

La cultura digital como factor de incidencia de la ciberdelincuencia

Patricia Stefany Balbin Linares^{1*}, Gerardo Francisco Ludeña González¹, Nilton Isaias Cueva Quezada¹

¹ Escuela de Posgrado. Universidad César Vallejo. Perú.

*Autor para correspondencia: Patricia Stefany Balbin Linares, pbalbinli793@ucvvirtual.edu.pe

(Recibido: 01-08-2023. Publicado: 16-09-2023.)

DOI: 10.59427/rccli/2023/v23cs.1810-1817

Resumen

La ciberdelincuencia ha registrado durante los últimos años un alto índice de daños a personas naturales como jurídicas en sus diferentes modalidades, siendo la falta de cultura digital el factor por el cual los ciberdelincuentes se valen para perpetrar sus ilícitos, el objetivo de la investigación fue identificar los factores que propician el accionar cibercriminal por la falta de cultura digital entendiéndose como tal las prácticas, costumbres y formas de comunicación social que se realizan mediante el empleo de las tecnologías de la información y la comunicación y el Internet. Metodología se efectuó la metodología de revisión sistemática a través de la revisión teórica de fuentes secundarias, disponible en la base de datos Scopus, Ebscohost, Dialnet, Scielo y Redalyc. Se utilizó la búsqueda y revisión de producción científica filtrando los términos de: "cultura digital" y "ciberdelincuencia". Los resultados refieren que la comunicación digital transforma la cultura y la producción, pero los ciberdelitos requieren medidas preventivas internacionales. Los jóvenes son los principales usuarios de las TIC y las redes sociales pueden promover contravalores. La falta de definición de la ciberdelincuencia dificulta su prevención. La transformación digital afecta nuestra forma de vida y se necesita más investigación sobre problemas sociales relacionados con las TIC. Medidas de prevención individualizadas pueden evitar delitos cibernéticos. Se concluye la importancia para las personas de cultivar una conciencia de seguridad en el buen empleo y manejo de las TIC e Internet, estableciéndose una cultura digital con medidas acertadas para precaver la incidencia de la ciberdelincuencia.

Palabras claves: Cultura digital, ciberdelincuencia.

Abstract

The cybercrime has registered in recent years a high rate of damage to natural and legal persons in its different modalities, being the lack of digital culture the factor by which cybercriminals are used to perpetrate their crimes, the objective of the research was to identify the factors that lead to cybercriminal action due to the lack of digital culture understood as such the practices, customs and forms of social communication that are carried out through the use of information and communication technologies and the Internet. Methodology The systematic review methodology was carried out through the theoretical review of secondary sources, available in the database Scopus, Ebscohost, Dialnet, Scielo and Redalyc. The search and review of scientific production was used, filtering the terms "digital culture" and "cybercrime". The results indicate that digital communication transforms culture and production, but cybercrimes require international preventive measures. Young people are the main users of ICTs and social networks can promote counter-values. The lack of definition of cybercrime makes it difficult to prevent. Digital transformation affects our way of life and more research is needed on ICT-related social issues. Individualized prevention measures can prevent cybercrime. It concludes the importance for people to cultivate an awareness of security in the good employment and management of ICT and Internet, establishing a digital culture with accurate measures to prevent the incidence of cybercrime.

Keywords: Digital culture, cybercrime.

1. Introducción

La cultura digital es reconocida por las posibilidades de liberar la accesibilidad a la información y el conocimiento, pudiendo incluso ser útil en la difusión de movimientos de sustentabilidad, coyuntura que es utilizada por la ciberdelincuencia. En general, la tecnología social implica algunas reflexiones, como la inclusión social, la participación ciudadana, la emancipación de los sujetos y las construcciones comunitarias, con vistas al término de problemas sociales, ambientales y económicos, entre otros (Cultri y Bazilio, 2021). Se aprecia que los elementos de la cultura digital son: los nuevos tipos de interacción, comunicación, compartir y acción en la sociedad entrelazados con la educación (Brito & Furlan, 2020). Los estudiantes reconocen la importancia del empleo del Internet, predominando la utilización, el exceso, la falta de consideración, la indecencia, los riesgos agregados a la información, testimoniando la existencia de contravalores en las redes sociales (Renés et al., 2021).

El incremento de la tecnología asimismo ha transportado nuevas formas delictivas que tienen por medio los sistemas informáticos e internet (Leyva, 2021). El deterioro de las dimensiones de seguridad de la información y los delincuentes más inteligentes amenazan a las personas, las organizaciones y las naciones con delitos cibernéticos más nuevos, innovadores y más enfocados (Shashi et al., 2020). La ciberseguridad, ha sido regulada en cierta medida por normas administrativas y penales, pero algunas intervenciones constitucionales resultan de especial importancia (Fernandez, 2021).

El presente artículo expone una revisión de aplicaciones en relación al empleo de las TIC en la actualidad, las mismas que por la carencia de cultura digital son aprovechadas por los ciberdelincuentes para la ejecución de hechos delictivos en sus diferentes modalidades, con el objetivo de identificar e indagar los factores que propician la falta de cultura digital, de como la ciberdelincuencia aprovecha la falta de cultura de ciberseguridad como brecha de inseguridad y brindar aportes de cultura digital como iniciativas para cerrar brechas a la ciberdelincuencia.

