizan incluso en anuncios desde las sucursales y comunicados oficiales.
c) Al momento de realizar compras en línea, tener presente la revisión del url donde se está realizando la compra, así como hacerlo desde redes propias no públicas, junto con los controles de banca en línea.
d) Evitar dejar la tarjeta física al momento de pagar, pues como se mencionó, basta con una fotografía para la obtención de los datos confidenciales y así realizar compras, no dejarla fuera de vista al pagar se debe convertir en un acto de supervivencia digital básico.
e) En caso de detectar actividad inusual reportar de inmediato al banco de uso a través de los canales oficiales de comunicación, estos se encuentran en los portales web.

Lo anterior podrá servir como directriz de acción preventiva para los usuarios de servicios financieros y comercio electrónico, teniendo así miras en el conocimiento de cómo opera el atacante/ciberdelincuente y los respectivos resguardos de acción.

Escenario nacional (MX)

Para este último apartado analizaremos algunos de los casos relacionados a la ciberseguridad a nivel país, a diferencia de los dos escenarios anteriores el inalámbrico bajo un contexto y matiz más personal para el usuario en sentido de prevención digital a su información y todo lo que circula en una red que podría ser homologado a la seguridad con la que cuenta un hogar. En el escenario financiero el abordaje va en un sentido a escala superior al involucrar instituciones bancarias por ejemplo y terceros que pueden ser los gestores de comercio electrónico, aquí buscando resguardar el patrimonio del usuario, al final del día carding, clonación de tarjetas o conseguir los accesos del usuario víctima representará una afectación directa a su patrimonio y economía.

Para esta tercera escala la atención debe cumplirse en sentido mayor, bajo el resguardo que pudiese hacer garante a la ciberseguridad en distintas ópticas, desde políticas públicas, hasta la aplicación reactiva si fuese el caso.

Abrimos mencionando a la empolvada y dejada a la deriva la Estrategia Nacional de Ciberseguridad[15] la cual para el caso mexicano es la primera en su tipo, sin embargo no se ha tenido una continuidad y periodicidad de actualización, es menester hacer hincapié y mencionar que las tendencias digitales avanzan en instantes, los ciberataques evolucionan, los atacantes se especializan a un grado

15 Estrategia Nacional de Ciberseguridad. 2017. Disponible en https://www.gob.mx/gobmx/documentos/estrategia-nacional-de-ciberseguridad (Fecha de consulta 10 de enero del 2023)

que logran identificar huecos jurídicos y operan con tecnologías que sobrepasan políticas y lineamientos, justo por esto se requiere miras de contemplación a nuevas conductas y relacionadas a medios tecnológicos.

A manera de referencia la estrategia contempla rubros sociales relacionados a derechos, economía, instituciones, seguridad en vertiente pública y nacional, cada apartado es totalmente transversal a los otros, pues no podemos hablar de ciberseguridad sin dejar de lado algún aspecto importante, de impacto o con posibles afectaciones.

Es importante mencionar que, si el escenario nacional es afectado, los daños colaterales a toda escala transversal serán notorios y con afectaciones directas indirectas hacia la sociedad, empresas, y diversos rubros, dejando en claro que la ciberseguridad no puede ser separada de otros tópicos, pues es un tema pertinente de atención generalizado.

Por ejemplo, en el escenario del impacto a sitios web (cosa que se ha dado en niveles estatales, federales) a través de un desfiguro o "defacement" la infraestructura de funcionamiento de aplicación para los usuarios o sociedad en este caso tendría una notoria afectación.

El defacement es un tipo de ataque que se realiza contra un sitio web, en el que se modifica la apariencia de alguna de sus páginas, para llevar a cabo algún tipo de acción fraudulenta o de vandalismo.[16] Con esta definición un poco más clara, pensemos en la estructura de los sitios web de índole gubernamental que permiten la realización de trámites, por ejemplo citas vehiculares de verificación, consulta de infracciones y multas, actas de nacimiento, datos de registro poblacional, pagos por marcas, la lista sería muy larga, el punto está en que si uno de estos llega a fallar, ralentizaría todo sector transversal dejando afectaciones al usuario final, el ciudadano.

Con el ataque anterior van de la mano los DDoS. Un ataque de denegación de servicio distribuido (DDoS) es un intento malintencionado de interrumpir el tráfico normal de un servidor, servicio o red determinada, sobrecargando el objetivo o su infraestructura asociada con una avalancha de tráfico de Internet.[17]

A diferencia de los defacement, los DDoS no requieren que un atacante tome el control del sitio web, pasando los controles del panel de inicio de sesión/administración, estos simplemente requieren inyección de tráfico para dejar fuera de línea el sitio o servicio, y son de los más abundantes incluso contra empresas, los gobiernos son víctimas de ataques de denegación de servicio distribuido y nuevamente vemos las consecuencias matizadas en el usuario final.

En estos escenarios mencionados es complicado lograr un punto de prevención sin contemplar soluciones de software preventivas, dejando la parte jurídica de lado en un primer momento, pues a pesar de ser prevenibles, las capacidades técnicas muchas veces sobrepasan a las soluciones en el mercado convencional,

16 INCIBE. Defacement. Disponible en https://www.incibe.es/aprendeciberseguridad/defacement (Fecha de consulta 10 de enero del 2023)

17 CloudFare. ¿Qué es un ataque DDoS?. Disponible en https://www.cloudflare.com/es-es/learning/ddos/what-is-a-ddos-attack/ (Fecha de consulta 10 de enero del 2023)

sin embargo, hacer conciencia de los impactos y lo que está aconteciendo al usuario final a manera de impacto poblacional sería de lo mejor, pues cada día es más abundante este tipo de acciones. Obviamente a una escala de toma de decisiones se requiere la implementación y canalización de recursos para el soporte, infraestructura y parte humana de atención, sumado a unos actuales lineamientos relacionados a la ciberseguridad, para el caso mexicano esto es una total utopía, pues se vive en el sexenio en curso sin importancia a la tecnología y bajo un esquema de austeridad hacia estos temas que parecieran tabú o un retroceso de décadas, pero esto no es el punto.

Pasemos a otro escenario que requiere una mención, pues se ha convertido en una de las tendencias globales más utilizadas por los ciberdelincuentes, tendencia que ha dejado pérdidas millonarias y un shock de operaciones a escala nacional como el caso de nuestro vecino del sur.

Por primera vez, un grupo llamado Conti logró paralizar las operaciones financieras de todo un país: Costa Rica en abril de 2022; incluso llevando al país a declarar una emergencia nacional. Al principio se trataba de operaciones financieras, pero rápidamente los ataques se extendieron, ya que a finales de mayo el grupo repitió y atacó esta vez a la caja de seguridad social a través del ransomware Hive. El costo estimado de esta crisis se estima en $38 millones por día.

Como recordatorio, Conti (aparecido en 2020) es uno de los grupos más prolíficos del año 2022 con 200 millones de euros de ingresos en 2021. Desde el 27 de noviembre de 2021 hasta el 27 de febrero de 2022, el grupo Conti afirma haber comprometido a más de 50 nuevas víctimas, y dos tercios de las organizaciones tienen su sede en Europa y el Reino Unido.[18]

Millones en pérdidas, millones en ganancias para los ciberdelincuentes, antes de continuar hagamos mención de la definición de ransomware.

El malware de rescate, o ransomware, es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos. Las primeras variantes de ransomware se crearon al final de la década de los 80, y el pago debía efectuarse por correo postal. Hoy en día los creadores de ransomware piden que el pago se efectúe mediante criptomonedas o tarjetas de crédito.[19]

México en distintas instancias gubernamentales ha tenido afectaciones de ransomware, por mencionar una infraestructura de interés nacional como PEMEX, quien en 2019 fue víctima de un ataque a escala de impacto interno con consecuencias en el suministro petrolero. Ahora pensemos en el escenario dónde el sector salud es atacado por ransomware, sin un plan de prevención, mitigación, reacción queda totalmente en las manos de los atacantes, muchos de los pacientes conectados a un dispositivo que los mantiene con vida como respiradores

18 Datacenter Dynamics. 2022, el año del ransomware: el volumen de estas amenazas en Europa aumentó un 63%. Disponible en https://www.datacenterdynamics.com/es/noticias/2022-el-a%C3%B1o-del-ransomware-el-volumen-de-estas-amenazas-en-europa-aument%C3%B3-un-63/ (Fecha de consulta 10 de enero del 20233)

19 Malwarebytes. Ransomware. Disponible en https://es.malwarebytes.com/ransomware/ (Fecha de consulta 10 de enero del 2023)

o en una cirugía podrían perder la vida. Así de simple sería realizar un atentado a escala nacional con nuevamente repercusiones a distintos niveles. ¿Estamos listos para un ataque de tal magnitud? La respuesta es no, se requiere más que el impulso tecnológico, actualización jurídica, implementación técnica, se requiere importancia.

Los escenarios abordados a escala nacional son solamente algunos de los muchos que podrían darse, a entendimiento y palabras simples los abordamos, sin embargo, nuevamente hacemos mención de la evolución y especialización de alto nivel y actualidad de los atacantes, lo cual en este momento podría ser controlable, pero en un lapso de tiempo corto ya no hay control para ello y el impacto es mayor, con más daños colaterales.

A manera de importancia y reflexión social, las políticas públicas digitales alineadas a la ciberseguridad requieren una difusión mayor y constante actualización, como se ha planteado, dar a conocer los posibles escenarios de acción dónde las afectaciones podrían llegar a los usuarios/ciudadanos ayudarían a prevenir y no ser parte de ello.

Estamos en una era donde las amenazas digitales tienen repercusiones materiales, muchas de estas pueden matizarse en la pérdida de vidas humanas, algo que ha llegado a un alcance o incluso rebasar a la ciencia ficción.

Consideraciones finales

La ciberseguridad tiene impactos en distintas escalas, sin embargo todas están conectadas, habiendo un usuario final quien podría ser afectado, hacer énfasis en la importancia de la información y el valor de la misma, así como algunos de los controles preventivos desde el hogar hoy en día es una total necesidad de supervivencia digital, reconocer el valor del patrimonio personal que hasta hace décadas solamente era relacionado a la parte física tangible, hoy es una realidad abstracta donde por medios digitales y tecnológicos se pueden gestar diversas afectaciones en detrimento del mismo. Reconocer el valor de la ciberseguridad a una escala garante de derechos, impulsada por políticas públicas e importancia gubernamental es una realidad de crecimiento incluso para los países.

Como pudimos analizar, el caso México, cuenta con diversos matices, pero el punto medular de todo ello es dar a conocer al usuario la forma de cómo operan los atacantes, y también el escenario de acción con su respectivo nombre técnico a palabras simples para que lo pueda procesar y se vuelva una acción de conocimiento preventivo.

La realidad controlada a través de hilos invisibles supera cada día a la ficción y la importancia de todas las acciones digitales tienen repercusiones físicas tangibles, una premisa que los usuarios de tecnología deben conocer y sobre todo comenzar a darle importancia.

Referencias

Banco de México. Ciberseguridad en Banco de México. https://www.banxico.org.mx/sistema-financiero/seguridad-informacion-banco.html

Banco Mundial. La COVID-19 incrementa el uso de los pagos digitales a nivel mundial. https://www.bancomundial.org/es/news/press-release/2022/06/29/covid-19-drives-global-surge-in-use-of-digital-payments

Cisco. ¿Qué es Wi-Fi? https://www.cisco.com/c/es_mx/products/wireless/what-is-wifi.html

CloudFare. ¿Qué es un ataque DDoS?. https://www.cloudflare.com/es-es/learning/ddos/what-is-a-ddos-attack/

CONDUSEF. CONDUSEF informa sobre las compras en comercio electrónico, durante el primer trimestre de 2022. https://www.condusef.gob.mx/?p=contenido&idc=2028&idcat=1#:~:text=%C2%B7%20En%20el%20primer%20trimestre%20del,mil%20913%20millones%20de%20pesos.

CONDUSEF. La CONDUSEF informa sobre las compras en comercio electrónico durante el primer trimestre de 2021. https://www.condusef.gob.mx/?p=contenido&idc=1750&idcat=1#:~:text=En%20el%20primer%20trimestre%20del,decir%2C%20177%20millones%20de%20operaciones

Datacenter Dynamics. 2022, el año del ransomware: el volumen de estas amenazas en Europa aumentó un 63%. https://www.datacenterdynamics.com/es/noticias/2022-el-a%C3%B1o-del-ransomware-el-volumen-de-estas-amenazas-en-europa-aument%C3%B3-un-63/

DOF. DECLARATORIA de vigencia de la Norma Mexicana NMX-I-1362-NYCE-2021. https://www.dof.gob.mx/nota_detalle.php?codigo=5642167&fecha=08/02/2022#gsc.tab=0 (

Estrategia Nacional de Ciberseguridad. 2017. https://www.gob.mx/gobmx/documentos/estrategia-nacional-de-ciberseguridad

INCIBE. Defacement. https://www.incibe.es/aprendeciberseguridad/defacement

Kaspersky. Los ataques financieros crecen en América Latina y aumenta la preocupación por el uso de la piratería. https://latam.kaspersky.com/blog/panorama-amenazas-latam-2022/25509/

Malwarebytes. Ransomware. https://es.malwarebytes.com/ransomware/

SARS-CoV-2: Virus que causa una enfermedad respiratoria llamada enfermedad por coronavirus de 2019 (COVID-19). El SARS-CoV-2 es un virus de la gran familia de los coronavirus. https://www.cancer.gov/espanol/publicaciones/diccionarios/diccionario-cancer/def/sars-cov-2

Statista. Número de usuarios de internet en México de 2015 a 2025. https://es.statista.com/estadisticas/1171866/usuarios-de-internet-mexico/

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO
(SEGUNDA ÉPOCA)

FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES
DE DERECHO E INFORMÁTICA

ISSN 2530-4496 – N.º 13, 2023, PP. 105-118

APROXIMACIÓN A LAS FALSIFICACIONES INFORMÁTICAS EN LA LEGISLACIÓN PENAL VENEZOLANA

APPROACH TO COMPUTER FORGERIES IN VENEZUELAN CRIMINAL LEGISLATION

José Gregorio Pumarejo Luchón[1]

1 Universidad Central de Venezuela. Abogado, Estudiante en la Especialización en Ejercicio de la Función Fiscal, Escuela Nacional de Fiscales del Ministerio Público (ENFMP), Estudiante de pre grado en Ingeniería en Informática, Universidad Nacional Experimental de las Telecomunicaciones e Informática (UNETI) Correo electrónico: luchon78@gmail.com

Resumen

La era informática ha traído consigo la falsedad de documentos, en este caso en el Documento Electrónico su tipificación con respecto a la falsificación del Código Penal, así como los elementos del tipo.

Palabras Claves

falsificación, documento electrónico, firma electrónica, delitos informáticos.

Abstract

The computer age has brought with it the falsification of documents, in this case in the Electronic Document its typification with respect to the falsification of the Criminal Code, as well as the elements of the type.

Keywords

Forgery. Electronic Document. Electronic signature. Cybercrime.

Prolegómenos

Con el avance de las nuevas tecnologías de información y comunicación (TIC), se ha facilitado el trabajo, en los cuales se necesitaba la asistencia de particulares para la celebración de determinados actos, como lo son la suscripción y emanación de documentos las cuales requerían por lo menos la presencia de la persona.

Con el Decreto con Rango, Valor y fuerza de Ley de Mensajes y Firmas Electrónicas[2] de las cuales surge nueva formas de comunicación y celebrar negocios, se utilizan los medios electrónicos y telemáticos para el intercambio comercial, ya sea desde una contratación electrónica hasta un mensaje electrónico, desde la publicación de la ley euisdem, se reguló la manera y el carácter probatorio de los mensaje de datos, firma electrónica y certificación electrónica, dentro de los cuales están los documentos electrónicos.

Los documentos per se, cumplen con diversas funciones, como garantía[3] en tanto y en cuanto la declaración en el presentada le es atribuida a la persona mediante la firma en el caso de los documentos electrónicos, la firma electrónica, la función de fe pública[4], dado que para determinado actos era necesario para la validez jurídica, la suscripción y la fe que otorgan los funcionarios, la función representativa, un documento representa hechos que pasaron en el pasado, y a través del documento se busca reproducir, y la función probatoria, dado que hay leyes que determinan el carácter probatorio del documento.

El documento electrónico cumple todas estas funciones para el tráfico jurídico de la cotidianidad, en torno a las nuevas tecnologías.

Falsificación Documental

En el Código Penal Venezolano, dentro del título VI referente a los delitos contra la fe pública, se encuentran los tipos referido a la falsificación de actos y documentos[5] los cuales regula tanto el funcionario público como el particular que incurra en estos hechos.

En la falsedad de actos y documentos del Código Penal Venezolano, y en general en el título VI, se protege la fe pública, esto es, la determinada certeza de un acto o de un instrumento o el carácter probatorio.

La doctrina ha dado un acercamiento conceptual en cuanto a la fe pública, que es y porque se tutela en el derecho penal.

Comenta el profesor Figari. (Ruben. E. Figari, 2014) citando a carrara, en sus comentarios a los delitos de contra la fe pública del código penal argentino.

