LA IDENTIDAD DIGITAL COMO CONTENIDO DEL DERECHO A LA SEGURIDAD PERSONAL EN LA ERA DE LA IA

DIGITAL IDENTITY AS CONTENT OF THE RIGHT TO PERSONAL SECURITY IN THE ERA OF AI

David de Jesús Aníbal Guerra[1]

Nadín Andrés Madera Arias[2]

Julio Cesar Padilla Martínez[3]

Salomón Blanco Negrette[4]

Resumen: El presente artículo desarrolla uno de los objetivos específicos de la investigación científica: Eficacia de las garantías judiciales en la nueva revolución digital, mismo que, busca establecer el constructo del derecho a la seguridad personal como un derecho autónomo y la protección de la identidad digital como contenido de dicho derecho. Metodológicamente, se trata de una investigación que emplea el paradigma hermenéutico dentro de un estudio documental y del nivel propositivo cuyo desarrollo se da a través de los postulados del cualitativismo. Para tal efecto, las técnicas de recolección de la información utilizada son la observación y el análisis de contenido. En referencia a los aportes teóricos, se cuenta con los planteamientos de Gallardo (2023); Moreno, Paucar & Cajas (2022); Mir, Kar & Gupta (2022); Weitzberg, Martin, Schoemaker (2022); Martínez (2021); Sule, Zennaro & Thomas (2021), inter alia. Los resultados precisan que la identidad digital hace parte del contenido del derecho a la seguridad personal y, que los Estados, deben tomar todas las medidas tendientes a proteger a las personas de los riesgos y de las amenazas que se derivan de los cambios en el plano cibernético y, más concretamente, en la era de la inteligencia artificial, para lo cual deben atender al carácter progresivo de los derechos humanos.

Palabras claves: Derechos humanos, identidad digital, inteligencia artificial, no sustitución de la racionalidad humana, seguridad personal.

Abstract: This article develops one of the specific objectives of scientific research: Effectiveness of judicial guarantees in the new digital revolution, which seeks to establish the construct of the right to personal security as an autonomous right and the protection of digital identity as content of said right. Methodologically, it is a research that uses the hermeneutic paradigm within a documentary study and the propositional level whose development occurs through the postulates of qualitativeism. For this purpose, the

[1] Abogado egresado de la Universidad Simón Bolívar; Doctor (PhD) en Ciencias Políticas; Master (Mtr) en Derechos Humanos, Estado de Derecho y Democracia en Iberoamérica, Especialista en Derechos Humanos. Profesor universitario, Escritor. david.anibal@unisimon.edu.co. Código ORCID: https://orcid.org/0000-0002-1671-8469

[2] Abogado egresado de la Universidad Simón Bolívar, Magister en Derecho del Estado de la Universidad Externado de Colombia, candidato a Doctor en Derecho. Correo electrónico:docente_investigador5@uajs.edu.co

[3] Estudiante del Programa de Derecho de la Universidad Simón Bolívar. Miembro del Semillero de Investigación en Derechos Humanos, línea de Ética y Formación en Derecho. Semillerista Elite

[4] Abogado egresado de la Universidad Católica Luís Amigó, estudiante de la Especialización en Derechos Humanos de la Universidad Simón Bolívar.

information collection techniques used are observation and content analysis. In reference to the theoretical contributions, there are the approaches of Gallardo (2023); Moreno, Paucar & Cajas (2022); Mir, Kar & Gupta (2022); Weitzberg, Martin, Schoemaker (2022); Martínez (2021); Sule, Zennaro & Thomas (2021), inter alia. The results specify that digital identity is part of the content of the right to personal security and that States must take all measures to protect people from the risks and threats derived from changes at the global level. cybernetic and, more specifically, in the era of artificial intelligence, for which they must attend to the progressive nature of human rights.