2. Metodología

La metodología que se utilizó fue un estudio y revisión sistemática de producción científica relacionada al tema, iniciándose la búsqueda de información en revistas indexadas a nivel de Latinoamérica, Europa, Asia y África en ficheros digitales de Scopus, Doaj, Ebsco, Dialnet y Redalyc. Se realizó en el ámbito de una verificación ordenada de artículos de elaboración científica, el cual incluía: identidad del autor o autores, año, denominación, origen, DOI y menciones.

Se introdujeron estudios sobre la cultura digital como factor que contribuye a la incidencia de la ciberdelincuencia en sus diferentes modalidades, siendo excluidas aquellas verificaciones de literatura de creación teórica o que no sean parte del tema investigado. Considerando la cantidad restringida de investigaciones sobre la cultura digital y la ciberdelincuencia, el objetivo de esta reseña es analizar los conocimientos existentes sobre el asunto e identificar en los productos de estudio, los planteamientos de formación, clases, variables y ponderaciones. Se escogieron como productos principales los consecuentes, sucesos de estudios, indagaciones empíricas, comprobaciones y semejantes. Se realizó una indagación manejable empleando menciones de estudios preferentes y complementarios hallados en la averiguación digital. Las indagaciones se efectuaron abiertamente en la base de datos Scopus, Doaj, Ebsco, Gale y Redalyc, habiéndose tenido como principio la búsqueda por títulos, síntesis y por las palabras clave "Cultura digital" y "ciberdelincuencia".

El desarrollo de recopilación de las investigaciones fue efectuado por el investigador. Los estudios se eligieron referenciado dos periodos. Como primer avance se fundamentó reexaminando los títulos y síntesis de citas halladas con variadas pericias de búsqueda, distinguiéndose las investigaciones eventualmente elegibles. De la averiguación sistemática y conjugación se obtuvo una muestra de 30 resultados. Como segundo avance se procedió investigando el texto completo de las investigaciones preseleccionadas para ratificar su elegibilidad, dando en total de 18 artículos.

3. Resultados

En la tabla 1 se explica los artículos seleccionados abordando su relevancia:

Tabla 1: Autores de textos y de revistas científicas indexadas cuyos contenidos fortalecen el tema de estudio.

Autores/ Año/ Título	Base de Datos	Tipo de Estudio	Métodos	Resultados	Conclusiones
Aleksey, (2020). Manifestaciones Sociales de la Cultura Digital.	Elsehost	Estudio Cualitativo	Enfoques sistémicos y dialécticos	La naturaleza cambiada de las Comunicaciones se está convirtiendo en una manifestación social de la cultura digital.	El poder tecnológico el surgimiento de un lenguaje especial de comunicación; programabilidad del comportamiento humano; formalización y fragmentación de los procesos de comunicación; el predominio del pensamiento clip; ecologismo, son manifestaciones sociales de la cultura digital.
Arellano (2020). Las brechas digitales en México.	Redalyc	Estudio Cualitativo	Metodología de cálculo	Los ties han ejercitado una transformación en la estructura de la producción como en su composición.	En las políticas públicas debe considerarse el desarrollo del ecosistema digital y el derecho ciudadano al acceso universal del internet; el empleo de las tecnologías en salud, educación, sectores productivos y la administración pública.
Avila (2018). Las menores víctimas de la ciberdelincuencia.	Elsehost	Enfoque cualitativo	Descriptivo	Las dimensiones preventivas que se fijan para los ciberdelitos que dañan a la niñez, deben adoptarse por las Naciones Unidas, organizaciones internacionales y los países.	Los padres de familia y las comunidades ejercen un rol crucial en el momento que un niño pueda o no ser víctima por el ciberdelito, a través de la protección en uso de las TICs.
Cherniavskiy et al. (2021) Measures to combat cybercrime: analysis of international and Ukrainian experience.	Elsehost	Estudio Cualitativo	Descriptivo	Los estados en el mundo se están espaciando y creando entidades y servicios que fomentan el desarrollo de competencias acometidas en el ciberespacio.	La ciberdelincuencia, es consecuencia del bajo nivel de formación en tecnologías de la información.
Escuder (2019), Santiago (2019). Regionalización de la brecha digital. Desarrollo de la infraestructura de las TIC en Latinoamérica y Uruguay.	Redalyc	Enfoque Cuantitativo	No experimental	Los espacios de acceso a las TICs, se hallan descartados o precarizados tecnológicamente como consecuencia de complejas contingencias territoriales.	El problema de la brecha digital, retroalimenta el círculo repetido de la dinámica de la disparidad social.
Flores et al. (2020). Tecnologías de información: Acceso a internet y brecha digital en Perú.	Redalyc	Estudio Cualitativo	Revisión documental	La población juvenil es la que mayormente accede a internet y que el dispositivo más utilizado es el móvil.	Es necesario tomar conciencia respecto a la brecha digital que adolece distintos lugares del Perú, y los cambios urgentes en la infraestructura de las telecomunicaciones y el acceso al internet.
Mordvinov y Udevikina (2022). Ciberdelincuencia en Rusia: desafíos actuales y buenas prácticas en la lucha contra la ciberdelincuencia.	Doaj	Enfoque cualitativo	Descriptivo	La transformación digital en relación con el ciberdelito, tiene como tendencia: el aumento de la actividad de los intrusos, la modernización de los métodos para cometer y ocultar delitos utilizando las TICs.	En la era de la globalización, la transformación digital y el rápido desarrollo de las tecnologías informáticas y de TI, la sociedad moderna, aprovecha las nuevas tecnologías y se enfrenta a la ciberdelincuencia.
Mpashieu y Mahler (2022). La ciberseguridad como respuesta para combatir el ciberdelito.	Elsehost	Estudio Cualitativo	Revisión documental	La falta de una definición de ciberdelincuencia, tiene un impacto en su prevención asociado con la comisión del ciberdelito.	El cibercrimen y la ciberseguridad son conceptos surgidos en las últimas décadas. Sin embargo, la ciberdelincuencia es una actividad delictiva que ocurre en el ciberespacio e involucra una red informática y un usuario de la red.
Quijano (2018). Jóvenes y cultura digital: abordajes críticos desde América Latina.	Gale	Estudio Cualitativo	Revisión documental	Las investigaciones sobre la juventud y la cultura digital guían a calificar el perfil de los jóvenes que utilizan los entornos digitales como medios de interacción, afinidad, aprendizaje y ocio.	Resulta inviable hablar de una única cultura digital, porque existen variadas culturas digitales que se entrelazan con las culturas juveniles.
Renés et al. (2021). Countervailing of the digital ethos perceived by future trainees.	Scopus	Estudio Cualitativo	Revisión documental	Las redes sociales mediante sus foros, se han convertido espacios para encontrar y exponer contravalores, siendo algunas de sus expresiones la enemistad o el egoísmo.	Los estudiantes identificaron los peligros y los vincularon con desigualdades o vulnerabilidades de las personas, al enfrentarse a la cantidad de información y costumbres existentes en las redes de Internet.
Risquete (2018). De la cultura a la cultura digital: nuevos escenarios en una nueva era.	Gale	Estudio Cualitativo	Descriptivo	La digitalización actúa en el orden cultural y, en las actuales formas de comunicación que prevalecen en las nuevas formas de vivir el tiempo y el espacio.	En la cultura digital los modernos escenarios se vinculan con la educación, la religión, los gustos y estilos de vida, la cultura popular, la sociedad del espectáculo.
Rojas (2022). Panorama de riesgos por el uso de la tecnología en América Latina.	Redalyc	Estudio Cualitativo	Revisión documental	Se evidenció que los problemas sociales relacionados al uso de las TICs son permanentes, pero con carencias investigativas en varias de ellas.	En el contexto latinoamericano falta más desarrollo investigativo y publicación científica con respecto a las consecuencias negativas del uso tecnológico.
Veresha (2018). Preventive Measures against Computer Related Crimes: Approaching an Individual.	Elsehost	Estudio Cualitativo	Descriptivo	Tomar medidas de prevención individualizadas para las personas propensas a cometer delitos cibernéticos evitará que estos ocurran incluso antes de que ocurran.	La prevención individualizada es necesaria entre las personas con mayor probabilidad de cometer delitos contra la ciberseguridad.