2 Publicado en Gaceta Oficial N.° 37.076 del 13 de diciembre del 2000.

3 Para ampliar más sobre este tema, véase, Bacigalupo. E. Documento electrónicos y delitos de falsedad documental, Revista Electrónica de Ciencia Penal y Criminología [Versión digital], 2002

4 En cuanto a este tema, Véase, Devis. Hernando. Tratado de la Prueba Judicial Tomo II, Buenos Aires, Argentina: Victor. P de Zavalia, 1989

5 Artículo 316 y ss del Código Penal Venezolano.

"Es así que surgen los sellos o timbres; los funcionarios públicos que dan a los ciudadanos testimonios fehacientes con presunción de veracidad y los documentos públicos que prueban hechos y contratos consignados en ellos. "De este modo nace en los asociados una fe que no proviene de los sentidos, ni del juicio, ni de las simples afirmaciones de un individuo, sino de lo prescripto de la autoridad que la impone…En todos los casos, mi fe ya no es privada, sino pública; y lo es subjetivamente, pues esas condiciones no originan la creencia de un solo individuo particular, sino la creencia pública, la de todos los ciudadanos" (Pág. 4). En cuanto a la fe pública, por su parte Pessina comenta (Pessina. Enrico, 1884)

"La fe pública es la sancionada por el Estado, la fuerza probatoria atribuida por él a algunos objetos, signos o formas exteriores y los delitos que la lesionan se consuman cuando se adulteran aquellos actos, signos, formas a los cuales la ley atribuye el destino de hacer fe de la verdad de un estado de cosas del cual se deriva cualquier consecuencia jurídica" (Pág. 294).

Así que en grandes rasgos esta clase de tipos penales busca proteger la confianza de determinados actos o emisiones, en el que el Estado tiene un interés social, para la sana convivencia de la sociedad.

La Falsificación hace referencia a conductas materiales, recaen sobre la integridad de las cosas u objetos, mientras que la falsedad, hace referencia a una actitud intelectual, que se hace por declaraciones o invocaciones de algo falso[6] . Entre falsificación y falsedad hay una relación de género a especie, toda falsedad es una falsificación, pero no toda falsificación es una falsedad[7]

En cuanto a la falsedad específicamente, se ha entendido en la doctrina dos (02) clases de falsedades las cuales están en el código penal venezolano.

La falsedad ideológica, regulada en el art. 317 Código Penal, tiene que ver con la verdad del documento, con que si lo que dice el documento es cierto o no, si se ajusta o no a la realidad. La falsedad material, prevista en el art. 316 Código Penal, es cuando altero el documento, por ejemplo, si borro el nombre y le coloco otro. El legislador distingue también cuando lo hace un funcionario a cuando lo hace un particular. Por particulares la falsedad ideológica está en el art. 320 del Código Penal.

La falsificación puede ser también por supresión, tipificada en el art. 324 del Código Penal Venezolano. Hay una última distinción que es la falsedad por el uso del documento, en el art. 322 del Código Penal.

Con la evolución de las nuevas tecnologías de comunicación e información, entre las cuales nace el mensaje de datos, documento electrónico y firma electrónica, evolucionaron las formas para la falsificación de documentos, entre los cuales se afecta como se dijo la fe pública[8] esto en vista, del denominado Gobierno Electrónico, (e-Gobierno), en el que órganos y entes de la administración pública deben utilizar las nuevas tecnologías para su organización, funcionamiento y

6 Véase Boumpadre, J. Manual de Derecho Penal Parte Especial, Astrea Argentina, 2012

7 Troconis, Mendoza, J. Curso de Derecho Penal Venezolano "Comprendo parte especial" Tomo I y II, Novena Edición: Editorial "el cojo", C.A, Venezuela, 1986 p. 252

8 En referencia a las leyes las cuales otorgan fe pública a los actos que los funcionarios

relación con las personas[9]. Algunas leyes que regulan tal afirmación, Decreto con Rango, Valor y Fuerza de Ley de Mensaje de Datos y Firma Electrónica (DLMDYF), Ley de Infogobierno[10], Decreto con Rango, Valor y Fuerza de Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado[11]. Sin dejar de mencionar la Ley de Registro y Notariado[12], Ley Orgánica del Registro Civil[13].

A través del gobierno electrónico, se busca simplificar algunos pasos que requerían la presencialidad y a través de los medios tecnológicos coadyuvar a la realización de los fines del Estado.

No obstante, somos de la idea de que los Delitos informáticos, no afecta un bien jurídico sino una pluralidad de bienes jurídicos, es decir, son los denominados delitos *pluriofensivo*, que también se afecta la funcionalidad del sistema de información y comunicación.

Tipo objetivo

La LECDI, prevé en unos de sus tipos penales la falsificación documental, esta conducta realizada por medios electrónicos o telemáticos, en su artículo 12 dispone lo siguiente:

> **Artículo 12.** *Falsificación de documentos.* Quien, a través de cualquier medio, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias. Cuando el agente hubiere actuado con el fin de procurar para sí o para otro algún tipo de beneficio, la pena se aumentará entre un tercio y la mitad. El aumento será de la mitad a dos tercios si del hecho resultare un perjuicio para otro.

En primer lugar, hay que aclarar si la falsificación se da en un documento ya impreso, la responsabilidad caería a la falsificación en el código penal, es decir la ley ordinaria, y no la ley colateral (Ley Especial Contra los Delitos Informáticos), ahora si es un documento electrónico, entendemos que el ámbito de protección si corresponde a la Ley in comento.

9 Véase Sira Santana. G. Algunas notas sobre la ley de Infogobierno y el Gobierno Electrónico en Venezuela [Versión Digital] disponible en: http://redav.com.ve/redav-n-6/, 2015, p. 261-298.

10 Publicada en Gaceta Oficial N.° 40.274 de fecha 17 de octubre del 2013

11 Publicada en Gaceta Oficial N° 39.945 de fecha 15 de junio de 2012

12 Última reforma de la Ley, publicada en Gaceta Oficial N.° 6.668 Extraordinaria de fecha 16 de diciembre del 2021, en la cual regula el manejo electrónico y la firma electrónica de los registradores y notarios, artículos 24 y 25 respectivamente.

13 Publicada en Gaceta Oficial N.° 9.264, de fecha 15 de septiembre de 2009, la cual regula la utilización de mecanismo tecnológico

Antes de hablar de la falsificación de documentos en la ley especial, hay que determinar cuándo es un documento electrónico a diferencia del documento en sentido estricto.

La doctrina patria, en cabeza de Jesús Eduardo Cabrera comenta sobre el Documento (Cabrera, Jesús Eduardo, 1994)

"Conceptualizar qué es un documento en nuestro Derecho Probatorio no es tarea sencilla, porque los elementos que permiten comprenderlo y definirlo están regados sin sistematización alguna en diversas leyes" (Pág. 628-629).

Devis Echandia, excelso doctrinario en cuanto derecho probatorio colombiano comenta al respecto siguiendo a Carnelutti

(Devis Echandía, Hernando, 1970)

"En sentido estricto, documento toda cosa que sea producto de un acto humano, perceptible por los sentidos de la vista y el tacto, que sirve de prueba histórica indirecta y representativa de un hecho cualquiera" (Pág. 321). El cual puede ser declarativo-representativo, cuando contenga la declaración de quien lo crea u otorga, como lo son de un documento público o privado".

Con el auge de las tecnologías de información y comunicación en las cuales nace la contratación electrónica, la prueba digital, con el decreto con Rango, Valor y Fuerza de Ley de mensaje de datos y firmas electrónicas, se regula al respecto el carácter probatorio de los mensajes de datos, firmas electrónicas, dentro de los cuales entran los documentos electrónicos.

(Peñaranda Quintero. Héctor, 2008) define los documentos electrónicos de la siguiente manera:

"Los documentos electrónicos están en capacidad de brindar similares niveles de seguridad que el papel y, en la mayoría de los casos, un mayor grado de confiabilidad y rapidez, especialmente con respecto a la identificación del origen y el contenido de los datos, siempre que se cumplan los requisitos técnicos y jurídicos plasmados en la ley." (Pág. 121).

Soto Caldera (2001: 658), define el documento electrónico como "Toda aquella representación del pensamiento y de la voluntad del hombre materializado en soportes magnéticos de acceso inmediato, capaz de trasladarse de un lugar a otro por medio de redes telemáticas".

Entre los principios que se guía la ley se establecen los siguientes:

Equivalencia Funcional. Principio se pretende otorgar la misma validez y efectos jurídicos a la información contenida en medios electrónicos y a la información contenida en los medios tradicionales como lo es el papel

Tecnológicamente neutra. No se inclina a una determinada tecnología para las firmas y certificados electrónicos. Incluirá las tecnologías existentes y las que están por existir.

Libertad contractual. Permite a las partes la modalidad de sus transacciones, es decir, si aceptan o no las firmas electrónicas.

No discriminación del mensaje de datos firmado electrónicamente. Garantiza la fuerza ejecutoria, el efecto o la validez jurídica de una firma electrónica que no sea cuestionado por el solo motivo de que se presente bajo la forma de mensaje de datos.

Independencia de Soporte. Este principio implica que la información tendrá la validez que jurídicamente corresponda en cada caso, con independencia del soporte en que conste. El hecho de que éste sea electrónico o en papel, ha de ser indiferente a efectos de validez.

Estos principios con su carácter más procesalista que sustantivo, nos deja en claro, no hay distinción en cuanto al documento electrónico, para el tráfico jurídico en las relaciones jurídicas en cotidianidad, comercio electrónico, gobernanza electrónica, igual que el de papel, puede ser falsificado para procurarse un fin, ya sea económico, social o jurídico.

Acción Típica

Ya entrando en el tipo penal, y habiendo hecho una caracterización del documento y documento electrónico, el artículo 12 de la Ley Especial Contra los Delitos Informáticos (Desde ahora en adelante entendida como LECDI). Se tutela la creación, modificación y eliminación, de un documento que se encuentre en un sistema, esto es, un documento electrónico, que como vimos y por los principios no tiene discriminación alguna por estar en soporte digital.

La teoría del falso, la cual es utiliza en los documentos con soporte en papel, también le es aplicable a los casos de documentos electrónicos y su falsificación.

La acción típica, es crear, modificar o eliminar o que cree un documento inexistente, primero hay que acotar que, en cuanto a la creación o modificación o eliminación (Primera Parte del tipo) se habla de un documento ya existente, en donde se cree información no existía al momento de su elaboración, esto es la falsedad material en el entorno informático, cuando se altera el documento original, en el que se le atribuye a una persona distinta al otorgante, para crear, modificar o eliminar datos o información del documento, hay que haberlo obtenido previamente, por lo que en principio habría un *acceso indebido,* como delito núcleo de la Ley, se estaría quebrantando unos de las características del documento electrónico y las tecnologías de información y comunicación, el cual es la alterabilidad, confidencialidad, resguardo y privacidad de datos

Crear es un verbo transitivo que según la RAE[14] es *Producir algo de la nada,* consiste en fabricar un documento y atribuírselo a alguien diferente del otorgante[15]

Modificar verbo transitivo que la RAE[16] define como: *Transformar o cambiar algo mudando alguno de sus accidentes,* es decir de un documento ya existente se alteran sus rasgos esenciales,

14 Disponible en https://www.rae.es/drae2001/crear

15 Ídem Boumpadre. Jorge. Manual de Derecho Penal Parte Especial

16 Disponible en https://www.rae.es/drae2001/modificar

Eliminar Verbo transitivo que la RAE[17] define como: *Quitar, separar algo, prescindir de ello.* Se altera el documento prescindiendo de algún dato o información en él contenida.

En cuanto y en tanto el documento sea existente se puede modificarse y eliminarse, lo que puede denominarse falsedad parcial, si el documento se crea es lo que se denomina falsedad total.

La alteración del documento siempre es en cuanto al significado y alcance del texto, en este caso en el documento electrónico, debe darse en el sistema que utilice tecnología de información, es decir, el documento debe estar resguardado en una Computadora Personal (PC) o Laptop, también pudiera darse que se altere el documento desde un teléfono inteligente.

En su segunda parte el artículo dispone: *o incorpore a dicho sistema un documento inexistente*, es decir, el documento en forma electrónica no existe, no se encuentran en ningún sistema de información, esto es lo que se denomina falsedad total, dado que el documento que se está incorporando al sistema cuya existencia en el sistema no se encuentra, puede ser los casos del documento en soporte en papel, y se pase a la forma electrónica, en la que el destinatario no corresponda, o que el documento en papel haya sido falsificado y a través de su incorporación se le quiera dar validez a tal documento a través del sistema. Las falsificaciones informáticas, pueden ser como objeto o instrumento, si la falsificación se hace para llevar a cabo otro delito previsto en la LECDI, tal como fraude, sabotaje a sistema, etc. Entendemos , cuando el tipo habla de "cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente", se está utilizando la falsificación como instrumento, es decir se utilizan las computadoras para la finalidad la cual puede ser el fraude, posesión de equipos, espionaje informático, cuando el tipo menciona "a través de cualquier medio, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información" se está en presencia de la falsificación como objeto, la finalidad en estos casos es alterar el documento, para afectar la fe pública y la funcionalidad del sistema para los cuales fueron creados.[18]

Bien jurídico tutelado

La protección de este tipo penal, o como denomina algunos doctrinarios, el bien jurídico tutelado. No obstante un sector de la doctrina entiende lo que se tutela es el restablecimiento normativo, la norma comunica algo y al infligirse la norma se está comunicando otra cosa, en vista de eso se pena, por lo que, lo relevante no sería el bien jurídico, sino la infracción de la norma, dado que en muchos de los casos, el derecho penal actúa ya cuando ese "bien jurídico" fue lesionado o puesto en peligro, a fines didácticos, hablaremos del bien jurídico tutelado, sin dejar de mencionar la infracción de la norma y el restablecimiento de la expectativa normativa. La protección normativa de este tipo penal se encuentra consagrado en el título II que, por denominación de la ley, es "De los delitos

17 Disponible en https://www.rae.es/drae2001/eliminar

18 En cuanto a la clasificación que da las naciones unidas a las falsificaciones informáticas, puede consultarse en http://www.forodeseguridad.com/artic/discipl/disc_4016.htm

contra los sistemas que utilizan la tecnología de información" en este caso, como se dijo anteriormente se quebranta las características de las tecnologías de información y comunicación (TIC) y del documento electrónico, accediendo de manera indebida antes los sistemas.

Somos partidarios que los delitos informáticos, tutelan los sistemas para que no se dé un uso indebido y no se afecte a la colectividad y también otros bienes tutelados en la ley ordinaria, es decir, el patrimonio, honor, etc. En este tipo penal se protege como se dijo anteriormente los sistemas que utilizan tecnología de información y la fe pública, así como en los documentos en soporte de papel, dado que hay documentos en la era tecnológica se elaboran y suscriben determinados funcionarios, con el denominado gobierno electrónico y las leyes que lo regulan (Ley de Infogobierno, Decreto con Rango, Valor y Fuerza de Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado, Ley del Registro y Notariado, Ley Orgánica del Registro Civil, Ley Orgánica de la Administración Pública) y el Decreto con Rango, Valor y Fuerza de Ley de Mensajes de Datos y Firmas Electrónicas, así para particulares como funcionarios dándole amplitud a establecer la fuerza probatoria de los mensajes de datos y documentos electrónicos.

Así los bienes vitales que se tutelan son: en primer aspecto, los sistemas que utilizan las tecnologías de información y no afectar su buen funcionamiento.

La arquitectura del computador se puede dividir en Funcionamiento y Estructura[19].

Estructura: el modo en que los componentes están interrelacionados.

Funcionamiento: la operación de cada componente individual como parte de la estructura. Dentro del funcionamiento se encuentra procesamiento de datos, almacenamiento de datos, transferencia de datos y control[20].

En segundo aspecto, la fe pública en el documento electrónico. Se busca proteger la confianza en determinados actos realizados mediante las tecnologías, entre los principios que encontramos en la Ley de Mensaje de Datos y Firma Electrónica la no discriminación y la equivalencia funcional, en el que tendrá el mismo valor probatorio entre uno en soporte en papel y un documento electrónico.

En cuanto a la certificación de la firma electrónica, según la providencia N.° 004-10 emanada de Superintendencia de Certificación Electrónica (SUSCERTE)[21], establece, necesario la firma electrónica, para garantizar la autenticidad, integridad, y valor jurídico, es menester la firma electrónica certificada por un proveedor de servicios de certificación, mensaje de datos, correo electrónico y demás actuaciones semejante, para los cuales requieran consecuencia jurídica, exige el uso de la firma electrónica, así como la certificación electrónica, de esta

19 Véase Stallings. W. Organización y Arquitectura de computadores, 7ma edición: PEARSON-PRENTICE HALL, México, 2007, p. 10-11

20 Ídem Stallings. Williams. Organización y Arquitectura de computadores, p. 11

21 Publicada en la Gaceta Oficial N.° 39.432 del 26 de mayo del año 2010.

manera se exige los sistema de certificación electrónica[22] esta también puede verse alterada mediante la modificación o eliminación de la certificación de la firma.

Objeto material

El objeto material del delito donde recae la acción típica, es en los sistemas que utilizan la tecnología de información y comunicación, y en el documento electrónico que en él se contiene, dada las funcionalidades del sistema que puede ser afectada mediante la acción típica, así como los caracteres del documento electrónico.

Tipo subjetivo

Es un tipo penal, que puede ser cometido bajo la modalidad dolosa, entendiendo el dolo como conocimiento y voluntad, como es entendido modernamente por la doctrina mayoritaria, sin dejar de mencionar el dolo normativo-atributivo[23] que ha sido desarrollado por un sector de la doctrina. La falsificación informática requiere el dolo, acepta las tres modalidades de dolo, es decir, el dolo de primer grado o dolo directo, dolo de segundo grado o de consecuencias necesarias y el dolo de tercer grado o dolo eventual[24].

Sujetos

Los sujetos que pueden ejecutar la acción típica, es indeterminado, la ley no establece una cualidad o determinación en cuanto quien pueda ejecutar el verbo rector, pero están en el contexto informático o telemático, podrá ser un Hackers o Crackers para determinadas circunstancias que ameriten en manera de acceder al sistema, se utiliza el vocablo de *hacking,* relacionado a acceso indebido.