Keywords: Human rights, digital identity, artificial intelligence, non-substitution of human rationality, personal security

Introducción:

El ciber espacio y la inteligencia artificial (IA) han acaparado gran atención debido a los avances que en el campo de la ciencia, la tecnología y la innovación se vivencian día a día gracias a la capacidad resolutiva de estos. Con ellos, se han logrado satisfacer parte de las demandas en los diferentes sectores de la sociedad y, más puntualmente, en el sector financiero, el educativo, el sistema de salud, el informático, el sistema de transportes, en seguridad, entre otros más; conllevando con esto a la necesidad de la incorporación de una reglamentación legal respectos de los usos y de las prácticas que se puedan derivar del uso de la inteligencia artificial y de las condiciones de acceso en el ciber espacio habida cuenta de sus múltiples ventajas.

Esto pone de relieve que, a mayor interacción en el ciber espacio y entre más asuntos se puedan resolver, delegar y/o confiar a la Inteligencia Artificial, más propenso estará el ser humano a factores de riesgo en un ambiente en el cual la sustitución de la racionalidad humana va en aumento y el control humano sobre las nuevas tecnologías parece incierto. De hecho, la identidad digital de las personas siempre está en juego debido al notable incremento del e-commerce, el uso excesivo de las bases de datos que demandan el registro de la

información personal, el uso de las redes sociales y los algoritmos que ellas emplean para conocer las preferencias del individuo.

En otras palabras, la información que una persona deposita en el ciber espacio es sensible y ello permite colocarla en un nivel de riesgo que demanda de reglamentaciones eficaces que propendan por la protección de la identidad digital y, con ello, a la concreción de las garantías del derecho a la seguridad personal en los entornos mediados por la intervención de la inteligencia artificial.

En razón de lo anterior, la presente obra tiene por objeto establecer el constructo de derecho a la seguridad personal como un derecho autónomo y la protección de la identidad digital como contenido de dicho derecho habida cuenta de las transformaciones que trajo consigo el ciber espacio, la inteligencia artificial y el carácter progresivo de los derechos humanos. Para tal efecto, la metodología aplicada en el presente estudio adopta los lineamientos del paradigma hermenéutico y del enfoque cualitativo de la mano de la tradición de la teoría fundamentada. Las técnicas de recolección de la información implementadas son la observación y el análisis de contenido.

Para el desarrollo de la obra se abordan temas como: el derecho a la seguridad personal, dentro del cual, se dialoga sobre su concepto, su naturaleza y su estructura. Seguidamente, se arriba a la conceptualización de la identidad digital como contenido del derecho a la seguridad personal, para lo cual es necesario referirse a la progresividad de los derechos humanos y a las transformaciones en la era de la IA. Posteriormente, se ahondará sobre la justicia digital y los principios de no sustitución de la racionalidad humana y del control humano.

Dentro de los teóricos que contribuyeron con el presente estudio se destacan a: Gallardo (2023); Moreno, Paucar & Cajas (2022); Mir, Kar & Gupta (2022); Weitzberg, Martin, Schoemaker (2022); Martínez (2021); Sule, Zennaro & Thomas (2021). Paralelamente, se trajeron a colación los aportes jurisprudenciales de algunos tribunales constitucionales y de la Corte Interamericana de Derechos Humanos.

Método:

El desarrollo de la presente obra estuvo liderado por los postulados del paradigma hermenéutico, producto del cual se tiene un estudio del tipo documental y del nivel propositivo que acoge la tradición de la teoría fundamentada. En relación con las técnicas de recolección de la data se emplean la observación y el análisis de contenido.

Se trata de una investigación documental porque implementa:

> Una serie de métodos y técnicas de búsqueda, procesamiento y almacenamiento de la información contenida en los documentos, en primera instancia, y la presentación sistemática, coherente y suficientemente argumentada de nueva información en un documento científico, en segunda instancia. De este modo, no debe entenderse ni agotarse la investigación documental como la simple búsqueda de documentos relativos a un tema. (Tancara, 1993, p. 94)

Es decir, su senda hermenéutica reconoce la existencia y la importancia de las contribuciones que se hayan en documentos, para de esta manera, consultar, extraer y analizar la información contentiva en ellos mediante la aplicación de la objetividad interpretativa con el fin de comprender la visión de los autores en relación con el tema de estudio. En ese orden de ideas, se tiene como indispensable la sistematización de la información para la construcción del conocimiento científico.