El primer artículo presentado por (Aleksey, 2020), sobre Investigación original realizada en Rusia; La digitalización, según los científicos, comprende la producción, los negocios, la ciencia, el entorno social y el diario vivir de los ciudadanos, lo que exige la elaboración de cada miembro de la sociedad para la interacción con el entorno digital. Los procesos que se desenvuelven en la sociedad generan un nuevo tipo de cultura de la afluencia moderna la cultura digital. Concluyo que es posible diversificar las manifestaciones sociales de la cultura digital, como el poder tecnológico, el surgimiento de un estilo especial de comunicación, la formalización y fraccionamiento de los procesos de comunicación, disminución de su contenido ético, abandono de la persona en el problema de la confort personal; la influencia del pensamiento clip, tecnologismo.

La segunda es una publicación hecha por Arellano (2020), de su artículo de investigación hecho en México; Se obtuvo como resultado descubrimientos en la investigación que indican la presencia de un avance relativo en el aumento y el beneficio de las tecnologías digitales en el estado. Sin embargo, continúan las brechas digitales respecto de las mejores praxis internacionales. Se colige que la táctica digital nacional, como título de política pública sobre la causa, plantea cinco objetivos: transformación pública, formación de calidad, economía digital, fortaleza efectiva universal y seguridad ciudadana. Al mismo momento, se proponen cinco facilitadores esenciales como herramientas transversales: siendo la conectividad, la interoperabilidad, la inclusión y habilidades digitales, los datos abiertos y el marco jurídico.

El tercer artículo mostrado por Avila (2018), investigación realizada en Colombia. Se efectuó el estudio de las intervenciones teóricas y las dimensiones preventivas que sujetan a los ciberdelitos que perjudican a menores de edad y de las medidas tomadas por la Organización de las Naciones Unidas, organismos internacionales y algunos países. Se destaca como principal conclusión que los padres y sus familiares ejercitan un rol fundamental al momento que un menor pueda o no ser dañado por un ciberdelito, mediante la vigilancia en uso de las Tic.

El cuarto artículo entregado por Cherniavskiy, estudio original de Ucrania; se realizó el análisis de las medidas empleadas para hacerle frente al ciberdelito en diferentes países. El procedimiento utilizado fue la observación de normas utilizadas para hacerle frente al ciberdelito en diferentes países. Los resultados apuntaron que la normatividad jurídica en la lucha contra el ciberdelito es la raíz de todo el sistema de lucha contra el ciberdelito. Finalizaron indicando que los ciberdelitos sí tienen un elevado grado de peligrosidad pública, con consiguientes daños económicos, psicológicos y otros, así como que requieren de conocimientos y habilidades en el campo de la tecnología informática. Uno de los aspectos que dificulta el ciberdelito es el bajo nivel de educación en TI de las personas de diferentes países.