Por lo que nos atrevemos afirmar si bien, no establece una cualidad debe ser realizada por los Hackers o Crackers, para determinados fines.

La contextualización de estos términos

> *Hackers:* "es una persona que, por simple curiosidad, invade a sistemas operativos, bases de datos, los actos que realiza la toma como un reto intelectual, más no por causar daños a terceros. Estas personas son capaces de

22 En este sentido véase, Silva Dugarte. María F. Certificación electrónica aplicada en Venezuela y su legislación: garantías y desventajas para negociaciones seguras, Visión Gerencial, [Versión digital, consultado el 04/02/2022] nro 1, 2011, p. 207-220.

23 Véase para ampliar este tema a Pérez. Barberá, G. El concepto de dolo en el derecho penal. Hacia un abandono definitivo de la idea de dolo como estado mental [Versión electrónica] Cuaderno de Derecho Penal, N.° 6, Argentina, 2012.

24 En Venezuela a través de jurisprudencia se ha aceptado el dolo eventual, para ello véase Sentencia N.° 1703 de Sala de Casación Penal en ponencia del Magistrado Angulo Fontiverios (Caso: Roberto Alexander Terán), Sentencia N.° 302 de Sala de Casación Penal en ponencia de la Magistrada Deyanira Bastidas (Caso: Carlos Eduardo Hernández)

> inventar su propio software para vulnerar las seguridades de la información. No buscan ganancias económicas[25].
>
> *Cracker*: "personas que se introducen en sistemas remotos con la intención de destruir los datos denegar el servicio a usuarios legítimos y en general a causar problemas. El pirata informático tiene dos variantes. (Borrando, dañando o revelando información por lo general son exempleados) los motiva la curiosidad y la venganza[26].

Cabe acotar, que puede caer la responsabilidad jurídica en una persona jurídica, si el hecho fue realizado por uno de sus socios o director, esto en tenor del artículo 5 de la ley especial. Por lo que la responsabilidad puede ser en una persona natural (la cual en principio sería indeterminado, pero normalmente es llevada por personas especialidad en la materia, como lo sería un Cracker o Hackers) o persona jurídica en sentido estricto.

El sujeto pasivo, en el que puede recaer la acción puede ser cualquier persona natural o jurídica, ente u órgano con forma de derecho público o privado, en que se utilice los sistemas de tecnología y de información. Anteriormente vimos, a través de diferentes disposiciones legales, se busca un gobierno electrónico (Gobierno-e), en el que, se busca la interoperabilidad entre los Poderes Públicos y así con los particulares, así que pueden ser sujeto pasivo del delito, cualquier ente u órgano del estado que utilice los sistemas de tecnología e información, así como los particulares.

Clasificación de la falsificación informática

En la clasificación de los delitos por su resultado, existen los delitos de resultado y de mera actividad

Delitos de Resultado también denominado Delito Material: Exigen una modificación del mundo exterior perceptible por los sentidos y diferenciable en el tiempo y espacio del comportamiento del autor.

Delitos de Mera actividad también denominado Delito Formal: Aquí el delito se consuma una vez realizada la acción, no requiere de un resultado. Es un delito de mera actividad, en el que la acción típica coincide con el resultado, al no dividirse la ejecución en diferentes momentos, es decir, es un delito *unisubsistente*, por lo que no admitiría tentativa.

Es un delito de lesión y no de peligro, por lo que requiere que se haya afectado el bien jurídico para su punibilidad.

25 Véase Villalobos, Edgardo. "Diccionario de derecho informático", Editorial Litho, Editorial Chen S.A., Panamá, Panamá, 2002, pag.54.

26 También denominados "Sombreros Negros", buscan sistemas, programas, manipulan, acceden, interceptan información, de manera malintencionadas, puede consultarse https://protecciondatos-lopd.com/empresas/cracker-informatico/ y https://ayudaleyprotecciondatos.es/2021/10/18/cracker/

Conclusión

En medida que se implemente con más apego el uso de las nuevas tecnologías en la cotidianidad venezolana, estos hechos cobraran más relevancia, nuestra LECDI una Ley novedosa para la época y a nuestra manera de ver muy bien estructurada para la época de su elaboración, sistemáticamente dispuso en sus articulados los hechos en lo que pudieran estar inmersos sujetos con el uso de las tecnologías, en el caso que nos ocupa de las falsificaciones informáticas, para atentar contra la fe pública o incluso contra los sistemas que utilizan la tecnologías de información.

Las nuevas tecnologías son una realidad para la vida cotidiana de las personas, con el gobierno electrónico en el que se utilizan estas formas de comunicación para la prestación de servicios, a manera de reflexión habría que reforzar la ciberseguridad, adiestrando al personal que hace uso de las tecnologías aprovechar todas las bondades que nos brindan estos sistemas.

De Lege refrenda, queremos aportar a la LECDI, incorporar la palabra "manipulación" como verbo rector del tipo similar a la fórmula del fraude de la ley ejusdem, pero en relación a la manipulación del sistema y que con esta se busque crear, modificar o eliminar los datos o información del documento o que cree uno inexistente cuando hace referencia a las falsificaciones informática, de modo, que su texto legal quede redactado "Quien mediante del uso de manipulaciones de cualquier tipo, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente" a nuestro modo de ver abarcaría aún más la conducta típica en estos hechos, donde normalmente, primer se manipula el sistema ya sea para acceder al documento o incluso en la modificación o eliminación de la información en el contenida. También abarcaría cuando se éste manipulando el sistema, pero en el uso de una Inteligencia Artificial (IA), la cuales se abarca el uso del robot como forma tecnológica.

Dada las diversas modalidades en la que puede ser utilizada la falsificación informática, esto es como objeto o como instrumentos, y la relación que tienen cada uno de estos hechos en la LECDI en donde normalmente se puede estar en presencia de un concurso de delitos sugerimos el uso de firewall, el uso de cursos especializados en la materia a los diferentes integrantes del gobierno electrónico

Referencias Bibliográficas

Cabrera. Romero, J. E. (1994). Algunas apuntaciones sobre el artículo 433 del Código de Procedimiento Civil, en Liber Amicorum *Homenaje a la obra científica y docente del profesor José Muci Abraham*, Editorial Jurídica Venezolana.

Bacigalupo. E. (2002). Documento electrónicos y delitos de falsedad documental, *Revista Electrónica de Ciencia Penal y Criminología* [Versión digital].

Boumpadre, J. (2012). *Manual de Derecho Penal Parte Especial*, Astrea.

Carrara, F. (1996). *Programa de Derecho Penal.* Parte Especial 5º edición revisada, t. IX, Temis.

Devis Echandia. H. (1970). *Teoría General de la Prueba Judicial*, Tomo II, Victor. P de Zavalia.

Figari. R. (2014). *Delitos Contra la Fe Pública, Asociación Pensamiento Penal,* Comentarios al Código Penal de Acceso Libre [Versión digital] https://www.pensamientopenal.com.ar/cpcomentado/40205-art-282-291-delitos-contra-fe-publica

Pessina. E. (1884). *Elementi dei Diritto Penale,* vol. III. (s.d.).

Peñaranda Quintero. H. (2008). El Documento Electrónico, Editorial de La Universidad del Zulia

Pérez. Barberá, G. (2012). El concepto de dolo en el derecho penal. Hacia un abandono definitivo de la idea de dolo como estado mental [Versión electrónica] Cuaderno de Derecho Penal, N.° 6.

Silva Dugarte. María F. (2011). Certificación electrónica aplicada en Venezuela y su legislación: garantías y desventajas para negociaciones seguras, Visión Gerencial, [Versión digital] nro 1.

Sira Santana. G. (2015). *Algunas notas sobre la ley de Infogobierno y el Gobierno Electrónico en Venezuela* [Versión Digital]

Soto Caldera, M. M. (2001). "Consideraciones sobre la prueba documental electrónica en el proceso civil venezolano". Estudios de derecho civil. Vol. III. *Libro homenaje a José Luis Aguilar Gorrondona.* Tribunal Supremo de Justicia. Colección Libros homenaje Nro. 5.

Stallings. W. (2007). *Organización y Arquitectura de computadores,* 7ma ed. Pearson-Prentice Hall.

Troconis, Mendoza, J. (1986). *Curso de Derecho Penal Venezolano* "Comprendo parte especial" Tomo I y II, Novena Edición: Editorial "el cojo", C.A, Venezuela.

INFORMÁTICA Y DERECHO

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO
(SEGUNDA ÉPOCA)

FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES
DE DERECHO E INFORMÁTICA

ISSN 2530-4496 – N.º 13, 2023, PP. 119-132

LA ORDEN DE CONSERVACIÓN DE DATOS: UNA MEDIDA DE ASEGURAMIENTO DE FUENTES DE PRUEBA IMPRESCINDIBLE PARA LA INVESTIGACIÓN DE LOS DELITOS DE ODIO COMETIDOS EN LÍNEA

THE DATA PRESERVATION ORDER: AN ESSENTIAL MEASURE TO SECURE SOURCES OF EVIDENCE FOR THE INVESTIGATION OF HATE CRIMES COMMITTED ONLINE

Juan Alejandro Montoro Sánchez[1]

Investigador Posdoctoral Margarita Salas. Universidad Pablo de Olavide de Sevilla

1 Trabajo vinculado al Proyecto de Investigación de Excelencia del Ministerio de Economía y competitividad «Límites a la utilización de datos, evidencias e información entre procesos y procedimientos diversos en España y la Unión Europea (LUDEI)». Esta publicación ha sido financiada por la Unión Europea "NextGenerationEU", por el Plan de Recuperación, Transformación y Resiliencia y por el Ministerio de Universidades, en el marco de las ayudas Margarita Salas, para la Recualificación del sistema universitario español 2021-2023 convocadas por la Universidad Pablo de Olavide, de Sevilla

Resumen

El presente trabajo aborda el estudio de la regulación de la orden de conservación de datos prevista en el art. 588 octies *LECrim*, como medida idónea de aseguramiento de fuentes de prueba a disposición de la Policía Judicial y del Ministerio Fiscal para garantizar la eficacia de la investigación de los delitos de odio cometidos en línea.

Palabras clave

Ciberdelitos de odio, orden conservación datos, investigación del delito.

Abstract

This paper studies the regulation of the data preservation order provided for in art. 588 octies LECrim, as a suitable measure for securing sources of evidence at the disposal of the Judicial Police and the Public Prosecutor's Office to guarantee the effectiveness of the investigation of hate crimes committed online.

Keywords

Cyber hate crime; data preservation order; crime investigation.

Los delitos de odio cometidos en línea: un preocupante fenómeno creciente

La Organización para la Seguridad y la Cooperación en Europa, como institución encargada de supervisar los delitos de odio y la incitación al odio, define a éstos como cualquier infracción penal donde la víctima, el local o el objetivo de la infracción se elija por su (real o percibida) conexión, simpatía, filiación, apoyo o pertenencia a un grupo basado en una característica común de sus miembros, como su raza real o perceptiva, el origen nacional o étnico, el lenguaje, el color, la religión, el sexo, la edad, la discapacidad intelectual o física, la orientación sexual u otro factor similar[2]. En nuestro Código Penal, son diversas las modalidades de tipos delictivos los que pueden ser calificados como auténticos delitos de odio, constituyéndose el art. 510 CP (Código Penal) como el principal de éstos, sin perjuicio de que asimismo puedan considerase como tales los catalogados en los arts. 170.1; 173.1; 174; 314; 511 y 512; 515.4 y 522 a 525 del mismo texto legal.

De acuerdo con las últimas estadísticas publicadas por la Oficina Nacional de Lucha contra los Delitos de Odio en el "Informe de la Evolución de los Delitos de Odio en España" correspondiente al ejercicio 2021[3], se contabilizaron en éste un total de 1802 hechos delictivos de odio por las Fuerzas y Cuerpos de Seguridad del Estado, bien por mediar la interposición de una denuncia, bien por tener constancia durante el desarrollo de sus labores propias. Esta cifra, que en términos absolutos puede parecer reducida, supone un nada desdeñable incremento del 28,62 % de los delitos conocidos en el año anterior, en el que se contabilizaron un total de 1401[4]. En cualquier caso, es imprescindible apuntar que esta cifra solo representa la punta del iceberg de la situación real, ya que se considera que la mayor parte de los delitos de esta índole que se cometen no se llegan a conocer oficialmente, lo que impide la inclusión en las estadísticas oficiales[5]. De hecho, la

2 Esta es la definición utilizada por la OSCE en sus informes sobre los delitos de odio motivados por el racismo y la xenofobia (2021), los delitos de odio por motivos de género (2021), los delitos de odio por motivos de antisemitismo (2019) y los delitos de odio por motivos de islamofobia (2018), basados en la Decisión n.º 9/09 del Consejo Ministerial de la OSCE, de 2 de diciembre de 2009, sobre la lucha contra los delitos de odio, acordada por consenso por todos los Estados de la OSCE, incluidos todos los Estados miembros de la UE.

3 Disponible en https://www.fiscal.es/memorias/memoria2021/FISCALIA_SITE/index.html. (Fecha de consulta 15 de enero de 2023)

4 La Memoria de la Fiscalía General del Estado de 2019 ya era consciente tales incrementos, que se vienen repitiendo con más intensidad desde entonces y afirma incluso que "Si en la Memoria del año pasado comenzábamos haciendo referencia a un incremento de los denominados delitos de odio, tanto de las agresiones por motivos racistas, xenófobos, antigitanos, homófobos y otras formas de intolerancia y discriminación, como del discurso de odio en internet y las redes sociales, ahora podemos decir que no hay un día en que los medios de comunicación no relaten hechos que, con mayor o menor fortuna, entienden ser delitos de odio". Disponible en https://www.fiscal.es/memorias/memoria2019/FISCALIA_SITE/index.html. (Fecha de consulta 15 de enero de 2023).

5 TAMARIT SUMALLA, J. M., "Los delitos de odio en las redes sociales", *Revista de Internet, Derecho y Política*, núm. 27, 2018, p. 18.

Agencia Europea de Derechos Fundamentales estima que el 80 % de los delitos de odio no son denunciados por las víctimas y, por tanto, no llegan a conocerse[6].

En el mismo informe elaborado por la Oficina Nacional de Lucha contra los Delitos de Odio se informa que un total de 232 de todos los delitos de odio de los que se tuvo constancia en 2021 fueron cometidos a través de las TIC (Tecnologías de la Información y Comunicación) o valiéndose de instrumentos tecnológicos, siendo los delitos vinculados a la ideología, racismo, orientación sexual e identidad de género los que presentan una mayor incidencia en este concreto ámbito[7]. Este dato representa un porcentaje del 16,55 % respecto al total de los delitos de esta naturaleza, lo que supone, a su vez, un nada desdeñable incremento del 22,75 % respecto al ejercicio anterior, dato que evidencia una notoria tendencia alcista de esta vía comisiva. Cifras, ambas, que por ser muy significativas han merecido la preocupación de diversas instituciones implicadas en la lucha contra esta lacra. Por ejemplo, la Fiscalía General del Estado en su Memoria correspondiente al ejercicio 2018 ya advertía de esta creciente problemática por las facilidades que ofrecen las TICS para publicitar contenidos relativos al discurso del odio o para permitir la comisión de estas modalidades delictivas[8], de las que se deriva un incuestionable y perverso efecto sobre los valores y principios que inspiran nuestro modelo de convivencia[9]. Mientras en la más reciente Memoria de la FGE de 2021, elaborada una vez superada la pandemia por COVID19, se menciona que dado que las actividades de todo orden que desarrollan los ciudadanos se vieron intensamente limitadas y la interacción social fuertemente restringida, particularmente durante la vigencia de las medidas más estrictas de confinamiento, buena parte de las relaciones entre las personas y los grupos sociales se desarrollaron no de forma directa y personal sino a través de las TIC y redes sociales, factor que propició un aumento de los delitos de odio producidos a través de las tecnologías digitales de la información y la comunicación[10].

6 Se recomienda la lectura del apartado 12.7 de las Estadísticas de la Memoria anual de la Fiscalía General del Estado del año 2019, en el que se ponen de manifiesto algunos de los factores adicionales que impiden ofrecer una cifra más realista de las estadísticas en esta materia. De hecho, se enfatiza en la existencia de un problema estadístico sobre estos delitos que impide la obtención de una visión realista de su alcance en la sociedad.

7 Adviértase nuevamente que estas cifras no revelan la realidad. La Memoria FGE de 2019 se hace eco del hecho de que las redes e internet se encuentran llenas de mensajes de odio y de incitación al odio, unos más o menos espontáneos, otros muy organizados, sin embargo la estadística no depende tanto de su número tanto como de las denuncias y del rastreo que se pueda hacer en las redes por las Fuerzas y Cuerpos de Seguridad del Estado o la Administración.

8 Con anterioridad, la Memoria de la FGE de 2017 ya recogió un incremento de las denuncias por delitos de odio a través de internet y las redes sociales, pasando de 40 en 2015 a 99 en 2016. Disponible en https://www.fiscal.es/memorias/memoria2017/FISCALIA_SITE/index.html. (Fecha de consulta 15 de enero de 2023).

9 Pues como ya advirtió el Tribunal Supremo en su STS de 4 de mayo de 2015, "los valores de antirracismo o la tolerancia ideológica y religiosa son esenciales de la convivencia…".

10 Disponible en https://www.fiscal.es/memorias/memoria2021/FISCALIA_SITE/index.html. (Fecha de consulta 15 de enero de 2023).