En referencia a la técnica de recolección de la data aplicada, se opta por el análisis de contenido debido a que este permite extraer la información de un documento para su posterior análisis cualitativo (Kripka et al, 2015). Es una técnica que facilita estudiar a profundidad los textos de manera sistemática para ahondar en el conocimiento del objeto de estudio y, a partir de ahí, realizar contribuciones válidas al quehacer científico. En otras palabras, se analizan las afirmaciones y las negaciones que se hayan en los documentos (Sabourin, 2009).

En ese orden de ideas, se elaboró una matriz de congruencia en la cual se operacionalizaron las variables, las dimensiones y los indicadores de los objetivos específicos de la investigación, producto de lo cual, en relación con esta obra surgieron las subvariables: seguridad personal e identidad digital.

Resultados y Discusión:

El derecho a la seguridad personal

El derecho a la seguridad personal siempre ha sido comprendido desde la interdependencia con el derecho a la libertad personal, a la vida y a la integridad personal. Diversos instrumentos en materia de derechos humanos lo consagran así, tal y como es el caso del artículo I de la Declaración Americana de los Derechos y Deberes del Hombre, el artículo 3 de la Declaración Universal de los Derechos Humanos, el artículo 9 del Pacto Internacional de Derechos Civiles y Políticos, el artículo 7.1 de la Convención Americana sobre Derechos Humanos, el artículo 5 del Convenio Europeo de Derechos Humanos y Libertades Fundamentales y el artículo 6 de la Carta de Banjul, inter alia.

Se trata de un derecho que, en el caso colombiano no está previsto por la Constitución Política, pero su fundamentabilidad como derecho se deriva de su conexidad con el derecho a la vida, a la integridad personal y el deber general de protección de las personas y de sus derechos a cargo del Estado (Corte Constitucional de Colombia [CCCO], 2018). Desde su dimensión unipersonal hace parte de los denominados derechos de primera generación y, según su estructura, se le puede atribuir el calificativo de ser un derecho de estructura compleja debido a que contiene un componente como derecho reaccional y otro como derecho prestacional.

Esto implica que, desde el primer componente, sea un derecho que no permite intervenciones sobre una situación de la persona debido a que para su goce no se requiere realizar una actividad especial, de ahí que, se pueda afirmar que en algunos eventos dicho derecho se ejerce inconscientemente (Escobar, 2014). Por su parte, el componente prestacional hace relación al conjunto de instituciones y de las acciones que estas deben desplegar para evitar atentados contra la seguridad personal de un individuo y, para tal efecto, dispone de los organismos que se encargan de la protección de esta, así como, de las instituciones habilitadas para recepcionar las denuncias frente a tales afectaciones.

Y es que, razonar sobre este derecho desde su estructuralidad es importante, porque se pueden precisar las garantías que en cada caso concreto se deben implementar de cara a la naturaleza del titular del derecho, las obligaciones que recaen sobre el obligado -*es decir el Estado*- y el contenido del derecho (Corte Interamericana de Derechos Humanos [Corte IDH], 2011). De esta manera, se consiguen dos finalidades, la primera, la de determinar el objeto de protección de acuerdo con las necesidades del titular del derecho y, la segunda, la

de evaluar el nivel de riesgo y los factores objetivos y subjetivos que rodean una situación particular (CCCO, 2022).

De ahí que, cuando se analiza una posible violación al derecho a la seguridad personal, la situación fáctica se aborda desde la repercusión que desde este derecho se puede generar sobre otros más, como lo es frente al derecho a la vida y a la integridad personal (CCCO, 2021). En otras palabras, si no se demuestra la conexidad lesiva entre el derecho a la seguridad personal y otro, no se podría predicar la amenaza o vulneración de aquel de manera autónoma. En efecto, la jurisprudencia constitucional y comparada reconocen que se está frente a una amenaza o violación de este derecho cuando la persona se encuentra frente a un riesgo extraordinario o extremo contra su vida (Tribunal Constitucional del Perú [TCP], 2004).