El quinto artículo prologado por Escuder (2019), exploración original realizada en México; tuvo un diseño metodológico que explora el fenómeno de la brecha digital tanto a nivel continental, como en los diferentes provincias de Uruguay y barrios de Montevideo. En sus conclusiones señalaron que el problema de la brecha digital no produce más que retroalimentar el perímetro vicioso de la activa diferencia social. Los sectores alejados digitalmente convienen con la exclusión espacial y socio-económica de los hogares enclavados en los barrios más contiguos.

El sexto artículo dado por Flores et al. (2020), investigación original realizada en Venezuela; Los resultados mostraron que adolescentes y jóvenes son los que poseen un considerable acceso a internet (80,5 %) y que el teléfono móvil fue el medio más empleado para tal fin (81,0 %). Concluyeron tomar más conciencia sobre la brecha digital existente en varios sectores del Perú, además de apremiar una transformación en la proporción de la infraestructura de telecomunicaciones y las facilidades de acceder al internet en el estado.

El séptimo artículo entregado por Mordvinov y Udavikhina (2022), investigación original realizada en Rusia: Sus resultados precisan que existen dos tendencias: por un lado, el incremento de la actividad de los intrusos como consecuencia del avance tecnológico, la modernización de las modalidades para cometer y ocultar delitos utilizando las TICs; por otro lado, las formas de vigilar las transacciones financieras y de propiedad, la transparencia de la interacción entre los pobladores y el estado, y mucho más. Se coligió que el desarrollo y la implementación de prácticas victoriosas para combatir el ciberdelito utilizando TICs requieren la consolidación de impulsos para organizar una investigación integral que agrupe a científicos y profesionales líderes para solucionar problemas apremiantes en el área de la protección de la información.

El octavo artículo presentado por Mphatheni y Maluleke (2022), publicación académica efectuada en Sudáfrica. Los resultados indican la diferencia de la delincuencia común, la ciberdelincuencia no detenta fronteras geográficas. No necesita ningún contacto físico entre el delincuente y la víctima. Lo puede perpetrar un individuo, una empresa o un país contra alguna persona o una empresa de otro país. Los Estados seguirán enfrentándose a obstáculos para evaluar la legalidad de su respuesta a un ataque dado en ausencia de una explicación internacional integral de los tipos de ataques cibernéticos.

El noveno artículo expuesto por Quijano (2018) investigación desarrollada en Ecuador. Se destaca que las investigaciones de la nublidad y la cultura digital, propenden a caracterizar la figura de las colectividades jóvenes conectadas y urbanas, que concurren en los dominios digitales como sitios de interacción, elaboración de la identidad, ocio, aprendizaje, participación política. Se concluyó que no es posible discutir de una única cultura digital, ya que existen variadas culturas digitales que se entrelazan con las culturas juveniles.

El décimo título presentado por Renés et al. (2021). investigación científica hecha en España. Los estudiantes determinaron a través de sus alocuciones riesgos y la vinculación a la desigualdad o vulnerabilidad de las personas cuando se confrontan a demasiada información y contenidos en las redes de Internet, principalmente en riesgos asociados a la información; o a la existencia de contenido. Se demostró que muchos de los estudiantes reconocen la existencia de contravalores al emplear Internet, preponderando la violencia y la manipulación, la falta de tolerancia, la desigualdad y la falta de honradez, así como los peligros afiliados a la información y la comunicación, evidenciando la existencia implícita de contravalores en los discursos de las redes sociales.

El décimo primer artículo enseñado por Risquete (2018), investigación original realizada en España. La digitalización tiene un gran dominio en el orden cultural y muy significativamente en las novedosas dinámicas de comunicación que predominan las formas de comprender y vivir el espacio y el tiempo, nuevas vinculaciones de la cultura local y la cultura global. Infirió que los actuales marcos de la cultura en la era digital, la examina en su relación digital con la educación, los gustos, la religión, estilos de vida, la cultura pública, la sociedad del espectáculo, el deporte, los ídolos hasta su correlación con la ideología o el nacionalismo.

El décimo segundo enunciado formulado por Rojas (2022), investigación efectuada en Colombia. Se evidencio que los problemas sociales afiliados al uso de las TIC se encuentran en las regiones, con carencia investigativa en varias de ellas. Se deduce la exigencia de ampliar los estudios en estos problemas para nivelar la apropiación tecnológica y los efectos de uso irreflexivo, acrítico e indeterminado de las TIC.

El décimo tercer artículo ofrecido por Veresha (2018), estudio original realizada en Ucrania; Las medidas preventivas contra cualquier tipo de delito se suelen fraccionar en comunes, especiales e individualizadas. Dedujeron la necesidad de promover en las personas hábitos de precaución para impedir peligros o riesgos, y tomar acciones preventivas para no ser víctimas de ciberdelincuencia. Esto se aplica primeramente a los jóvenes, porque este segmento particular de la población es más proclive a cometer ciberdelitos. El estudio determinó que las medidas preventivas específicas contra el ciberdelito implican la innovación de la denominada Ciberética que incluye la mejora de la cibercultura entre las personas, principalmente niños y adolescentes, a través de proyectos de difusión y educación.