Del total de los 232 delitos de odio denunciados en 2021 que se produjeron por vía telemática, un 37,83 % se cometieron a través de internet mediante publicaciones insertadas en páginas webs, blogs o foros. El 22,29 % de las denuncias se referían a publicaciones vertidas o mensajes proferidos en cualquiera de las distintas y numerosas redes sociales existentes. Con una cifra muy cercana a la anterior, esto es, con un 25,22 % se posicionarían los delitos de odio cometidos a través de vía telefónica, categoría que aglutina a los ilícitos cometidos mediante llamadas telefónicas o bien valiéndose de la mensajería tradicional (SMS, MMS) o de la instantánea a través de alguna de las distintas aplicaciones OTP que permiten este tipo de comunicación. Y en último lugar, con un 5,28 % de incidencia, se encontrarían los delitos cometidos a través de medios de comunicación, esto es, a través de publicaciones localizadas en diarios, rotativos y revistas que presentan una edición digital.

Vistos los anteriores datos, puede concluirse sin temor a duda que las tecnologías de la información y comunicación se han convertido tanto en un instrumento, como en un medio habitual para la comisión de acciones delictivas vinculadas al discurso del odio en cualquiera de las diferentes modalidades que encuentran acomodo en el código Penal. La facilidad de acceso a los medios tecnológicos y la sencillez de publicación de contenido en la red, el aparente anonimato que posibilitan estos medios, la desinhibición con la que los usuarios actúan y el desarrollo de identidades disociativas son factores que favorecen y propician que en estos canales se produzca la difusión o emisión de contenidos que incitan al odio, a la violencia o la discriminación respecto de individuos que son diferentes por su raza, religión, nacionalidad, sexo, orientación sexual, enfermedad o por su mera ideología[11].

Estas circunstancias no resultan baladíes para el desarrollo de las labores de investigación llevadas a cabo por las autoridades públicas competentes dirigidas al esclarecimiento de los hechos delictivos y la determinación de sus verdaderos, con miras al posterior ejercicio del *ius puniendi*. De hecho, lo cierto es que la utilización de estas vías comisorias condiciona sobremanera las técnicas y medidas que las autoridades deben emplear para la obtención exitosa del material probatorio requerido para la acreditación de los hechos tipificados. Pero muy especialmente, estos cada vez más habituales canales delictivos influyen en el tiempo de reacción que se precisa para la práctica de las primeras diligencias destinadas a recolectar los efectos del delito y las fuentes de prueba pertinentes, puesto que un grado notable de la eficacia de los iniciales actos de prevención o investigación va a depender de la inmediatez con la que se ejecuten tras el momento de la comisión del delito o, en su caso, de la toma de conocimiento de la *notitia criminis*. Piénsese que la información y los datos electrónicos que se albergan en la red, y particularmente aquellos que se generan voluntariamente en ciertos espacios de encuentro, redes sociales o aplicaciones de comunicación se caracterizan precisamente no ya por la facilidad con que pueden alterarse, si no por la extremada sencillez con la que pueden ser objeto de supresión o incluso

11 GONZÁLEZ JIMÉNEZ, A., "Implicaciones jurídicas de los usos y comentarios efectuados a través de las redes", *Revista de Internet, Derecho y Política*, núm. 27, p. 19.

destrucción[12]. Tan sencillo y rápido es publicar un comentario de odio dirigido a una persona o colectivo en una multitudinaria red social, a través de una entrada de blog o en una revista digital como proceder a su inmediato borrado, eliminando cualquier huella aparente de su previa existencia. De hecho, la doctrina ha destacado a la volatilidad como una de las notas características e inherentes que presenta la información de carácter electrónico[13].

Por tanto, en los supuestos en los que produzca la interposición de una denuncia por la comisión de delito de odio a través de la publicación de contenido ofensivo en la red, es esencial que las primeras diligencias de investigación destinadas a la obtención de rastros y evidencias se desarrollen de forma apresurada y ágil, a fin de sortear los riesgos de alteración o supresión que acechan y que podrían dificultar, *a priori* y sin perjuicio de que se desarrollen otras diligencias más complejas, la constatación del delito. Asimismo, hay que advertir, que tales riesgos no dependen exclusivamente de la voluntad del sujeto responsable, si no que pueden tener origen, incluso, en la propia actividad del titular del medio o canal electrónico en el que se incorpore el contenido ofensivo. Por ejemplo, piénsese en aquellos supuestos en que medie una denuncia interna de la propia víctima o de otros usuarios que han tenido acceso al contenido ilícito y el proveedor del sitio web procede a eliminar o restringir el acceso para minimizar sus efectos lesivos y evitar cualquier tipo de responsabilidad como prestador, según las disposiciones establecidas en los arts. 10 y siguientes de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Ahora bien, debe tenerse en cuenta que gran parte de la investigación de estos delitos comienza por la denuncia que se interpone en dependencias policiales. Sin embargo, la solicitud o requerimiento de entrega de datos e información a los prestadores de servicios de comunicaciones electrónicas o de la sociedad de información, en tanto titulares de las plataformas o redes sociales en las que se almacenan y desde las que se difunden las manifestaciones y declaraciones de odio, requiere ineludiblemente de la pertinente autorización judicial dada la consecuente injerencia en ciertos derechos fundamentales de los individuos titulares de la información, como por ejemplo, en los derechos a la intimidad personal o a la protección de datos. Piénsese, por ejemplo, en los datos electrónicos conservados por los prestadores de servicios en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas o por propia iniciativa con fines comerciales o, los datos almacenados en servidores y equipos, cuya entrega requiere preceptivamente la respectiva autorización judicial

12 La STS 300/2015, de 19 de mayo afirma que "la posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas". No obstante, a pesar de esta mutabilidad, lo cierto es que como contrapartida, la información digital o electrónica también se caracteriza por su trazabilidad, es decir, por la posibilidad de rastrear la huella de la misma a través de los registros que se generan y conservan en los sistemas informáticos por razón de su uso.

13 Por ejemplo, DELGADO MARTÍN señala que "la prueba electrónica ostenta frecuentemente la característica de la volatilidad, es decir, la información o datos relevantes son mudables y sometidos a constante cambio, especialmente en relación con los contenidos de Internet". DELGADO MARTÍN, J., "La prueba electrónica en el proceso penal", *Diario La Ley*, núm. 8167, 2013.

de conformidad con lo dispuesto en los arts. 588 *ter* j) y 588 *septies* a) LECrim. En consecuencia, los agentes de la Policía Judicial no están facultados en la mayoría de los supuestos, para solicitar y requerir coercitivamente, por sí mismos, a los proveedores de servicios electrónicos a que entreguen los datos y la información que constituyen a todas luces, las fuentes de prueba del delito, sino que requieren que con carácter previo el juez de instrucción competente autorice dicha entrega, previa solicitud y de conformidad con los presupuestos y requisitos de la concreta diligencia de investigación que proceda en cada caso. De forma análoga, los miembros del Ministerio Fiscal también ven limitada su capacidad de actuación y maniobra en estos supuestos cuando se encuentren al frente de una investigación preliminar por mor de la recepción de una *notitia criminis* por la comisión de un delito de odio y deben de acudir consecuentemente al juez de instrucción para obtener información relativa a las comunicaciones electrónicas o a servicios de la sociedad de la información.

Esta limitación de las facultades indagatorias a la que se enfrentan las fuerzas policiales y el Ministerio Fiscal podría derivar en la frustración, o al menos disminución de la capacidad de obtención de las fuentes de prueba necesarias para el buen fin de la investigación de ciertas conductas delictivas cometidas en la red, pues el dictado y entrega de la preceptiva autorización judicial puede requerir de un lapso de tiempo superior a las veinticuatro horas previstas en el art. 588 bis c) LECrim, con el riesgo que dicha demora conlleva. Adviértase que se requiere de la traslación de la oportuna denuncia al Juzgado de Instrucción junto a la solicitud de adopción de actos de la investigación necesarios conforme a lo establecido en el art. 588 bis c) LECrim y el posterior examen del juez antes de que se proceda al dictado de la resolución habilitante, debiendo asimismo ser notificada posteriormente al prestador de servicios.

Para evitar estas situaciones, es por lo que el ordenamiento procesal ha previsto un instrumento jurídico de aseguramiento de fuentes de prueba que permite evitar la desaparición de datos o información de las bases de datos, de entre otros sujetos, proveedores de servicios de comunicaciones electrónicas o de la sociedad de la información, en tanto en cuanto se obtiene la resolución judicial autorizante de la diligencia de investigación: la denominada en nuestra Ley de Enjuiciamiento Criminal como orden de conservación de datos o en el ámbito convencional como orden rápida de conservación de datos o *quick freeze data*. Herramienta que como se va a comprobar a continuación, se convierte en una aliada imprescindible de las autoridades policiales y del Ministerio Fiscal para garantizar la disponibilidad e integridad de la información almacenada en sistemas y archivos informáticos de terceros, que resulte necesaria para la persecución e investigación de los delitos de odio que se cometen a través de la red o mediante la utilización de medios electrónicos.

Regulación de la orden de conservación de datos

Enmarcado en el Capítulo X del Título VIII del Libro II de la Ley de Enjuiciamiento Criminal se localiza el art. 588 *octies*, precepto introducido por la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento

Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica[14] con la finalidad de instaurar un nuevo instrumento procesal para el aseguramiento de fuentes de prueba de naturaleza electrónica y al que se ha denominado orden de conservación de datos. Esta novísima herramienta jurídica de gran utilidad práctica y que contribuye notablemente a mejorar la eficacia de las investigaciones relacionadas con los ciberdelitos, halla su origen y configuración en la llamada diligencia de conservación rápida de datos informáticos almacenados prevista en los arts. 16 y 17 del Convenio del Consejo de Europa sobre Ciberdelincuencia de 23 de noviembre de 2001[15]. Instrumento está destinado a asegurar que las autoridades competentes de los Estados parte puedan conseguir de forma ágil y rauda la conservación de datos electrónicos almacenados en un sistema informático[16], especialmente, cuando éstos resulten particularmente susceptibles de una inminente pérdida o modificación[17]. Así pues, con la incorporación a la LECrim de la diligencia de conservación de datos a través del art. 588 *octies*, el legislador nacional dio efectivo cumplimiento a los compromisos asumidos en los referidos preceptos del Convenio de Budapest.

En virtud de esta medida de aseguramiento de fuentes de pruebas, tanto el Ministerio Fiscal como la Policía Judicial se encuentran legitimados[18] para requerir y ordenar, de forma autónoma y sin necesidad de previa orden judicial[19], a un sujeto a que conserve incólume y proteja un dato, un conjunto de

14 «BOE» núm. 239, de 6 de octubre de 2015. BOE-A-2015-10725.

15 También conocido como Convenio de Budapest sobre Ciberdelincuencia, por ser la ciudad en la que tuvo lugar su firma. Fue ratificado por España el anterior 20 de mayo de 2010 y cuyo Instrumento de Ratificación fue publicado en el «BOE» núm. 226, de 17 de septiembre de 2010. BOE-A-2010-14221.

16 OTAMENDI ZOZAYA, F., *Las últimas reformas de la ley de enjuiciamiento criminal: una visión práctica tras un año de vigencia*, Dykinson, Madrid, 2017, p. 147.

17 ASENSIO GALLEGO, J. M., "Los delitos informáticos y las medidas de investigación y obtención de pruebas en el convenio de Budapest sobre la ciberdelincuencia", *Justicia penal y nuevas formas de delincuencia*, dir. J. M. Asensio Mellado, Tirant lo Blanch, Valencia, 2017, p. 56.

18 Nada obsta, a que también el Juez de Instrucción pueda dictar una orden de conservación de datos, por ejemplo, cuando se encuentre a expensas del resultado de otras medidas de investigación acordadas, evitando de este modo la adoptación de medidas limitativas de derechos fundamentales y garantizando la disponibilidad de los datos que potencialmente pueden ser útiles para el esclarecimiento del delito.

19 Sostiene la Fiscalía General del Estado, en la Circular 1/2019, de 6 de marzo, de la Fiscal General del Estado, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológicas en la Ley de Enjuiciamiento Criminal, que por no exigir su dictado orden judicial, la orden de conservación de datos no requiere una motivación especial para garantizar su validez, sin perjuicio de la necesariedad de justificar sucintamente la necesidad de acordar la conservación para posibilitar la eficacia de una ulterior medida que se solicite. De este modo, su validez estaría condicionada a que indicara además, los datos que deben ser conservados, el plazo de conservación y el destinatario de la orden, así como las prevenciones oportunas que permitan la posterior exigencia de responsabilidad penal por delito de desobediencia en caso de no ser atendida la solicitud o no ser respetado el deber de sigilo y reserva que el precepto establece. En este punto, discrepamos de tal parecer y consideramos imprescindible como parte de su

éstos o cierta información concreta y delimitada que se albergue en un sistema informático o de almacenamiento electrónico que se halle bajo su disposición y control, y ello con el objeto de evitar su eliminación o alteración voluntaria o automatizada en tanto en cuanto se obtiene la autorización judicial necesaria que disponga y ordene su ulterior entrega de conformidad con la específica regulación de la diligencia de investigación que se requiera de las previstas en la Ley de Enjuiciamiento Criminal o en cualquier otro instrumento normativo, incluso de cooperación judicial[20]. Y es que se trata de una diligencia de aseguramiento trascendental no solamente en el marco de la investigación de la ciberdelincuencia nacional, sino destinada a jugar un papel fundamental en el ámbito de la cooperación judicial internacional, que es el entorno inspirador del Convenio de Budapest. Por ello la Convención de Budapest prevé en sus arts. 29 y 30 que un Estado parte pueda solicitar a otro que ordene la conservación rápida de datos almacenados por medio de un sistema informático que se encuentre en el territorio de ese otro Estado, respecto de los cuales el Estado requirente tenga la intención de presentar una solicitud de asistencia mutua con vistas al registro o acceso de forma similar, confiscación, obtención o revelación de datos. Es, por tanto, una medida que permite garantizar la inmovilización de ciertos datos que pretenden ser incorporados al proceso como medio de prueba o para su análisis forense, en tanto en cuanto se logre concluir la diligencia judicial requerida para su entrega, sin que se vea frustrada por la eventual desaparición, alteración o deterioro de los datos[21].

La orden de conservación puede tener por objeto la conservación de cualquier modalidad de dato o de información que se halle previamente almacenado en un sistema informático o de almacenamiento[22], pudiendo incluso extenderse a los

contenido, la motivación, siquiera mínima, relativa a la justificación, necesidad y proporcionalidad de la medida, atendiendo las circunstancias del caso, los indicios existentes, los principios rectores de las medidas de investigación y especialmente a la posible contribución de los datos bloqueados a la investigación.

20 ASENSIO GALLEGO, J. M., «Los delitos informáticos y las medidas de investigación y obtención de pruebas en el convenio de Budapest sobre la ciberdelincuencia»…, *op. cit.*, p. 57.

21 El art. 16.1 del Convenio sobre Ciberdelincuencia justifica la razón de ser de esta medida en aquellos supuestos en los que existan razones para creer que los datos informáticos resultan especialmente susceptibles de pérdida o de modificación. Lo que justifica QUEVEDO GONZÁLEZ en la vulnerabilidad de las evidencias electrónicas y la posibilidad de que sean destruidas o modificadas bien sea de forma intencional o por procesos automáticos predeterminados. De este modo su posterior aportación como medio de prueba o, en su caso, su análisis forense no se verá frustrado por la desaparición, alteración o deterioro de unos elementos inherentemente volátiles. QUEVEDO GONZÁLEZ, J., *Investigación y prueba del ciberdelito* (tesis doctoral), Universidad de Barcelona, 2017, p. 192. Disponible en https://www.tdx.cat/bitstream/handle/10803/665611/JQG_TESIS.pdf?sequence=1&isAllowed=y. (Fecha de consulta 16 de enero de 2023).

22 Nótese que el art. 588 octies LECrim se refiere de manera genérica a "datos o informaciones concretas", sin establecer ningún tipo de límite en cuanto a la naturaleza de los datos objeto de conservación. La Circular 1/2019, de 6 de marzo, de la Fiscal General del Estado, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológicas en la Ley de Enjuiciamiento Criminal, también mantiene un criterio amplio y señala como posibles datos objetivo de la orden a: "El contenido de

datos alojados en servidores externos o en sistemas *cloud* o virtuales[23]. Además, no debe haber inconveniente legal en que la orden de conservación no se refiera exclusivamente a datos previamente conservados, sino que también conmine a la conservación de datos adicionales cuya generación o captación sea posterior a su emisión, ya de forma inminente o previsible durante el plazo por el que se extienda la medida, evitando con ello la reiteración de sucesivas órdenes en el tiempo conforme se va generando información susceptible de aprehensión[24].