En esa misma línea argumentativa, la Corte Constitucional de Colombia (CCCO, 2021; CCCO, 2013) se ha pronunciado en varias decisiones precisando que:

> En suma, la seguridad personal es un derecho fundamental que debe ser garantizado y preservado por el Estado, de manera que cuando una persona se encuentra ante un riesgo extraordinario o extremo debe adoptar las medidas de protección necesarias para salvaguardar sus derechos fundamentales. En concordancia con estos deberes, las autoridades tienen una serie de obligaciones relacionadas con la debida diligencia respecto de la valoración y determinación de las amenazas. Su incumplimiento también conduce a la vulneración de este derecho. Estos deberes también están referidos a la adopción oportuna de las medidas de protección adecuadas. En casos de vulneración de las distintas obligaciones estatales referidas a la seguridad personal, la Corte ha ordenado que se adelante una nueva evaluación de riesgo. Por último, excepcionalmente, mientras se adelanta esa nueva evaluación se puede ordenar el restablecimiento de esquemas de protección previos de acuerdo con los criterios definidos en el fundamento jurídico anterior.

Por su parte, la Corte Suprema de Justicia de Colombia (CSJ, 2019) ha sido del criterio que:

> La seguridad debe ser entendida como un valor constitucional, un principio y un derecho fundamental inherente a todo ser humano y además, un presupuesto necesario para el goce de todas las restantes garantías de la persona. Por tal razón, el Estado tiene el deber de respetarla y protegerla.
>
> Uno de los deberes a cargo del Estado en relación con ese axioma es el de protección, en virtud del cual las autoridades tienen la misión de adoptar las medidas positivas necesarias para brindarle al ciudadano las condiciones de seguridad adecuadas que permitan eliminar los riesgos extraordinarios contra la vida e integridad física.

Complementariamente, Morales (2010) insiste por una concepción más amplia del derecho a la seguridad personal en los siguientes términos:

> En su versión restringida, el derecho a la seguridad personal parece vincularse al derecho a la integridad física, en el sentido de tutelar al individuo contra daños a su cuerpo. Pero en una acepción más amplia, comprende también la protección frente a otros ataques conexos, como privaciones o perturbaciones a la libertad ambulatoria, atracos, invasiones a su domicilio, atentados sexuales, y en general amenazas o intimidaciones que impidan a un ser humano disfrutar de su derecho a la tranquilidad, sin temer lesiones a su persona o a sus bienes (p. 48).

Ahora bien, el asunto toma otra connotación si se analizan las nuevas dinámicas y los riesgos a los que se expone la persona por su interacción en el ciber espacio y del empleo de la inteligencia artificial en el mismo; espacios en los cuales, no se requiere de un acto de privación de la libertad ni de un atentado directo contra la vida y la integridad personal, pero sí de una afectación en contra de la persona debido a la información que de ella queda en esos entornos virtuales, tal y como ocurre con las redes sociales, las transacciones on line, la protección de la identidad digital, entre otras. De ahí que, abogar por el reconocimiento del derecho a la seguridad personal como un derecho autónomo, relacional y de estructura compleja con un contenido jurídico propio, facilita el andamiaje para debatir sobre las medidas de seguridad en el ciber espacio como contenido de este derecho para así responder

a las exigencias contemporáneas y al reconocimiento del carácter progresivo de los derechos humanos.

Así las cosas, se tiene que, la necesidad de la elaboración de un constructo del derecho a la seguridad personal como derecho autónomo y relacional, partiría, en principio, de los siguientes supuestos:

1. Que la relación de dependencia del derecho a la seguridad personal con el derecho a la vida, a la integridad personal y a la libertad personal en los términos actuales, limita la judicialización efectiva de este derecho en el contexto y en la dinámica de los nuevos tipos de violencia,
2. Que la ausencia de la autonomía del derecho a la seguridad personal, desconoce el carácter progresivo de los derechos humanos y, con ello, de las nuevas demandas que acordes con la dignidad humana se muestran como necesarias para hacer frente a los riesgos que se derivan de la interacción en el ciber espacio y del uso de la inteligencia artificial,
3. Que el carácter autónomo del derecho a la seguridad personal, materializaría el mandato del artículo 2 superior, en cuanto al servicio y la protección de la comunidad frente los riesgos que las personas no están jurídicamente obligadas a soportar producto de la ciberdelincuencia,
4. Que el carácter autónomo del derecho a la seguridad personal, diferenciaría los eventos en los cuales la afectación producida por la interacción en el ciber espacio y del uso de la inteligencia artificial recaería sobre el derecho a la intimidad personal y al buen nombre, de aquellos eventos en los que se cuestiona la inoperancia del Estado en cuanto a su deber de protección de la persona en los