4. Discusión

La sociedad en la actualidad experimenta una permanente transformación y crecimiento. La Cultura Digital aparece con modernas praxis sociales que vienen modificando grandes aspectos de nuestras actividades, que denominamos Cultura Digital, siendo sus elementos fundamentales el Internet y la Tecnología, que ha reformado el mundo y de cómo interactuamos en el mismo. Los diferentes dispositivos electrónicos facilitan nuevas y variadas oportunidades, concediéndonos beneficios económicos, educativos, sociales y otros. Por ello, la Cultura Digital se puntualiza como el cúmulo de experiencias, estilos y formas de comunicación social mediante el empleo de los recursos de las TICs y el Internet, que viene generando un impacto en las diferentes fases sociales de la vida humana.

La cultura se desarrolló a través del tiempo en contenidos existentes, y en esta nueva era denominada digital observamos que se desenvuelve en el ciberespacio. En este espacio virtual las personas se asocian por intereses habituales, generan vínculos laborales, políticos, sentimentales y otros. Tal como lo refiere Risquete (2018) en su artículo, al referirse que la digitalización influye en el orden cultural, muy en especial en las novedosas formas de comunicarse, de cómo percibir y existir en el tiempo y el espacio, así como los nuevos vínculos entre la cultura del lugar y la cultura global. Los recientes medios de la cultura en la era digital estudian su relación con la educación, la política y los estilos de vida, la sociedad, el deporte y otras actividades. En su artículo Quijano (2018) relata que la cultura digital y las tecnologías digitales se apropiaron de un lugar céntrico. La estancia de contextos digitales ha transformado el aspecto primordial de la cotidianidad del existir, al extremo que en los entornos familiares y educativos involucra la preocupación para recobrar las dimensiones presenciales de interacción y socialización. Las nuevas generaciones de hoy cuentan con destrezas digitales que los diferencian de generaciones pasadas. Es por ello que en la actualidad hablamos de nativos digitales cuando nos referimos a esta nueva posición psicocognitiva para el empleo de la tecnología, con fluidez en el manejo de los equipos de cómputo, los videojuegos e Internet. Asimismo, existen ciertas características dentro de los entornos tecnológicos, como el tipo de conectividad, velocidad de la conexión, formas de conectarse, y los hábitos en el internet. Los científicos indican que la digitalización, alcanza a la ciencia, el medio social y el diario vivir de los ciudadanos, lo que demanda la preparación de cada integrante de la población para la socialización con el entorno digital. Los procedimientos que se desenvuelven en la sociedad generan un nuevo tipo de cultura de la humanidad moderna denominada la cultura digital. Conuerdo con el artículo de (Aleksey, 2020), al señalar que la apertura y accesibilidad de la información genera que los jóvenes ya no necesiten de los adultos; Ellos crean su particular forma de comunicación. Las principales preferencias de comportamiento se inician en Internet identificándolos como la generación Z, quienes se conducen por los intereses del individualismo, siendo el sentimiento de su particularidad, la pretensión de popularidad. Los primordiales temores de los jóvenes son el miedo a la soledad y la carencia de confianza en sus capacidades comunicativas. En su artículo Renés et al. (2021). indica que esta generación enfrenta gran cantidad de información y contenidos en las redes de Internet, identificaron que existe desigualdad y vulnerabilidad en las personas en riesgos referentes a la información, la existencia de contenidos en el que se incita a la violencia, el entusiasmo a través de las redes, errores por falta de discernimiento, así como los riesgos vinculados a los procesos comunicativos. Convengo con el autor respecto a que las páginas webs, videos o redes sociales son entendidos como lugares en que las personas pueden difundir contravalores en redes sociales, como cuando se exponen en Twitter o Instagram espacios donde manifiestan sus opiniones y pensamientos, accediéndose a publicaciones xenófobas o inapropiadas que no solo acarrear espacios de discriminación, sino que fomentan focos de victimización que pueden generar cuestiones de autoestima o depresión.

El empleo de las TIC ha generado, variabilidad social que demuestra bienestar y crecimiento en la sociedad. Pero, también ha exteriorizado diferentes modelos de problemas afiliados al uso de la tecnología, como las ciberadicciones, los ciberdelitos y la utilización discutible del internet, las cuales, a pesar de su relevancia e impacto, carecen de una percepción amplia y adecuada que admita el diseño de actuaciones de intervenciones eficaces y oportunas. A ello debe sumarse el bajo nivel de educación en las TIC como fenómeno problemático en las poblaciones. Del estudio respecto a la transformación y las preferencias del paradigma digital se precisa que el atraso de las naciones en desarrollar su empleo e implementación de tecnologías para mejorar espacios productivos y tecnológicos podría extender su situación de subdesarrollo, manifestándose persistente atraso tecnológico, la centralización económica y la disparidad social. Asimismo, países y regiones se encuentran excluidos o precarizados tecnológicamente como consecuencia de diversos contingentes territoriales. Según Symantec Security, cada año se generan en el mundo unos 556 millones de ciberdelitos, con perjuicios superiores a los 100.000 millones de dólares. En su artículo (Cherniavskyi et al., 2021), refiere que los delitos cibernéticos sí poseen un elevado grado de peligrosidad pública, debido a que las actividades que los constituyen son difíciles de implementar, requiriendo conocimientos singulares en el campo de la tecnología informática. Esto representa que el empleo de los métodos existentes de defensa contra ellos también necesita de un nivel de concienciación. Por ello, una de las figuras problemáticas del fenómeno del delito informático es el débil nivel de educación en TI de las personas de distintos países. El problema es que la tecnología informática genera dificultades de control, por lo que es importante que las personas, conozcan los métodos de protección más sencillos que no requieran de un conocimiento profundo. Sin duda, el funcionamiento de los sistemas de información, en particular de Internet, requiere del trabajo conjunto de distintos actores, públicos como privados, para estar dirigidos a resolver los problemas de ciberseguridad.