La orden de conservación puede instarse en el desarrollo de la instrucción de cualquier delito tipificado en el Código Penal para la que pueda requerirse acceso a datos electrónicos, sin que exista ningún tipo de limitación legal que atienda a la modalidad delictual o a su gravedad. No obstante, debe tenerse en cuenta que la posterior diligencia de investigación que se tramite para que se acuerde la entrega efectiva de los datos al órgano judicial para su incorporación a los autos, si se sujetará a los presupuestos y demás exigencias que le sean propios. Por tanto, es la posterior entrega de los datos, la que se encontrará supeditada al cumplimiento de los requisitos exigidos en la legislación procesal para la práctica de la medida de investigación que se utilice para conseguir su cesión de los sistemas informáticos del proveedor a las autoridades penales competentes.

comunicaciones telefónicas y telemáticas (art. 588 ter b). Los datos electrónicos de tráfico o asociados a procesos de comunicación, así como los que se produzcan con independencia del establecimiento o no de una concreta comunicación (art. 588 ter b). Los datos electrónicos, diferentes de los anteriores, conservados por los prestadores de servicios o personas que faciliten la comunicación en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas o por propia iniciativa por motivos comerciales o de otra índole (arts. 588 ter j, k, l y m). Los datos contenidos en ordenadores, instrumentos de comunicación telefónica o telemática, dispositivos de almacenamiento masivo de información digital o repositorios telemáticos de datos (arts. 588 sexies a, a 588 septies a). Se comprenden, en consecuencia, tanto los datos de tráfico y accesorios cuyo deber de conservación entre ya dentro de las obligaciones que el art. 3 de la Ley 25/2007, de 28 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones impone a los operadores de comunicaciones electrónicas, como cualesquiera otros que pudieran encontrarse almacenados en un sistema accesible o no por el investigado (entre los primeros, su correo electrónico o su cuenta de almacenamiento en la nube; entre los segundos, los datos almacenados en redes sociales, por ejemplo)". No obstante, en este sentido, discrepamos de la posibilidad de que dicho instrumento sea utilizado para conservar preventivamente el contenido material de las comunicaciones que se mantengan por vía telefónica, habida cuenta de que las mismas no son objeto de registro y almacenamiento simultáneo en un archivo o base de datos.

23 RAYÓN BALLESTEROS, M. C., "Medidas de investigación tecnológica en el proceso penal: la nueva redacción de la Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015", *Anuario jurídico y económico escurialense*, núm. 52, 2019, p. 203.

24 En cambio, el criterio de la Fiscalía General del Estado plasmado en la Circular 1/2019, de 6 de marzo, de la Fiscal General del Estado, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológicas en la Ley de Enjuiciamiento Criminal, parece que. La medida se va a referir, siempre, a datos que ya existen y están almacenados, parece rechazar que puedan ser objeto de una orden de conservación los datos pendientes de generación, al indicar que "La medida se va a referir, siempre, a datos que ya existen y están almacenados".

La orden de conservación puede dirigirse no solo a los operadores de comunicaciones electrónicas para la custodia de los datos de tráfico, sino a los proveedores de servicios de internet y, en general, a cualquier persona física[25] y jurídica que tenga a su disposición o bajo su control sistemas informáticos u electrónicos en los que se almacene cualquier tipo de información que pueda ser relevante para la investigación o enjuiciamiento de delitos[26]. En todo caso, en los supuestos en los que los sistemas no se encontraran bajo el dominio o disposición del sujeto al que se dirija la orden, la autoridad deberá de dirigirse al prestador de servicios titular del sistema de almacenamiento, a fin de asegurar un correcto cumplimiento de la medida conservativa.

En consecuencia, se trata de una medida de aseguramiento que cobra sentido en aquellos supuestos en los que no se dispone de forma inminente de la respectiva autorización judicial para el acceso a aquellos, pese a ser requerida, permitiendo asegurar que el titular o responsable de los mismos no proceda a su cancelación, destrucción o alteración. Por ello, el responsable o titular del fichero o sistema informático requerido por la Policía Judicial o Ministerio Fiscal vendrá obligado a prestar su plena colaboración en la ejecución de la medida, debiendo conservar y proteger los datos a los que se circunscriba la orden en el mismo sistema informático en que se hallen y en idéntico estado y situación a la que se encontraran en el momento de recibir la misma, hasta la recepción de la oportuna orden judicial o alternativamente hasta la expiración del plazo recogido en la orden. Es decir, el destinatario de la orden será responsable de mantener la integridad e indemnidad de la información objeto de entrega, garantizando su inmutabilidad respecto al momento al que se refiera la orden. Y para la consecución de ello deberá de un lado adoptar todas las medidas técnicas y organizativas que se requieran para lograr la conservación de la información en las condiciones expresadas – por ejemplo, efectuando copias de seguridad de la información en sistemas paralelos- y de otro lado, impedir que el titular de los datos o el propio sistema informático lógico que gestione las bases de datos alteren voluntaria o automáticamente la información objeto de entrega.

Igualmente, el sujeto obligado al cumplimiento de la orden deberá consecuentemente que rechazar de plano las solicitudes de ejercicio de los derechos de supresión, oposición o rectificación vinculados al derecho a la protección de datos de carácter personal que pudiera instar el interesado al que pertenezca la información. Por ello, habida cuenta del objeto de la orden de conservación,

25 En este punto la Fiscalía General del Estado mantiene que no estarán exceptuados de su cumplimiento ni los parientes del investigado ni quienes resulten amparados por el secreto profesional (como podría ser su abogado). Y ello debido al silencio que guarda la Ley sobre este punto, a diferencia de los casos en los que el legislador ha exceptuado a estas personas (arts. 588 sexies c.5 y 588 septies b.2 LECrim) y al hecho de que el cumplimiento de la orden supone un comportamiento neutro que no puede equipararse a la prestación de una declaración o a cualquier otra colaboración activa en la persecución del delito.

26 TEJADA DE LA FUENTE, E., "La retención obligatoria de datos de tráfico de las comunicaciones electrónicas y telemáticas y la preservación específica de datos informáticos como herramientas de investigación criminal", *El Derecho de Internet*, coord. F. PÉREZ BES, Atelier, Barcelona, 2016, p. 342.

podría decirse que es medida análoga en cuanto a sus efectos a la del bloqueo o limitación de datos prevista en la normativa del derecho protección de datos de carácter personal, que si bien, amén de ser instada por una autoridad facultada en lugar del interesado, extiende su alcance material a cualquier tipo de información que pueda conservarse en un sistema informático y no exclusivamente a datos de carácter personal. En cualquier caso, ello no impedirá que una vez entregados los datos a las autoridades o caducada la orden de conservación de datos sin que se hubiera recibido la autorización judicial oportuna, pueda atender el derecho de supresión que se hubiera solicitado, siempre y cuando concurran los requisitos exigidos en la normativa específica que resulte de aplicación.

Una vez notificada a su destinatario una orden de conservación de datos, éste deberá de conservar en su integridad los datos concretados por el plazo que el órgano requirente hubiera fijado en la misma, el cual deberá atender al previsible plazo que se considera necesario para la tramitación del instrumento judicial por el que se pretenda obtener la cesión de los datos, sin que en ningún caso pueda sobrepasarse inicialmente el plazo de noventa días[27]. No obstante, la regulación nacional prevé la posibilidad de que las autoridades competentes acuerden una eventual y única prórroga del periodo de conservación inicial cuando el plazo fijado no hubiera resultado suficiente para la obtención de la orden judicial o cuando su solicitud se retrasare a expensas de la obtención de avances de la investigación. En tal supuesto, la medida se podrá extender por el plazo necesario para completar la obtención definitiva de la autorización judicial, sin que en ningún caso pueda superarse el plazo de ciento ochenta días desde la emisión de la orden inicial[28].

Una vez expirado el plazo fijado como límite, bien en la orden inicial o bien en la prórroga, sin que se hubiera recibido la concreta orden judicial de entrega o acceso, el responsable del sistema informático no vendrá obligado a prolongar la conservación de los datos requeridos, sin perjuicio de que por otra norma legal pudiera venir impuesta su custodia por un periodo mayor. Mientras que para el caso de que vigente la orden de conservación se obtuviera la autorización judicial correspondiente a la diligencia de investigación por la que se concediera acceso a los datos conservados, el responsable o titular de la base de datos estaría obligado a entregar éstos al agente facultado o autoridad competente que se hubiera determinado en la resolución habilitante y bajo las condiciones fijadas.

En último lugar hay que hacer mención al deber de secreto que adquiere el destinatario de la orden sobre la propia diligencia y que se extiende durante no únicamente durante el periodo en que se extienda su desarrollo, sino incluso con posterioridad con carácter indefinido, so pena de incurrir en la responsabilidad penal reseñada en el apartado 3º del art. 588 *ter e*) LECrim prevista para el

27 Plazo máximo que el legislador nacional ha establecido de conformidad con lo previsto en el art. 16.2 del Convenio de Budapest, en el que se fija la duración de la medida en un máximo de noventa días.

28 Nuevamente, a la hora de establecer el plazo máximo de duración de la medida, incluida la prórroga, se establece el

supuesto de la interceptación de las comunicaciones telefónicas y telemáticas, esto es, en un delito de desobediencia grave[29].

Conclusiones

Por lo expuesto en el presente trabajo, no cabe duda de que la orden de conservación de datos es una novedosa herramienta procesal de aseguramiento de datos a disposición de la Policía Judicial y del Ministerio Fiscal que se convierte en esencial para la investigación no únicamente de los delitos de odio cometidos por vía electrónica, a través de algún medio o servicio de comunicaciones electrónicas o de la sociedad de la información, sino de cualquier otro delito consumado por esta vía.

Su utilización permite garantizar la disponibilidad e integridad de las fuentes de prueba del delito de naturaleza electrónica, minimizando los riesgos de desaparición o alteración que pueden tener origen en el propio victimario o en factores ajenos a éste.

En todo caso, la plena efectividad de la orden de conservación requiere de una actuación rápida y proactiva de la autoridad competente, puesto que deberá anticipar con la mayor antelación posible sobre qué información electrónica es necesario actuar e identificar al prestador o proveedor titular de los servidores o servicios en los que se aloja aquella, dado que cuando más tiempo transcurra entre la comisión del delito y la inmovilización de los datos, más probabilidad existe de que se eliminen o alteren los contenidos delictivos o los rastros y vestigios electrónicos o digitales de la acción ilícita.

Referencia

Delgado Martín, J. (2013). «La prueba electrónica en el proceso penal» en *Diario La Ley*, núm. 8167.

González Jiménez, A. (coord.) (s.f.). «Implicaciones jurídicas de los usos y comentarios efectuados a través de las redes» en *Revista de Internet, Derecho y Política*, núm. 27, pp. 17-29.

Asensio Gallego, J. M. (2017). «Los delitos informáticos y las medidas de investigación y obtención de pruebas en el convenio de Budapest sobre la ciberdelincuencia» en Asensio Mellado, J. M. (dir.), *Justicia penal y nuevas formas de delincuencia*, Tirant lo Blanch, Valencia, pp. 44-67.

29 Advierte OTAMENDI ZOZAYA acerca del silencio que guarda la LECrim sobre las consecuencias legales que depararía al sujeto obligado el incumplimiento del sujeto obligado del deber de colaboración y cumplimiento de la orden de conservación de datos, lo que no sucede respecto a otras diligencias de investigación contempladas en la misma norma. Sin embargo, considera el autor que cuando éste incumpliere la misma de forma voluntaria e intencionado incurrirá en un delito de desobediencia grave a la autoridad tipificado art. 556 Código Penal. *Vid*. OTAMENDI ZOZAYA, F., *Las últimas reformas de la ley de enjuiciamiento criminal: una visión práctica tras un año de vigencia*, Dykinson, Madrid, 2017, p. 148.

Otamendi Zozaya, F. (2017). *Las últimas reformas de la ley de enjuiciamiento criminal: una visión práctica tras un año de vigencia*, Dykinson, Madrid.

Quevedo González, J. (2017). *Investigación y prueba del ciberdelito* (tesis doctoral), Universidad de Barcelona.

Rayón Ballesteros, M. C. (2015). «Medidas de investigación tecnológica en el proceso penal: la nueva redacción de la Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015» en *Anuario jurídico y económico escurialense*, núm. 52, 2019.

Tamarit Sumalla, J. M. (2018). «Los delitos de odio en las redes sociales» en *Revista de Internet, Derecho y Política*, núm. 27, 2018, pp. 17-29.

Tejada de la Fuente, E. (2016). «La retención obligatoria de datos de tráfico de las comunicaciones electrónicas y telemáticas y la preservación específica de datos informáticos como herramientas de investigación criminal» en Pérez Bes, F. (coord.) *El Derecho de Internet*, Atelier, Barcelona, 2016, p. 315-345.

INFORMÁTICA Y DERECHO

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO
(SEGUNDA ÉPOCA)

FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES
DE DERECHO E INFORMÁTICA

ISSN 2530-4496 – N.º 13, 2023, PP. 133-148

PREVENCIÓN DE LOS CIBERDELITOS. ALGUNAS REFLEXIONES DESDE CASOS OCURRIDOS EN EL PERÚ

PREVENTION OF CYBERCRIMES. SOME REFLECTIONS FROM CASES THAT OCCURRED IN PERU

Carmen Milagros Velarde Koechlin[1]

1 Universidad de Lima. ORCID 0000-0002-2668-7774

Resumen

El presente trabajo da a conocer algunas de las normas aprobadas en el Perú para combatir los delitos informáticos y la ciberdelincuencia, recogiendo casos especiales como la norma de neutralidad de la red que faculta el bloqueo de nombres de dominio o aplicativos informáticos maliciosos. Se destaca también la regulación peruana de ciberseguridad y seguridad de la información, así como el uso de la geolocalización para las investigaciones de determinados delitos. Se resaltan casos de lucha contra la ciberdelincuencia y delincuencia como son el caso The Pirate Bay, el caso Picap y el caso de la suplantación de identidad a través del uso de la biometría con huella dactilar.

Palabras clave

delitos informáticos, neutralidad de la red, suplantación de la identidad, ciberseguridad, biometría dactilar.

Abstract

This paper discloses some of the standards approved in Peru to combat computer crime and cybercrime, collecting special cases such as the net neutrality standard that authorizes the blocking of domain names or malicious computer applications. The Peruvian regulation of cybersecurity and information security is also highlighted, as well as the use of geolocation for the investigation of certain crimes. Cases of fight against cybercrime and crime are highlighted, such as The Pirate Bay case, the Picap case and the case of identity theft through the use of fingerprint biometrics.

Keywords

Computer Crime, Net Neutrality, Identity Theft, Cybersecurity, Fingerprint Biometrics.

La regulación de los delitos informáticos en el Perú

Los avances de las tecnologías de la información y comunicación (TIC) han conllevado a un mejor acceso a los servicios y productos para toda la población. El uso de Aplicativos (Apps) a través del teléfono móvil ha contribuido a la reducción de tiempo en el acceso a servicios. Por ejemplo, la contratación del servicio de taxi (Cabify, Uber), el servicio de música (Spotify, Apple Music), la banca móvil, los servicios aéreos, hasta juegos y aplicaciones de entretenimiento. La mayoría de estas aplicaciones requiere una suscripción previa o configuración del acceso a través de una identidad digital. Además, para obtener los servicios, solicita un medio pago que puede ser una tarjeta de debido o crédito que, en varios casos, queda registrada en la aplicación. También recolecta nuestros datos personales que quedan grabados en el App; por ejemplo, los récords de nuestras actividades (compras, viajes realizados con fechas y horarios, rutas, entre otros).

Otra mejora de las tecnologías de la información y comunicación ha sido la posibilidad de crear bases de datos con amplia información, la que puede ser tratada, comparada, cotejada e intercambiada. Así, las entidades públicas y privadas han generado sus propias bases de datos que incluyen no sólo información personal, sino data biométrica dactilar o facial. Los propios teléfonos móviles recolectan estos datos cuando nos dan la posibilidad de grabar en él nuestra huella digital o nuestro rostro como clave para el desbloqueo del equipo. El uso de la biometría dactilar, incluso, ha comenzado a utilizarse como una firma electrónica en la suscripción de determinados contratos.

Pero, así como las TIC nos traen beneficios, también nos exponen a una delincuencia informática o ciberdelincuencia. Sujetos que buscan apropiarse de nuestros datos, romper nuestras contraseñas, acceder a los aplicativos como si fuéramos nosotros, alterar los sistemas o capturar la información de pago. Por eso, los países han adoptado medidas de seguridad informática, de seguridad de la información e incluso de ciberdefensa ante posibles ataques a la seguridad nacional. Desde el ámbito europeo, la suscripción del Convenio sobre la Ciberdelincuencia – también conocido como Convenio de Budapest, adoptado en esa ciudad el 23 de noviembre de 2001 – ha sido una de las herramientas más eficaces para que los Estados armonicen sus estrategias de lucha contra las nuevas formas de crimen informático. Cada vez más, los países de distintos continentes se suman a esta convención.

En el caso del Perú, el país decidió incorporarse al Convenio sobre la Ciberdelincuencia, el que entró en vigor el 01 de diciembre de 2019. Y, aunque realizó reservas al mismo, consideró asumir varios de los delitos listados en el convenio. En realidad, previamente, Perú había recogido en su ley de delitos informáticos varias de las formas penales de la convención.

Efectivamente, el Perú regula los delitos informáticos mediante Ley N.°30096 (del 21 de octubre de 2013); posteriormente, emitió una modificatoria a la misma con Ley N.°30171 (del 17 de febrero de 2014). Esta norma incluyó las figuras de delitos contra datos y sistemas informáticos que a su vez contempla el acceso ilícito a sistemas, vulnerando las medidas de seguridad. También recoge en su artículo 3 el atentado a la integridad de datos informáticos que se configura cuando

una persona de manera "deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos"; e incorpora en su artículo 4 el atentado a la integridad de sistemas informáticos para quien de forma "deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios".

Los delitos contra la intimidad y el secreto de las comunicaciones son también recogidos en la ley de delitos informáticos, incluyendo entre estos a la interceptación de datos informáticos, es decir, cuando alguien "deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos".

El fraude informático se presenta como un delito informático contra el patrimonio y es definido como aquel en que una persona "deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático".

Otro de los delitos a destacar, incorporado en la normatividad peruana es el de suplantación de identidad, considerado como un delito informático contra la fe pública y que es descrito así: "El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral". La norma peruana de delitos informáticos incluye otras disposiciones que tienden a facilitar las investigaciones a través de la fiscalía pública, la intervención de la policía nacional e incluso la cooperación de las empresas de telecomunicaciones para ofrecer datos de geolocalización con la debida confidencialidad.