Cabe indicar que en su producto Flores et al. (2020), alude que el aumento y uso del Internet ha ocasionado cambios trascendentales en la sociedad; tales como estudiar, trabajar, comprar, entre otros, repercutiendo la percepción de la interactividad humana, reformando la óptica del mercado, generando novedosas economías digitales que se reforman con innovaciones y resultados; pero uno de los primordiales obstáculos lo constituye lo referido a la brecha digital, concibiéndose como el fenómeno de la separación respecto del acceso y utilización de las TIC en diversos aspectos como económicos, geográficos, culturales, entre otras, que entorpece el desarrollo. Cabe precisar que el acceso a Internet resulta reducido y no ha llegado a todos los lugares, apreciándose una mayor concentración del acceso en sectores urbanos con relación a las rurales. Es la brecha digital, la que produce diferencias de oportunidades de desarrollo en las poblaciones y que distancia entre aquellas que tienen o no tienen acceso a las mismas.

El criterio de brecha digital ha cambiado, ya que al principio se aludía a problemas en relación con la conectividad y después al desarrollo de las capacidades y cualidades requeridas para utilizar eficientemente las TIC. Escuder (2019) precisó que la falta de acceso a la infraestructura y conectividad, se le define como brecha digital y representa una nueva desigualdad social. Estoy de acuerdo con el autor al indicar que el acceso a las TIC puede obedecer a factores, como los lugares con conectividad, la rapidez de la red (banda móvil o fibra óptica). A ello es importante tener en cuenta la calidad del performance de los dispositivos como el almacenamiento, memorias entre otros. Se considera también que los recursos y acceso a las TIC se consolida entre las personas, hogares o empresas de conformidad con el lugar geográfico donde viven. El espacio territorial también constituye nuevas desigualdades de utilización e implantación de contenidos en internet. Resulta distinta la velocidad y consumo del internet si se conecta mediante las TIC desde el trabajo, el centro educativo y el hogar; desde un sitio rural que una urbana. Queda claro que el rápido avance en las innovaciones que se estudia en torno a los diversos rubros que establecen las tecnologías digitales configura un dominio cambiante de oportunidades y desafíos para fomentar el crecimiento y el bienestar social en economías emergentes, por lo que estoy coincido con Arellano (2020) quien determinó que el paradigma digital está cambiando las tendencias de la producción global, los procedimientos de trabajo, las formas de negocios, los modelos de consumo y el ciclo de los productos. Las transformaciones asociadas con el sistema de las TIC, que se corroboran en las empresas y su nexos con socios, clientes y proveedores, pueden impulsar a una mejora considerable de la productividad y la competitividad. La estrategia digital plantea entre sus objetivos la conectividad, la inclusión digital y los datos abiertos. En internet el menor detalle se puede maximizar, produciendo presión social tan fuerte que genera un control social muy marcado. Acciones de hostilidad en internet y redes sociales son en la actualidad causas de peligro de comportamiento, ya que contenidos en la web podrían propiciar y favorecer riesgos de enfermedades mentales para los jóvenes; en su artículo Rojas (2022), determina que ante estos hechos, las decisiones de seguridad en el ciberespacio vienen siendo dirigidas por empresas privadas y organismos civiles, y que existe interés de los organismos públicos por proteger el ciberespacio en sus estados. Sin embargo, factores como la carencia de información, la falta de conocimiento sobre sus prácticas, padres con desconocimiento del medio, posibilidades de alternativas de prevención y participación, y el desconocimiento del Estado sobre la problemática del uso de las nuevas tecnologías de la información, genera articulaciones legales y publicas precarias y anticuadas para la realidad tecnológica actual.

La globalización diluye las fronteras entre los países contribuyendo a propiciar una delincuencia mejor organizada, que con el empleo de las tecnologías amplían sus actividades delictivas, generando la aparición de nuevas formas de ciberdelitos que tienen como espacio de complicidad el ciberespacio. La sociedad moderna se transforma con el desarrollo de las TIC, siendo uno de los primordiales problemas el construir una doctrina legal integral de dimensiones en seguridad de la información. Las herramientas que emplean los cibercriminales para consumir sus ilícitos tienen la complicidad del Internet, correo electrónico, redes sociales entre otros. Según Symantec, cada año unos 378 millones de personas son víctimas de ciberdelitos, que equivale a 12 víctimas por segundo. Por lo que se deduce que el mal empleo de las TIC y el Internet, propician el paso de la ciberdelincuencia transnacional. Las nuevas víctimas son especialmente grupos vulnerables, como los menores de edad, quienes debido a su falta de madurez física y mental, suelen ser objetivo fácil de la ciberdelincuencia. La ciberseguridad debe ser prioritaria en todos los ámbitos de la sociedad si deseamos facilitar el verdadero potencial de la seguridad digital. El Foro Económico Mundial (2022) subraya que las tendencias digitales y su desarrollo exponencial como consecuencia de la pandemia del coronavirus (COVID-19) han impulsado a las poblaciones del mundo un nuevo camino de digitalización e interconexión.