Sin embargo, en Perú, existen también otras normas que regulan situaciones reprensibles que utilizan las tecnologías y sus dispositivos como herramienta para su comisión y establecen responsabilidades. Por ejemplo, la Ley 29904, del año 20212, Ley de promoción de la banda ancha y construcción de la Red Dorsal Nacional de Fibra Óptica, señala en su artículo 6 referido a la libertad de uso de aplicaciones o protocolos de Banda Ancha que "Los proveedores de acceso a Internet respetarán la neutralidad de red por la cual no pueden de manera arbitraria bloquear, interferir, discriminar ni restringir el derecho de cualquier usuario a utilizar una aplicación o protocolo, independientemente de su origen, destino, naturaleza o propiedad". Pero agrega, luego, que "El Organismo Supervisor de Inversión Privada en Telecomunicaciones - OSIPTEL determina las conductas que *no serán consideradas arbitrarias, relativas a la neutralidad de red"*[2]. En esta parte final es donde se incorporarán las acciones que darán lugar al respeto de la neutralidad de la red, pero también a aquellas excepciones que pueden conllevar al cierre de sitios web bajo causa determinada.

2 El destacado es nuestro.

Así, el año 2016, el OSIPTEL aprobó el Reglamento de Neutralidad de Red –el Reglamento– con Resolución de Consejo Directivo Nº 165-2016-CD/OSIPTEL –modificado este año por Resolución de Consejo Directivo N.° 003-2023-CD/OSIPTEL– que estableció que las empresas de telecomunicaciones que proveen el servicio de Internet podían aplicar protección ante acciones maliciosas o gestionar el tráfico en situación de interrupción en casos de emergencia, pero también podía gestionar las direcciones IP o filtrar y bloquear servicios o aplicaciones para dar cumplimiento a contratos con el Estado, *si se contraviene alguna ley específica*[3], por actos administrativos emitidos por la autoridad competente o por mandato judicial. Concretamente y de acuerdo con el Reglamento, en estos casos, la empresa de telecomunicaciones puede "bloquear puertos desde y hacia internet; bloquear nombres de dominio y/o direcciones IP; o bloquear aplicaciones y/o servicios".

El artículo 25 de este Reglamento se refiere a la protección de la red ante acciones maliciosas y destaca que tales son: Ataques de denegación de Servicios (DoS), al que el Reglamento define como "Ataque informático, desde un solo punto de origen hacia la red de datos del Operador de Telecomunicaciones, que causa que un servicio o recurso sea inaccesible a los usuarios legítimos de la red"; y, ataques distribuidos de denegación de servicios (DDoS), conceptualizado como "Ataque informático, desde varios puntos de origen hacia la red de datos de un Operador de Telecomunicaciones, que causa que un servicio o recurso sea inaccesible a los usuarios legítimos de la red".

Acciones de regulación de la ciberseguridad y lucha contra la delincuencia informática en el Perú

Aunque Perú cuente con legislaciones que reprimen delitos informáticos o situaciones reprensibles, no resulta suficiente un marco punitivo posterior a la comisión de tales situaciones. La prevención, el cuidado, la cautela son fundamentales y requieren acciones anticipadas. El Perú viene regulando estas situaciones a través de normas técnicas y legales que promueven la ciberseguridad, la ciberdefensa y gestionan un sistema de seguridad de la información.

Precisamente la Ley peruana de Gobierno Digital, Decreto Legislativo N.° 1412, incluyó un capítulo sobre Seguridad Digital, definida en su artículo 30 como "el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas". Añade, en su artículo 31 que "El Marco de Seguridad Digital del Estado Peruano se constituye en el conjunto de principios, modelos, políticas, normas, procesos, roles, tecnología y estándares mínimos que permitan preservar la confidencialidad, integridad, disponibilidad de la información en el entorno digital administrado por las entidades de la Administración Pública. Además, el Reglamento de dicha

3 El destacado es nuestro.

Ley – Decreto Supremo N.° 029-2021-PCM – añade la creación de un Equipo de Respuestas ante Incidentes de Seguridad Digital para la gestión de los incidentes o ataques que afecten la confianza digital.

Se aprecia, entonces, que la prevención a nivel de protección de los sistemas informáticos, de redes, de hardware y software, de bases de datos y todo aquello incluido en la organización del funcionamiento de las TIC al servicio del Estado, implica políticas, lineamientos, principios y todo un entorno digital que deben generar confianza. Además, mediante Decreto de Urgencia N.° 007-2020, se aprobó el marco de confianza digital peruano para fortalecer las interacciones digitales que se den entre personas, entre empresas y entidades públicas, destacando la norma que la confianza digital tiene como ámbitos de intervención a la protección de datos personales, la transparencia, la seguridad digital y la protección del consumidor, siempre dentro de un entorno digital. Se crea, también, el Centro Nacional de Seguridad Digital como "responsable de identificar, proteger, detectar, responder, recuperar y recopilar información sobre incidentes de seguridad digital en el ámbito nacional para gestionarlos".

De otro lado, el Reglamento de la Gestión de Seguridad de la Información y Ciberseguridad, aprobado por Resolución SBS N.° 504-2021, de la Superintendencia de Banca, Seguros y AFP considera a la ciberseguridad como la "Protección de los activos de información mediante la prevención, detección, respuesta y recuperación ante incidentes que afecten su disponibilidad, confidencialidad o integridad en el ciberespacio; el que consiste a su vez en un sistema complejo que no tiene existencia física, en el que interactúan personas, dispositivos y sistemas informáticos". El artículo 3 de dicha norma precisa el detalle del sistema de seguridad de la información y ciberseguridad así:

> Artículo 3. Sistema de gestión de seguridad de la información y Ciberseguridad (SGSI-C)
>
> 3.1. El sistema de gestión de seguridad de la información y ciberseguridad (SGSI-C) es el conjunto de políticas, procesos, procedimientos, roles y responsabilidades, diseñados para identificar y proteger los activos de información, detectar eventos de seguridad, así como prever la respuesta y recuperación ante incidentes de ciberseguridad.
>
> 3.2. El sistema de gestión de seguridad de la información y ciberseguridad (SGSI-C) implica, cuando menos, los siguientes objetivos:
>
> a) Confidencialidad: La información sólo es disponible para entidades o procesos autorizados, incluyendo las medidas para proteger la información personal y la información propietaria;
>
> b) Disponibilidad: Asegurar acceso y uso oportuno a la información; e,
>
> c) Integridad: Asegurar el no repudio de la información y su autenticidad, y evitar su modificación o destrucción indebida.

El Instituto Nacional de Calidad ha aprobado también normas técnicas peruanas (NTP) que pretenden armonizar la protección de sistemas de seguridad de la información, por ejemplo, la NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. Esta Norma se basa en la Norma ISO de Sistemas de Gestión de Seguridad de la Información 27001.

Pero, además de las normas preventivas, existen igualmente normas de apoyo a la investigación de los delitos con apoyo de las TIC, como el Decreto Legislativo N.° 1182, del 2015, que regula el Uso de los Datos derivados de las Telecomunicaciones para la Identificación, Localización y Geolocalización de Equipos de Comunicación, en la lucha contra la delincuencia y el Crimen Organizado. Esta norma destaca la posibilidad de la Policía Nacional del Perú a acceder a datos de geolocalización d teléfonos móviles o dispositivos electrónicos en casos de flagrancia, cuando los delitos superen la sanción de 4 años de pena privativa de libertad o cuando el acceso a los datos sea realmente necesario para el éxito de la investigación. Por supuesto, la Policía debe dar parte de su intervención, dentro de las próximas 24 horas, a la Fiscalía para que se dé conocimiento al Juez sobre tal diligencia. Esta norma se complementa con el Código Procesal Penal Peruano en cuyo artículo 230, numeral 4 se estipula la obligación de las empresas de telecomunicaciones a proporcionar los datos de geolocalización a pedido del Fiscal:

> Artículo 230. – Intervención, grabación o registro de comunicaciones telefónicas o de otras formas de comunicación y geolocalización de teléfonos móviles
>
> 4. Los concesionarios de servicios públicos de telecomunicaciones deben facilitar, en forma inmediata, la geolocalización de teléfonos móviles y la diligencia de intervención, grabación o registro de las comunicaciones que haya sido dispuesta mediante resolución judicial, en tiempo real y en forma ininterrumpida, las 24 horas de los 365 días del año, bajo apercibimiento de ser pasible de las responsabilidades de Ley en caso de incumplimiento. Los servidores de las indicadas empresas deben guardar secreto acerca de las mismas, salvo que se les citare como testigo al procedimiento.
>
> Dichos concesionarios otorgarán el acceso, la compatibilidad y conexión de su tecnología con el Sistema de Intervención y Control de las Comunicaciones de la Policía Nacional del Perú. Asimismo, cuando por razones de innovación tecnológica los concesionarios renueven sus equipos y software, se encontrarán obligados a mantener la compatibilidad con el sistema de intervención y control de las comunicaciones de la Policía Nacional del Perú.

Se aprecia, entonces, que el Perú, viene adoptando medidas de prevención contra los delitos informáticos y otros delitos, haciendo uso de las TIC y previniendo y adoptando medidas para la seguridad de la información y la ciberseguridad.

El caso de cierre de dominios por acciones maliciosas, de acuerdo al reglamento de neutralidad de red

Hemos mencionado al Reglamento de Neutralidad de la Red como una norma que permite también accionar ante situaciones que comprometen la legalidad, bloqueando dominios, números IP o contenidos Web maliciosos. Precisamente, haciendo uso de ello, el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual – INDECOPI, institución encargada de la protección del consumidor y de resguardar las distintas formas de propiedad intelectual, ha ordenado en varios casos el cierre de sitios Web y bloqueo de los nombres de dominios que han vulnerado los derechos de autor.

El caso The Pirate Bay

El año 2013, INDECOPI, a través de su Secretaría Técnica de la Comisión de Derechos de Autor, interpuso de oficio, una medida cautelar de cese, disponiendo que la Red Científica Peruana – entidad encargada de la administración de los nombres de dominio .PE (Poder Ejecutivo) – ejecute tal medida suspendiendo el registro de dominio https://thepiratebay.pe/ A través de los medios de comunicación, INDECOPI había tomado conocimiento que el sitio Web "The Pirate Bay" había registrado un dominio en Perú y con ello, había activado un sitio Web a través del cual los usuarios de Internet intercambiaban obras musicales y películas sin el respectivo reconocimiento de los derechos de autor (sobre todo, los derechos patrimoniales).

The Pirate Bay, un sitio Web dedicado a rastrear archivos multimedia para compartir a través de la modalidad Torrent (como es el caso del puerto a puerto o P2P) había sido ya sancionado en otros países por dicho intercambio de obras y reproducciones que vulneraban los derechos de autor. Ante esta situación y para poder seguir en funcionamiento, The Pirate Bay se vio obligado a abrir dominios en otros países para funcionar, pero en ellos también era sancionado. Las autoridades del INDECOPI ingresaron al sitio Web y realizaron búsquedas de compositores peruanos, encontrando que el sitio arrojaba información de las canciones y de los usuarios que las tenían en su computadora y que podían compartirlas. Igual ocurrió con la consulta sobre películas peruanas. Por ello, la solución inmediata debía ser bloquear el dominio de la Web que transgredía las normas peruanas de derecho de autor, a fin de que ningún usuario pueda acceder a ella.

Otros casos de bloqueo de dominios

En los últimos años, INDECOPI ha continuado disponiendo el cese de dominios que, luego de la evaluación respectiva, estarían vulnerando los derechos de autor. Por ejemplo, en mayo de 2021, el INDECOPI, mediante Resoluciones N.° 149-2021/CDA-INDECOPI y N.° 152-2021/CDA-IDNECOPI, bloqueó 17 sitios Web que facilitaban la descarga de videos protegidos autoralmente y permitía ver videos eventos deportivos en línea (streaming). Todo ello, sin contar con las autorizaciones de los autores ni con las licencias de trasmisión. En julio de 2022, esta entidad bloqueó 147 sitios Web ilegales que explotaban diferentes obras artísticas sin contar con la autorización de los autores ni reconocer el pago de los derechos de autor en su vertiente patrimonial. La Resolución N.° 198-2022/CDA-INDECOPI recogió esta disposición de cierre de los dominios de las webs piratas que utilizan streaming, linking y streaming rippinp. Asimismo, en diciembre de 2022 se ordenó bloquear 51 sitios Web que ilegalmente transmitían los partidos del mundial de Qatar. Esta medida se estableció con Resolución N.° 0477-2022/CDA-INDECOPI, sosteniendo además que esta acción contribuía a evitar software malicioso y robo de información.

El Caso Picap

Entre agosto y setiembre de 2019 el diario peruano El Comercio daba cuenta de la existencia de la empresa Picap, denominándola "el Uber de las motos". Picap era una empresa colombiana que había llegado al Perú para ofrecer servicio de taxi en motocicletas utilizando para ello un Aplicativo. Similar a Uber, el usuario obtenía el aplicativo en su teléfono móvil para solicitar un viaje de taxi en motocicleta, proporcionando datos personales y compartiendo su punto de recojo y su punto de partida; en varios casos, algunos de esos lugares eran los domicilios de las personas. Sin embargo, el periódico denunciaba en sus reportajes que Picap no tenía un procedimiento de evaluación de los conductores de motocicleta y que contaba con choferes que, en algunos casos, no tenían licencia de conducir. Un reportero de investigación del diario El Comercio ingresó como participante al chat interno de WhatsApp de la empresa Picap y evidenció, de las conversaciones, que se daban datos de las clientes, promoviendo así el acoso sexual; se expresaban frases que reflejarían que los choferes estarían conduciendo bajo el efecto de alguna droga e incluso se hacía referencia a tener cuidado con la policía, pues algunos estarían requisitoriados. También se compartía material ilícito relacionado a la pornografía.

Ante esta denuncia, el Ministerio de Transportes y Comunicaciones del Perú optó por emitir el Decreto Supremo N.° 035-2019-MTC, mediante el cual se "precisa disposiciones sobre el Servicio de Transporte Público de Personas en Vehículos Menores No Autorizados y establece disposiciones sobre el bloqueo de aplicativos y/o páginas web". Dicha norma prohibió el servicio de transporte público en vehículos motorizados menores, como son las motocicletas y estableció el bloqueo de cualquier aplicativo móvil o sitio Web que ofreciera el servicio de transporte público de personas en estos vehículos. El artículo 3 de dicha norma precisó:

> *Artículo 3.* Bloqueo de aplicativos y/o páginas web que ofrecen el servicio de transporte público de personas en vehículos de la categoría L, a excepción de la categoría L5
>
> 3.1. Las autoridades competentes para fiscalizar el servicio de transporte informan a la Dirección General de Políticas y Regulación de Transporte Multimodal, de la existencia de aplicativos y/o páginas web que oferten servicios de transporte público de pasajeros en vehículos de categoría L, distintos a la L5.
>
> 3.2 La Dirección General de Políticas y Regulación de Transporte Multimodal de acuerdo a la información que obtenga, de forma directa o por la comunicación de las autoridades competentes en materia de fiscalización sobre la existencia de aplicativos y/o páginas web que oferten y/o presten servicios de transporte público de pasajeros en vehículos de la categoría L, a excepción de la categoría L5, se encarga de realizar la solicitud de bloqueo, con la periodicidad que estime pertinente, a la Dirección General de Programas y Proyectos de Comunicaciones.
>
> 3.3 La Dirección General de Programas y Proyectos de Comunicaciones requiere a los proveedores de servicios de internet el bloqueo de aplicativos y/o páginas web que oferten y/o presten el servicio de transporte público de personas en vehículos de la categoría L, a excepción de la categoría L5 desde el

día siguiente de recibida la comunicación cursada por la Dirección General de Políticas y Regulación de Transporte Multimodal.

3.4 Los proveedores de servicios de internet notificados con el requerimiento tienen la obligación de bloquear los aplicativos y/o páginas web en el plazo señalado por la Dirección General de Programas y Proyectos de Comunicaciones.

3.5 La Dirección General de Programas y Proyectos de Comunicaciones comunica también a la Dirección General de Fiscalizaciones y Sanciones en Comunicaciones para que en un plazo máximo de treinta (30) días hábiles, luego de recibido el requerimiento de bloqueo, fiscalice el cumplimiento de la medida.

Basado en esta disposición, el Ministerio de Transportes y Comunicaciones solicitó a las empresas de telecomunicaciones bloquear el acceso al Aplicativo Picap. Esta medida conllevó a un debate, pues se cuestionaba que no respeta la neutralidad de la red. Algunos defensores sostenían que el problema de informalidad de la empresa no se arreglaba bloqueando el aplicativo o el servicio. No obstante, la medida fue adoptada e implicó el cierre de dicha empresa en el Perú.

El caso de suplantación de identidad y la necesidad de la protección de los datos biométricos

Los datos biométricos se han convertido en una opción para la identificación certera de los ciudadanos, clientes o usuarios de servicios. El uso de la biometría dactilar se ha utilizado incluso en el Perú como una firma electrónica. Precisamente, esto ha ocurrido en el caso de la contratación de servicios públicos de telecomunicaciones. El Organismo Supervisor de Inversión Privada de Telecomunicaciones – OSIPTEL, a través de sus normas regulatorias aprobó la posibilidad de que las empresas de telecomunicaciones suscriban con sus clientes contratos biométricos basados en el uso de la huella dactilar. Para ello, la empresa operadora de telecomunicaciones debía solicitar al OSIPTEL la autorización para el uso de la contratación biométrica en el servicio determinado. Por ejemplo, la empresa podía solicitar autorización para el servicio de internet fijo y con ello, presentar un flujo y otros requisitos que mostraran cómo se llevaría a cabo el proceso de identificación biométrica y la suscripción del contrato biométrico, así como la impresión física de cómo ser vería la firma electrónica.