Conductas delictivas en el ciberespacio, como el cyberbullying son formas de agresión entre menores mediante el Internet, empleando el anonimato y formas interactivas de contacto continuas y permanentes a lo largo de tiempos ilimitados contra una víctima que no puede protegerse. Otra forma de ciberdelito contra menores es el child grooming, donde se contacta un adulto adoptando una identidad falsa haciéndose pasar como un menor a través de Internet con el objeto de seducir y obtener su confianza, para obtener material de connotación sexual para engancharlo y obligarle a realizar actos en contra de su voluntad e incluso citas posteriores en el ámbito físico. Adicional a ello, será fundamental el papel que ejerzan los padres y familiares como vigilantes de la navegación que realicen los menores en el ciberespacio. Por lo que resulta necesario determinar protocolos y programas de naturaleza pública y privada orientada al empleo seguro de la red en el ciberespacio de los menores de edad.

Asimismo, la educación es una acción preventiva muy importante que debe propiciarse en los menores, mediante el diseño de actividades formativas para promover un entendimiento crítico de las interacciones abusivas y violentas en la red. El aumento e implementación de habilidades exitosas para combatir el ciberdelito empleando las TIC requieren de la consolidación de trabajos para organizar una investigación total que concentre a científicos y profesionales líderes en solucionar problemas urgentes en la seguridad de la información (Mordvinov et al., 2022) en su artículo nos advierte que una de esas tareas sería la participación de piratas informáticos éticos en la contienda contra el ciberfraude por ejemplo, así como propiciar cursos formativos sobre hacking ético requeridas por las personas apasionadas en la ciberseguridad.

En la Federación Rusa, la localización de personas que perpetran actos ilegales utilizando las TIC se debe, al avance de los centros del Estado SOPKA, y los sistemas Antifraude de las agencias bancarias, que identifican transacciones sospechosas en cuentas financieras y asegura su bloqueo temporal; así como el desarrollo de actividades educativas entre los pobladores sobre los algoritmos del trabajo de los ciberestafadores y el método en caso de conflicto con ellos, que realizan las fuerzas del orden, los bancos y las empresas de TI; también el mejoramiento de la legislación rusa en la denominación de este tipo de delitos. Durante el desarrollo de un ciberdelito, la acción requiere de alguien que cuente con habilidades y conocimientos que aventajen a los del usuario empleando como medios dispositivos electrónicos e Internet. A semejanza de los delitos comunes que se realizan en un espacio físico particular, los ciberdelitos suceden en la intangibilidad del ciberespacio, donde los ciberdelincuentes permanecen anónimos y, casi siempre, son imposibles de rastrear. Por ello, el ciberdelincuente se siente invulnerable y diseña ciberataques cada vez más sofisticados. Concilio con Mphatheni y Maluleke (2022) que refiere que las nuevas características que emergen en el ciberespacio generan oportunidades en persistente evolución para los ciberdelitos, dichas características se traducen en oportunidades transformadoras clave, siendo estas la Globalización, las Redes de distribución, los Sinópticos y panoptismo y el rastro de datos. Las cifras estadísticas demuestran que se requiere de medidas individualizadas para hacerle frente al cibercrimen, debido a que la mayor cantidad de los ciberdelitos se generan en el hogar, en los cibercafé y en los centros de estudio con dispositivos tecnológicos personales. Otro dilema es la elaboración de medidas penales orientadas a garantizar la ciberseguridad de los menores que contribuya a coadyuvar su normal desarrollo y su seguridad en todos sus niveles, Veresha (2018) en su artículo nos explica la necesidad de introducir medidas preventivas más efectivas como la mejora de la cibercultura entre las personas, en especial la de los niños y adolescentes, mediante proyectos educativos y científicos que promueva en las personas una elevada cultura de comportamiento en el ciberespacio. Para ello, las organizaciones públicas como las privadas deben implementar este tipo de proyectos orientados a crear la llamada Ciberética. También deben aplicarse estrategias de prevención personalizadas a las personas propensas a cometer ciberdelitos contra la ciberseguridad. Las acciones preventivas vinculan a la participación de órganos gubernamentales encargadas en la búsqueda de dichas personas. Para ello es exigido criterios especiales para reconocer a las personas proclives a cometer los ciberdelitos antes de que consumen sus esfuerzos a cometerlos.