El Texto Único Ordenado de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones, aprobado con Resolución de Consejo Directivo Nº 138-2012-CD-OSIPTEL, modificado por Resolución N.° 96-2018-CD-OSIPTEL, del 01 de mayo de 2018, se definieron los mecanismos de contratación incluyendo los "Medios informáticos, que incluyan la utilización de contraseña o claves secretas que la empresa operadora le hubiere proporcionado previamente al abonado", así como otros mecanismos previamente aprobados por el OSIPTEL, dentro del cual se haya la contratación biométrica por verificación de huella dactilar. Asimismo, la norma exigía a las empresas de telecomunicación que antes de realizar alguna contratación, aplicara la identificación biométrica con huella dactilar, comparando la huella digital del cliente con la base de datos del Registro Nacional de Identificación y Estado Civil – RENIEC, entidad del Estado a

cargo de la gestión de los registros civiles y la entrega del Documento Nacional de Identidad de los peruanos.

En octubre de 2022, el OSIPTEL actualizó la Norma de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones, con Resolución de Consejo Directivo N.° 172-2022-CD/OSIPTEL en donde definió a los mecanismos de contratación como "Mecanismos de Contratación El mecanismo de contratación es todo medio que permita otorgar certeza de la manifestación de voluntad de solicitar y/o aceptar la contratación, resolución y/o modificación de los términos o condiciones de la contratación de un servicio público de telecomunicaciones". También definió al sistema de verificación biométrica como: "Sistema de verificación biométrica de huella dactilar: Sistema que permite la identificación de personas a partir de la característica anatómica de su huella dactilar, utilizando un dispositivo analizador o lector biométrico que permitirá la validación de la identidad del solicitante del servicio con la información contenida en la base de datos biométrica del RENIEC".

Si bien todas estas facilidades de dieron para lograr una contratación electrónica más ágil, ocurrió que, lamentablemente, la capacidad de venta de las empresas operadoras se amplió no sólo a tiendas formales y autorizadas, sino a personas naturales que desarrollaban la venta de chips en la calle y que, al vender líneas móviles, tenían acceso a los datos personales de los comprados, así como a su huella digital. Esta situación conllevó a que se presentaran casos de usuarios de servicios de telecomunicaciones que sostenía que habían tomado conocimiento de que existían servicios de telecomunicaciones a sus nombres sin que ellos lo hubiesen contratado. El Tribunal Administrativo de Solución de Recamos de Usuarios del OSIPTEL comenzó a recibir reclamos por contratación no solicitada donde los clientes negaban haber acudido a suscribir un contrato con su huella digital. En varios de estos casos, se solicitaba al RENIEC una confirmación de si se había hecho la consulta de comparación de huella digital el día y hora de la contratación, recibiendo respuesta positiva. Esta situación conllevó a que la Policía Nacional del Perú investigara estas situaciones encontrando bandas criminales que se dedicaban a obtener las huellas de los clientes y copiarlas en silicona para pasar el huellero biométrico. En algunos reportajes de medios de comunicación se menciona la participación de personas que tenían acceso a los datos biométricos por la venta de servicios de telecomunicaciones.

Ante este panorama, el OSIPTEL decidió prohibir la venta de chips en la vía pública, lo que conllevó a que las empresas de telecomunicaciones presentaran su demanda ante el INDECOPI por considerar esta medida una barrera burocrática. Si bien, la Comisión de Eliminación de Barreras Burocráticas del INDECOPI, en primera instancia, resolvió en mayoría con Resolución N.° 0033-2021/CEB-INDECOPI y Resolución N.° 0034-2021/CEB-INDECOPI, del 5 de febrero de 2021, declarar tal medida como barrera burocrática ilegal, sí reconoció en sus precisiones finales que "Esta Comisión considera importante precisar que lo resuelto en el presente caso no implica un desconocimiento de las facultades del Osiptel para establecer medidas que tengan por finalidad salvaguardar la seguridad de los usuarios en la contratación de los servicios públicos de telecomunicaciones (…). Además, añadió que "el presente pronunciamiento no altera

ni desconoce ninguna de las obligaciones establecidas en las normas que deben cumplir los operadores frente a los usuarios, tales como: (i) el uso del sistema de verificación biométrica de huella dactilar para identificar al usuario, (ii) el registro de los datos personales del usuario en el registro de abonados antes de la activación del servicio, (iii) la obligación de las empresas operadoras de mantener un archivo físico y/o digital que permita acreditar la utilización del procedimiento de identificación biométrica de huella dactilar, estableciéndoles la carga de probar que se realizaron las verificaciones correspondientes ante cualquier reclamo o investigación, entre otros".

No obstante, el OSIPTEL apeló la medida iniciando además una campaña para evitar comprar teléfonos móviles robados o chips de telefonía móvil en la vía pública, basados en la protección de los datos personales y evitar casos de suplantación de identidad ante el posible mal uso de la data personal. OSIPTEL sustentaba sus defensas en los casos de contrataciones fraudulentas que había detectado en sus labores de supervisión, esto es, chips de telefonía móvil pre activados a nombre de terceras personas. Además, expresó el crecimiento de reclamos por contrataciones no solicitadas, donde los usuarios sostenían no haber celebrado contratación biométrica con huella dactilar. Estos casos no sólo se limitaban a la contratación de nuevos servicios móviles, sino también a casos de portabilidad numérica, donde terceros, suplantando la identidad de una persona, realizan el cambio del número de telefonía móvil a otra empresa.

Finalmente, en segunda instancia, el INDECOPI, con Resolución N.° 661-2021/SEL-INDECOPI, declaro infundada la Resolución N.° 0034-2021/CEB-INDECOPI considerando que la Norma de Condiciones de Uso de los Servicios Públicos de Telecomunicaciones establecía que las empresas operadoras debían activar el servicio de identificación biométrica en sus locales de atención y centros de distribuidores autorizados, lo que no podían hacerse en la vía pública pues no cumpliría las pautas de la contratación.

Luego de ello, OSIPTEL ha impulsado otras acciones de lucha contra la suplantación de identidad a través del uso de la huella dactilar y datos personales de usuarios de servicios de telecomunicaciones imponiendo mayores seguridades al uso de la biometría. Justamente, una medida que ha adoptado el OSIPTEL y que rige desde el 12 de enero de 2023, es que el personal de las empresas de telecomunicaciones que participe en la suscripción de contratos de estos servicios deba identificarse primero a través de una verificación biométrica, lo que permitirá saber qué personas suscribió el contrato a nombre de la empresa. Con esta medida disuasiva, se pretende evitar que terceros no autorizados ingresen a la información personal de los clientes y la utilicen, suplantando identidad, en la suscripción de contratos no consentidos:

> Desde este jueves 12 de enero, el personal de las empresas operadoras o de sus distribuidores autorizados que intervengan en la contratación de servicios públicos móviles deberán validar su identidad mediante verificación biométrica de huella dactilar, previamente al trámite, según lo dispuesto por el Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL).
>
> Esta medida permitirá tener mayor trazabilidad en la contratación de los servicios e identificar a quienes intervinieron en el proceso para evitar que

> personas no autorizadas accedan a la información personal de los abonados y realicen operaciones sin su consentimiento. La disposición también aplica para el personal que realiza entrega del SIM card a domicilio (delivery) y participa en el proceso de contratación y activación del servicio.

Otra medida a destacar es que el año 2022, el OSIPTEL suscribió con el RENIEC un convenio de lucha contra la ciberdelincuencia por el cual cotejó poco más de 28 millones de datos de titulares de teléfonos móviles para verificar si las identidades coincidían a los verdaderos titulares, considerando los nombres y otros datos de identificación. Así, en una nota de prensa del 12 de setiembre de 2022, OSIPTEL indicó que, del resultado de dicho cotejo, encontró más de "400 mil datos inconsistentes en los registros de abonados de las empresas operadoras móviles". Algunos titulares de líneas de telefonía móvil las habían adquirido dando nombres como Ja jajaja; o, Té de Manzanilla; o, Me gustaría Gracias Por favor. Este trabado ayudó a que las empresas operadoras comiencen a limpiar su registro de abonados para obtener datos de identificación correctos y cerras líneas de usuarios desconocidos, previo envío de mensaje de texto para regularizar su situación.

Conclusiones

El Perú ha adoptado normas para sancionar el delito informático, pero también normas de prevención para la ciberseguridad y seguridad de la información.

La neutralidad de la red ha incluido medidas que permiten el bloqueo de sitios Web y aplicativos informáticos maliciosos y que, en su mayoría, vulneran los derechos de autor.

La lucha contra el cibercrimen no queda únicamente en las redes informáticas, sino que debe expandirse a la infraestructura externa, equipos físicos, y datos personales; aquí se presentan los casos de suplantación de identidad, adquisición de equipos móviles con identidades inconsistentes.

La lucha contra el cibercrimen, la aplicación de medidas de seguridad de la información y ciberseguridad son aplicadas por distintas entidades, no sólo en sus acciones de gestión, sino también, a través de sus resoluciones administrativas en la definición de casos vitales para la lucha contra la ciberdelincuencia.

Referencias

El Comercio (2 de setiembre de 2019). Llegó Picap, el 'Uber' de las motos en Lima: manejan hasta sin brevete. Sitio Web de El Comercio. Recuperado el 29 de enero de 2023 de https://elcomercio.pe/lima/transporte/informalidad-app-notepases-noticia-ecpm-671167-noticia/

El Peruano (20 de julio de 2012). Ley N.° 29904, Ley de promoción de la banda ancha y construcción de la red dorsal nacional de fibra óptica. Normas Legales

El Peruano (22 de octubre de 2013). Ley N.° 30096, Ley de delitos informáticos. Normas Legales.

El Peruano (10 de marzo de 2014). Ley N.° 30171, Ley que modifica la Ley 30096, Ley de delitos informáticos. Normas Legales.

El Peruano (29 de diciembre de 2016). Resolución de Consejo Directivo Nº 165-2016-CD/OSIPTEL, Reglamento de Neutralidad de Red. Normas Legales.

El Peruano (27 de julio de 2015). Decreto Legislativo 1182, decreto legislativo que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado

El Peruano (13 de setiembre de 2018). Decreto Legislativo N.° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital. Normas Legales.

El Peruano (14 de noviembre de 2019). Decreto Supremo N.° 035-2019-MTC, Decreto Supremo que precisa disposiciones sobre el Servicio de Transporte Público de Personas en Vehículos Menores No Autorizados y establece disposiciones sobre el bloqueo de aplicativos y/o páginas web. Normas Legales.

El Peruano (22 de setiembre de 2019). Convenio sobre la ciberdelincuencia. Budapest, 23.XI.2001. Normas Legales.

El Peruano (9 de enero de 2020). Decreto de Urgencia N.° 007-2020, Decreto de Urgencia que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento. Normas Legales.

El Peruano (19 de febrero de 2021). Decreto Supremo N.° 029-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N.° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo. Normas Legales.

El Peruano (23 de febrero de 2021). Resolución SBS N.° 504-2021, Aprueban el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, modifican el Reglamento de Auditoría Interna, el Reglamento de Auditoría Externa, el TUPA de la SBS, el Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos, el Reglamento de Riesgo Operacional, el Reglamento de Tarjetas de Crédito y Débito y el Reglamento de Operaciones con Dinero Electrónico. Normas Legales.

El Peruano (12 de enero de 2023). Resolución de Consejo Directivo N.° 003-2023-CD/OSIPTEL, modifican el Reglamento de Neutralidad de Red, aprobado por Resolución N.° 165-2016-CD/OSIPTEL. Normas Legales.

Instituto Nacional de Defensa de la Competencia y Protección de la Propiedad Intelectual – INDECOPI (25 de mayo de 2021). El Indecopi logra bloqueo de 17 sitios web ilegales que permitían descargas de obras y transmisión de eventos deportivos. Plataforma digital única del Estado Peruano. Recuperado el 30 de enero de 2023 de https://www.gob.pe/institucion/indecopi/noticias/494864-el-indecopi-logra-bloqueo-de-17-sitios-web-ilegales-que-permitian-descargas-de-obras-y-transmision-de-eventos-deportivos

Instituto Nacional de Defensa de la Competencia y Protección de la Propiedad Intelectual – INDECOPI (8 de julio de 2022). ¡Golpe a la piratería digital! Indecopi bloquea 147 sitios web ilegales que explotaban obras y

producciones protegidas por el derecho de autor. Plataforma digital única del Estado Peruano. Recuperado el 30 de enero de 2023 de https://www.gob.pe/institucion/indecopi/noticias/630376-golpe-a-la-pirateria-digital-indecopi-bloquea-147-webs-ilegales-que-explotaban-obras-y-producciones-protegidas-por-el-derecho-de-autor

Instituto Nacional de Defensa de la Competencia y Protección de la Propiedad Intelectual – INDECOPI (12 de diciembre de 2022). El Indecopi ordena bloqueo de 51 sitios web piratas que difundían ilegalmente partidos del Mundial de Qatar, películas y música. Plataforma digital única del Estado Peruano. Recuperado el 30 de enero de 2023 de https://www.gob.pe/institucion/indecopi/noticias/679157-el-indecopi-ordena-bloqueo-de-51-sitios-web-piratas-que-difundian-ilegalmente-partidos-del-mundial-de-qatar-peliculas-y-musica

Instituto Nacional de Defensa de la Competencia y Protección de la Propiedad Intelectual – INDECOPI (2023). Sitio Web Oficial y buscador de normas. Plataforma única digital del Estado Peruano. Recuperado enero de 2023 de https://www.gob.pe/indecopi

Organismo Supervisor de Inversión Privada en Telecomunicaciones – OSIPTEL (28 de junio de 2022). Reniec y Osiptel juntos contra la ciberdelincuencia. Recuperado el 30 de enero de 2023 de https://www.osiptel.gob.pe/media/jrjkoard/np-reniec-y-osiptel-luchan-contra-cibercriminalidad.pdf

Organismo Supervisor de Inversión Privada en Telecomunicaciones – OSIPTEL (12 de setiembre de 2022). OSIPTEL detecta más de 400 mil datos inconsistentes en los registros de abonados de las empresas operadoras móviles. Recuperado el 30 de enero de 2023 de https://www.osiptel.gob.pe/portal-del-usuario/noticias/osiptel-detecta-mas-de-400-mil-datos-inconsistentes-en-los-registros-de-abonados-de-las-empresas-operadoras-moviles/

Organismo Supervisor de Inversión Privada en Telecomunicaciones – OSIPTEL (9 de enero de 2023). Verificación biométrica permitirá identificar a personal de empresas que intervengan en contratación de servicios móviles. Plataforma única digital del Estado Peruano. Recuperado el 30 de enero de 2023 de https://www.gob.pe/institucion/osiptel/noticias/687984-verificacion-biometrica-permitira-identificar-a-personal-de-empresas-que-intervengan-en-contratacion-de-servicios-moviles

Organismo Supervisor de Inversión Privada en Telecomunicaciones – OSIPTEL (2023). Sitio Web Oficial y buscador de normas. Plataforma única digital del Estado Peruano. Recuperado enero de 2023 de https://www.gob.pe/osiptel

INFORMÁTICA Y DERECHO

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO
(SEGUNDA ÉPOCA)

FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES
DE DERECHO E INFORMÁTICA

ISSN 2530-4496 – N.º 13, 2023, PP. 149-160

COMENTARIO DE JURISPRUDENCIA

PLATAFORMAS DIGITALES COMO MEDIOS PARA LA CONCRECIÓN DE VIOLENCIA DIGITAL EN CONTEXTO DE GÉNERO

DIGITAL PLATFORMS AS A MEANS FOR THE PERPETRATION OF DIGITALVIOLENCE IN THE CONTEXT OF GENDER

Rodrigo Alejandro Gómez Torre[1]

1 Personal Docente Investigador de la Universidad de Salamanca, Reino de España. Profesor de Derecho Informático, Universidad Nacional de Cuyo, República Argentina.

Resumen

El sujeto activo del delito, desde locales denominados cibercafés, en vistas de ocultar la autoría del crimen, accedió en forma ilegítima a una base de datos personales (e-mail y perfil de una plataforma digital) imposibilitando a su titular hacer uso de ella. Ese delito se utilizó como medio para la perpetración de otros. Desde esa plataforma y correo electrónico se generaron contenidos injuriosos y calumniosos que luego se masificaron por la dispersión en diversas plataformas digitales. El victimario, se valió de esas cuentas "hackeadas" para abrir nuevas cuentas de correo electrónico y perfiles apócrifos en diversas plataformas. Individualizando en ellas a la víctima, para desde allí replicar mensajes al entorno social, familiar y laboral de esta en detrimento de su intimidad por su condición de mujer. Hechos que se complementaron con la creación de un perfil en una plataforma destinada a concretar encuentros sexuales, desde dónde tomaba contacto con diversos usuarios para encaminarlos a concretar personalmente las experiencias sexuales prometidas. Finalmente, el victimario, con identidad suplantada, denunció los hechos en los centros educativos donde la víctima ejercía la docencia, aduciendo que esta corrompía y/o abusaba de los menores a su cargo, hecho que derivó en la pérdida del puesto laboral.

Palabras clave

plataformas digitales, delito informático, violencia de género.