5. Conclusiones

Los ciberdelitos tienen un gran grado de peligrosidad pública, toda vez que sus actividades son complejas, además de requerir conocimientos de las TIC. La falta de conciencia de seguridad para defendernos y la limitada educación en Tecnologías, suman a la incidencia delictiva. Asimismo, la brecha digital, fenómeno que restringe el acceso a información y utilización de las TIC en diversas actividades humanas, dificulta el desarrollo, generando diferencias en las oportunidades de las poblaciones, que marca distancias entre aquellas que no tienen acceso a las mismas. También la falta de acceso a la infraestructura y conectividad, representan una nueva desigualdad social. El espacio territorial constituye una nueva desigualdad de utilización e implantación de contenidos en internet. Finalmente, la falta de información y buenas prácticas, el desconocimiento de los padres del entorno informático, las alternativas de prevención y participación, y el desconocimiento del Estado sobre el problema del buen uso de las nuevas tecnologías, genera articulaciones legales y públicas precarias y anticuadas para la realidad tecnológica actual. La cultura digital se desarrolla en el entorno virtual denominado ciberespacio, por lo que su digitalización influye en las nuevas formas de comunicarse, así como su relación con entornos familiares, la educación, los estilos de vida, la sociedad, entre otros. Asimismo, la nueva generación de nativos digitales cuenta con destrezas digitales, lo que demanda preparación para una mejor socialización con el entorno digital. La cultura digital al proporcionarnos mayor acceso a mayor información ha generado en los jóvenes la no dependencia de los adultos con nuevas formas de comunicación a través del Internet, con rasgos de individualismo, particularidad y popularidad. Ello también ha conllevado a que identifiquen desigualdad y vulnerabilidad en las personas, riesgos en la información y la existencia de contenidos inexactos, incitando a la violencia, dependencia de las redes sociales, así como errores por falta de discernimiento en los procesos comunicativos. Las medidas preventivas hacia los menores sobre los ciberdelitos, deben orientarse a evitar victimizaciones, así como intervenir en los grupos de cibervulnerabilidad, por su falta de desarrollo y madurez emocional. Es fundamental la participación de la familia como vigilantes en el ciberespacio, por ello urge la necesidad de establecer protocolos y programas públicos y/o privados que promuevan el empleo seguro del ciberespacio en los menores de edad. La educación es un factor preventivo muy importante, debiendo diseñarse actividades educativas que promuevan hacerle frente al ciberdelito mediante el empleo de las TIC, propiciando cursos formativos sobre hacking ético como medida de ciberseguridad. Finalmente, para hacerle

frente al cibercrimen, resulta necesario la elaboración de medidas penales orientadas a garantizar la ciberseguridad de los menores que permita su normal desarrollo y seguridad en la red, así como medidas preventivas más efectivas como la cibercultura entre las personas, que fomente el buen comportamiento en el ciberespacio.

6. Referencias bibliográficas

- Aleksey, S. (2020). Social manifestations of digital culture. *Humanitarian Vector*, 15(4), 46–52.
- Arellano, M. (2020). The digital gaps in Mexico: a relevant balance. *Trimestre Economico*, LXXXVII(2), 367–402.
- Avila, J. (2018). Los menores víctimas de la ciberdelincuencia. *Cybercrime. Advocatus*, 31, 79–90.
- Brito, G., & Furlan, M. (2020). Apresentação - Cultura digital e educação: desafios e possibilidades. *Educar Em Revista*, 36, 1–7.
- Cherniavskyi, S., Babanina, V., Mykytych, O., & Mostepaniuk, L. (2021). Measures to combat cybercrime: analysis of international and Ukrainian experience. *Cuestiones Políticas*, 39(69), 115–132.
- Cultri, C. N., & Bazilio, A. P. M. (2021). Tecnologia social e cultura digital. *Holos*, 37(2), 1–14.
- Escuder, S. (2019). Regionalization of the digital gap. Development of ICT infrastructure in Latin America and Uruguay. *PAAKAT: Revista de Tecnología y Sociedad*, 17(17), 1–26.
- Fernandez, E. (2021). Desafíos jurídicos interdisciplinarios de la ciberseguridad nacional: apuntes De Lege Ferenda. *Anuario de La Facultad de Derecho. Universidad de Extremadura*, 37, 75–118.
- Flores, J. J., Hernández, R. M., & Garay-Argandoña, R. (2020). Tecnologías de información: Acceso a internet y brecha digital en Perú. *Revista Venezolana de Gerencia*, 25(90), 504–527.
- Leyva, C. (2021). Estudio de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales. *Lucerna Iuris et Investigatio*, 1, 29–47.
- Mordvinov, V., & Udavikhina, U. (2022). Jurisprudencia teórica y aplicada. 2(April), 83–88.
- Mphatheni, M. R., & Maluleke, W. (2022). Cybersecurity as a response to combating cybercrime. *International Journal of Research in Business and Social Science* (2147- 4478), 11(4), 384–396.
- Quijano, P. (2018). Jóvenes y cultura digital: abordajes críticos desde America Latina. *Chasqui. Revista Latinoamericana de Comunicación*, 1(137), 1–13.
- Renés, P., Hernández, M., Caldeiro, M., & Alvites, C. (2021). Countervalue of the digital ethos perceived by future trainers. *Comunicar*, 29(69), 57–67.
- Risquete, J. (2018). De la cultura a la cultura digital: nuevos escenarios en una nueva era. *Revista Mediterránea de Comunicación*, 9, 505–506.
- Rojas, J. (2022). Panorama de riesgos por el uso de la tecnología en América Latina. *Trilogía Ciencia Tecnología Sociedad*, 14, 1–40.
- Shashi, S., Udo, G. J., & Bagchi, K. (2020). Determinants of cybercrime originating within a nation: a cross-country study. *Journal of Global Information Technology Management*, 23(2), 112–137.
- Veresha, R. V. (2018). Preventive measures against computer related crimes: Approaching an individual. *Informatologia*, 51(3–4), 189–199.