Abstract

From stores called "cybercafes", in order to hide the authorship of the crime, the offender accessed illegitimately to personal database (e-mail and profile of a digital platform) making it impossible for its owner to use it. This illegal activity served as a tool for committing other crimes, as slanderous and defamatory content was produced from that platform and email, and then widely spread across various digital platforms. The culprit utilized the hacked accounts to create new email accounts and fake profiles on different platforms, impersonating the victim only with the purpose of sending messages to the victim's social, family, and work network, damaging the victim's privacy as a woman.

To complement these facts, a profile was created on a platform designed for arranging sexual encounters. From this profile, the offender contacted various users and directed them to the victim's address to carry out the promised sexual experiences personally.

Finally, the perpetrator, using an impersonated identity, accused the victim of corruption and abuse of minors in the educational institutions where she worked as a teacher, leading to her losing her job.

Keywords

Digital platforms, Cybercrime, Gender-based violence.

Introducción

La Cámara Federal de Casación Penal de la República Argentina confirmó la sentencia del Tribunal Oral Federal Número 1 de la Provincia de Mendoza por la que se sentencia a 3 años de prisión en suspenso al exesposo de la titular de los perfiles de las plataformas digitales "hackeadas", al acreditar que era él quien desarrollaba estos hechos desde locales denominados "cibercafé", encontrándolo penalmente responsable del delito de coacción agravada en contexto de violencia de género. Autos FMZ 13017007/2011/TO1 TOral Crim. Fed. Nro. 1, Mendoza, 09/03/2022. R. B., C. R. s/ Coacción (art. 149 bis del CP).[2]

En tiempos en donde el mercado (y por ende la mayoría de la sociedad occidental) tiende a cosificar la figura de la mujer, se destaca que las "nuevas tecnologías" han logrado hacer más propenso el actuar de los victimarios, ya que, al tiempo que estos perciben más distante la sensación de estar perpetrando un delito, al sistema judicial se le dificulta la identificación del autor; por ello este fallo tiene especial trascendencia.

La relevancia que posee puede diseminarse en varios ámbitos. En el de la sociología jurídica podemos comenzar indicándole al lector que tanto el sujeto activo como el pasivo del delito no recaen en lo que comúnmente se identifican como jóvenes, adolescentes o nativos digitales. Rompiendo así el primer mito que afirma que este grupo etario es el que tiene propensión por la utilización de nuevas tecnologías para la concreción de conductas típicas, antijurídicas, culpables y punibles. En el caso traído a análisis, tanto víctima como victimario pertenecen a la generación definida como "Baby Boomers"[3], ambos poseen grados universitarios, desempeñan profesiones liberales, son docentes y mantuvieron un matrimonio durante casi dos décadas, en el cuál tuvieron tres hijos.

Otro de los aspectos a destacar es el rol que ocupan las plataformas digitales en la sociedad actual al momento de la distribución de este tipo de contenidos. Si pensamos en la acción de distribución como los circuitos por los que circulan los bienes culturales, históricamente encontramos una variedad de canales que raramente se documentaban, sin embargo, formaban parte de la transmisión social de contenidos. Tomando la caracterización económica con la que suele clasificarse la dinámica de la distribución, diremos entonces que siempre existió una distribución formal, una informal y una tercera clase que opera en los espacios grises que se generan entre las dos categorías anteriores, es decir, espacios habitados por actores y prácticas que no son del todo formales ni del todo informales.

2 Sentencia y fundamentos disponibles en el repositorio digital del Centro de Información Judicial de la República Argentina https://www.cij.gov.ar/d/sentencia-SGU-20cd6e0e-3971-4bab-a464-19f8f354150a.pdf y https://www.cij.gov.ar/d/sentencia-SGU-5d5d7ca5-b221-459c-af84-c7bef5696bf5.pdf (última fecha de consulta 30/03/2023).

3 Generación que se define generalmente como las personas nacidas entre 1946 y 1964, durante la explosión de natalidad posterior a la Segunda Guerra Mundial. SHEEBAN, P. "Greed of boomers led us to a total bust". The Sydney Morning Herald. 26 de septiembre de 2011.

Esos tres tipos de actores se encuentran históricamente en todos los mercados de distribución, desde los más regulados hasta los menos regulados, con mayor o menor presencia.

Con la irrupción de internet los mecanismos de distribución explotaron, más aún cuando pensamos que dentro de la *world wide web* se distribuyen contenidos digitales que replican la información con idéntica calidad al original. Por ello los mecanismos de distribución formal parecieron volverse incontrolables. Si debido a las nuevas tecnologías la transferencia en el espacio físico terminó por tener mayores circuitos de distribución formales e informales, aumentando por ello los espacios grises, en el espacio digital la superposición de circuitos es casi una condición de la distribución.

Es aquí donde las plataformas aparecen para dar orden a ese caótico intercambio de contenido cultural, que en forma desordenada y de superposición permanente entre circuitos formales e informales queda a disposición de cada usuario. Usuario que se hace del contenido en forma intencional, o no, gracias a los algoritmos que las plataformas utilizan.

Las compañías tecnológicas, atrás de estas plataformas, son un nuevo modo de llamar a los tradicionales intermediarios, quienes cuentan con un componente extra que es la posibilidad de compartir los contenidos, calificarlos, relacionarlos con otros y reordenarlos. Ahora bien, ¿Por qué no se los denomina directamente compañías tecnológicas o incluso intermediarios? De este modo se le aplicaría el mismo denominador lingüístico que históricamente tuvieron los sujetos que desempeñaron esas actividades.

Parafraseando a Gillespie[4], este tipo de posicionamiento discursivo tiene una finalidad. Denominar plataforma a un servicio online no es una afirmación ingenua o realizada al azar, a la industria digital le sirve utilizar palabras que sugieran mucho, pero que digan poco. Es decir, utilizar términos e ideas que son lo suficientemente específicos para significar algo y al mismo tiempo lo suficientemente vago para que su utilización sirva en diferentes sitios con audiencias múltiples.

Términos como plataforma, continúa la idea de Gillespie, importan tanto por lo que esconden como por lo que muestran. Esto es así toda vez que a pesar de las promesas que declaman de cara a la sociedad, las plataformas son mucho más parecidas a los medios tradicionales de distribución de bienes culturales de que lo que ellas mismas admiten. Así, su supuesta neutralidad radica en su (falsa) apertura y en el poder de control que da a los usuarios para diseñar sus propios circuitos de búsqueda, consumo y distribución.

En resumen, para redondear el análisis del fenómeno prenormativo en cuanto a los sujetos implicados en el caso, las plataformas ordenan y agregan lo que de otro modo estaría disponible pero en forma caótica, proponen un modelo de negocio para la industria, que se reacomoda a una nueva forma de distribución dominada por actores tecnológicos, habilitan la participación de los usuarios/

4 GILLESPIE, T., "The Politics of Platforms" New Media & Society 12 (3) 2010. Pag. 347-364. Disponible en https://doi.org/10.1177/1461444809342738

prosumidores, pero dentro de un marco por ellos definidos en donde establecen que está permitido y que está prohibido siendo actores principales en la distribución de contenidos digitales pero desenvolviéndose en un escenario que no es radicalmente diferente al modelo de mediados del siglo pasado.

El otro ámbito de relevancia del fallo analizado es el de la dogmática jurídica, ya que se interpretaron diversas normas de fondo, que generalmente se engloban sin mayores definiciones bajo el concepto de delitos informáticos, para luego armonizarlas con otros institutos penales y de orden público. Sobre ello se profundiza en los siguientes acápites.

Presentación del caso

La víctima había advertido desde el año 2006 algunas publicaciones extrañas en redes sociales, al tiempo que algunas personas de su entorno le habían comentado haber recibido correos electrónicos con contenido ofensivo que se relacionaban con ella, sin embargo, el proceso judicial se inició cuando advierte que no puede ingresar a sus cuentas de correo electrónico y de redes sociales, en el año 2011.

Al ser la correspondencia el bien jurídico vulnerado en forma inicial, acudió a realizar la denuncia ante la Delegación Mendoza de la Policía Federal Argentina debido a la competencia[5] en donde corresponde ventilar este tipo de delitos. Esta fue la denuncia que excitó el inicio del proceso.

Luego de las labores de investigación pertinentes, se da con el presunto autor del delito, quien sería su exesposo, que valiéndose de información personal que poseía de la víctima, sistemáticamente acudía a locales comerciales denominados "ciber" para ingresar a las diversas cuentas de la víctima (y a las creadas apócrifamente por él) para desde allí realizar nuevos hechos ilícitos. Por lo tanto, en un primer momento se imputó y luego se procesó al reo por los delitos tipificados en los artículos 153, 153 bis y 157 bis del Código Penal Argentino.

Al ser apelado el procesamiento por la defensa, ya que consideraba vaga e imprecisa la declaración indagatoria realizada, entre otros argumentos, la víctima contrata un abogado particular para constituirse como querellante y continuar con el impulso del proceso. Procura también, subsanar los requisitos procesales que parte de la doctrina entienden necesarios al momento de juzgar los delitos tipificados en los artículos 153, 153 bis y 157 bis del Código Penal Argentino. Al analizar la apelación, la sala A de la Cámara Federal de Apelaciones de la Provincia de Mendoza, consideró que correspondía recalificar los hechos atribuidos por lo que ordenó al juez instructor, recalificar dichas conductas en orden al delito previsto y reprimido por el artículo 149 bis 2º párrafo del Código Penal Argentino (coacciones agravadas).

Es en este momento que se entiende que la víctima no había sufrido solo un acceso ilegítimo a sus redes sociales o correos electrónicos, sino que, el accionar del victimario en su conjunto, había terminado por alterar el desarrollo normal

5 CSJN conf. Competencia 351, L. XLVÍII in re "Jutton, Juan Carlos s/denuncia delito c/la seguridad pública", resuelta el 20 de noviembre de 2012.

y ordinario de la vida de la víctima, provocando además incluso pérdidas económicas. Y que dichas maniobras constituirían, prima facie, un grave caso de violencia de género del que el Tribunal no podía hacer caso omiso por disposición de la ley 26.485.

En el debate oral, quedó acreditado que todas las acciones que desarrolló el agente activo del delito tuvieron por finalidad obligar a su exesposa a no formar una nueva pareja, a alejarla de sus amistades o personas allegadas y a causarle perjuicios en el ámbito laboral; de modo que pueda compelerla para consentir la entrega de ciertos bienes que se encontraban en litigio en el marco del proceso de separación y posterior divorcio que ambos mantenían en el fuero de familia.

Se deja de lado, exprofeso, el análisis de los medios probatorios tenidos en cuenta para llegar a destruir el estado de inocencia del reo para dar cumplimiento a la extensión que las normas editoriales establecen para este tipo de monografías.

El equilibrio en el debido proceso, el derecho de defensa y los derechos de la víctima de violencia de género

En este proceso se ventilaron hechos que para el ordenamiento penal argentino en una época fueron atípicos[6], que luego se continuaron desarrollando en fechas en las que fueron tipificadas por el ordenamiento penal argentino y fue por ello que se terminó imputando al reo. Sin embargo, al momento de ser apelado el procesamiento por la defensa, y en vista del contexto en que fueron desarrollados los hechos, se contrastó el total de las agresiones con los bienes jurídicos vulnerados de la víctima y se terminó por recalificarlos, ya que a priori encuadraban en el tradicional artículo 149 bis del Código Penal Argentino (coacciones agravadas).

A lo largo del proceso, y en cada una de estas instancias, las que a la fecha ya han sido todas agotadas, se ventilaron cuestiones que hacían a nulidades procesales, a discusiones de competencia y a la prescripción del ilícito, entre tantas otras particularidades de cada una de las instancias transitadas en un proceso.

Por esta razón el juicio culminó con el fallo ahora comentado consumiendo apenas frioleros 10 años, 10 meses, y 5 días. Desde la denuncia de la víctima en la Delegación Mendoza de la Policía Federal Argentina, el día 04 de mayo de 2.011, hasta la sentencia, dictada el día 09 de marzo del 2022, transcurrieron 3962 días. Este dato tiene una trascendental importancia y se lo retomará en las conclusiones. En este apartado alcanza con plasmarlo y resaltar que el tiempo insumido se debe en parte a los tiempos que actualmente demandan los diversos procedimientos policiales y/o judiciales (conocidos en la comunidad como "los tiempos de la justicia") y principalmente al agotamiento de todos y cada uno de los remedios procesales que la defensa interpuso a lo largo del proceso; hecho fundamental y positivamente valorado para la vigencia de un Estado de Derecho.

6 La ley 26.388 (conocida como ley de delitos informáticos) fue promulgada de hecho el 24 de junio del 2008.

Frente a los derechos efectivamente tutelados del reo, el andamiaje jurídico contiene un conjunto de derechos con el mismo nivel de preeminencia que acompañan a las víctimas de violencia de género. La República Argentina adoptó con rango constitucional normas que procuran tutelar los derechos de la mujer y en particular de esta cuando es sujeto pasivo de delitos por su condición de mujer. El andamiaje legal destinado a la protección integral de la mujer víctima de violencia de género, fue un vector a lo largo del proceso y los actores intervinientes, en su mayoría, procuraron amoldar sus actuaciones a estas normas.

Particularmente gravitaron en forma expresa en diversos actos procesales, derechos receptados en la "Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer" ("Convención de Belém do Pará") en lo que hace al Capítulo III, artículo 7 inc. F -norma de jerarquía constitucional conforme al art. 75 inc. 22 de la Constitución Nacional Argentina, mientras que se matizaron las diversas normas procesales con las reglas 11, 12, 67, 68, 69, 70, 76 y principios consecuentes de la Acordada nro. 5/2009 por la cual, la Corte Suprema de Justicia de la Nación Argentina, adhirió a las "Reglas de Brasilia sobre el acceso a la justicia de las personas en condiciones de vulnerabilidad". Finalmente, el artículo 16 inciso H e I de la ley 26.485 (ley de orden público) conocida como "Ley de Protección Integral para Prevenir, Sancionar y Erradicar la Violencia contra las Mujeres en los ámbitos en que desarrollen sus relaciones interpersonales" contribuyó a procurar la búsqueda del equilibrio entre el derecho de defensa del victimario, el debido proceso y el derecho de acceso a la justicia de la mujer víctima de violencia de género.

Conclusiones

El fallo comentado posee una especial trascendencia ya que los operadores jurídicos realizaron una interpretación holística de las normas en juego. Debido al buen arte de diferentes magistrados pertenecientes a diversas instancias procesales se hizo uso de los principios de razonabilidad y proporcionalidad para morigerar otros principios jurídicos tradicionales que informan al proceso judicial.

Por ello cabe destacar la loable labor de respetar todas y cada una de las garantías y defensas que puede utilizar en el proceso la persona acusada, pues hacen a las bases del Estado de derecho. Sin embargo, la interpretación de los derechos reconocidos a las víctimas de violencia de género (incorporadas al ordenamiento legal argentino con jerarquía constitucional) deben ser colocadas en pie de igualdad para evitar caer en discursos políticamente correctos que luego terminan en objetivos de cumplimiento imposible.

Ahora bien, no se quiere cerrar la intervención sin dejar de destacar que este importante precedente se logró gracias a la constante voluntad de la víctima para obtener una respuesta judicial a las características que se le atribuían en diversas plataformas digitales y que mancillaban la imagen que ella había autoconfigurado como mujer, madre y docente.

La gallardía de la víctima se trae a colación en el cierre de la intervención para invitar a la reflexión íntima de los lectores. Se propone una reflexión sobre el tiempo que el sistema jurídico actual precisa para brindar una solución o respuesta judicial a la sociedad del siglo

XXI. Para ello, se recuerda que en este caso particular se precisaron frioleros 3.962 días para determinar la responsabilidad penal del autor del ilícito. Por otro lado, se resalta que las propias plataformas ofrecen a los usuarios, dentro de su hábitat, la posibilidad de expiar estos conflictos mediante hechos conocidos como "escraches", que poco tienen que ver con el respeto de los derechos de los sujetos involucrados en el ilícito, pero que sin embargo otorgan mediante la exposición pública del supuesto "culpable" una sensación de justicia que, comparada en tiempo, para nada se condice con el consumido por el proceso judicial aquí analizado.

Referencias

Monografías y artículos:

Gillespie, T., "The Politics of Platforms" New Media & Society 12 (3) 2010. PAG. 347-364. Disponible en https://doi.org/10.1177/1461444809342738

Miró Llinares, F., "La oportunidad ciminal en el ciberespacio" Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen, Revista Electrónica de Ciencia Penal y Criminología. 2011, n.m. 13-07, p. 07:1-07:55.

Sheeban, P. "Greed of boomers led us to a total bust". The Sydney Morning Herald. 26 de septiembre de 2011.

Jurisprudencia:

Corte Suprema de Justicia de la Nación (República Argentina) conf. Competencia 351, L. XLVÍII in re "Jutton, Juan Carlos s/denuncia delito c/la seguridad pública", resuelta el 20 de noviembre de 2012.

Tribunal Oral Criminal Federal Número 1, Provincia de Mendoza, (República Argentina) en "R. B., C. R. s/ Coacción (art. 149 bis del CP) FMZ 13017007/2011/TO1" resuelta el 09 de marzo de 2022. Disponible en https://www.cij.gov.ar/d/sentencia-SGU-20cd6e0e-3971-4bab-a464-19f8f354150a.pdf y https://www.cij.gov.ar/d/sentencia-SGU-5d5d7ca5-b221-459c-af84-c7bef5696bf5.pdf

Legislación:

Ley Nacional número 26.388. (República Argentina)

Fundación
de Cultura
Universitaria

25 de Mayo 583 - Tel. 2916 1152
CP 11.000 Montevideo - Uruguay
libreria@fcu.edu.uy

www.fcu.edu.uy