entornos virtuales frente a una situación de riesgo real, inminente y latente; esto es ciberseguridad (Sule, Zennaro, & Thomas, 2021)

5. Que una visión actualizada del derecho a la seguridad personal, conllevaría al igual que como acontece con el derecho a la igualdad, de considerarlo como un derecho relacional y, a partir de ahí, al reconocimiento de los niveles de riesgo y de exposición en el que se encuentra la persona en el ciber espacio y bajo la constante influencia de la inteligencia artificial,

Conceptualización de la identidad digital como contenido del derecho a la seguridad personal

La identidad digital puede comprenderse como la identificación de un individuo en el ciber espacio debido a su interacción con el mismo mediante la creación de usuarios, cuentas y el acto de compartir información sensible en los entornos virtuales. No se trata de un derecho en sentido estricto -*ya que el mismo no está reconocido*-, sino, que es el fruto de los cambios que ha experimentado el mundo por los avances de las tecnologías de la información y de la comunicación -TIC-.

De acuerdo con Martínez y Rincón (2021)

> La identidad digital es una construcción que realizan los individuos en el mundo digital y que se asocia tanto con las herramientas tecnológicas como con factores sociales y de contacto en la red con otros individuos. Por tanto, para contar con una identidad digital, se requiere una participación activa en internet que permita tal construcción (p. 254).

Bajo esos mismos supuestos, Gallardo (2023) sostiene que:

> La identidad digital se construye a través de la información que cada persona comparte sobre él en Internet. Además, dicha identidad digital se configura por nuestro comportamiento y forma de actuar en las redes sociales. En este

> sentido, es importante tener en cuenta que puede ser alterada a lo largo del tiempo, y que nuestra identidad digital puede estar disociada con nuestra identidad física, no debiendo tener la misma personalidad ni rasgos de identidad en terreno físico que en el terreno virtual (p. 1013).

En ese orden de ideas, la identidad digital es un atributo de la persona en el ciber espacio que le permite estar en la capacidad de identificarse y de compartir información personal en los sitios web de acuerdo con sus intereses y sus preferencias. Razón por la cual, se puede afirmar que la identidad digital hace parte del conjunto de acciones que despliega el internauta en la red, con lo cual, la interacción en la misma, genera ciertos rangos de exposición de la información debido al tráfico de los algoritmos que guardan información y predicen las preferencias de los usuarios y sus patrones de comportamiento, dejando un registro de todo lo actuado en tiempo real en los servidores.

De ahí que, tal y como sostienen Moreno, Paucar & Cajas (2022) es necesario lograr la protección de los usuarios en el ciber espacio dada las diversas formas de interacción en la red, a la par de, las nuevas modalidades de la delincuencia organizada en el entorno virtual y las emergentes formas de violencia en aquel. Motivo por el cual, es indispensable que los Estados procuren el establecimiento de regulaciones normativas eficaces que protejan a la persona humana de los riesgos del entorno virtual. Para lograr tal finalidad, se debe partir del reconocimiento de las afectaciones y de los peligros que se derivan del tráfico de la información en el ciber espacio, mismos que, facilitan la atmósfera para la suplantación de la identidad digital (Weitzberg, Martin, Schoemaker, 2022).

En ese estado de cosas, se sostiene que la suplantación de la identidad digital se concreta cuando se produce la sustitución de una persona en el ciber espacio empleando como

medio la creación de usuarios o accediendo ilegalmente a uno, así como, cuando mediante el uso de fotografías o información sensible de una persona se crean perfiles falsos para producir daños a terceros afectando con esto varios derechos (Mir, Kar & Gupta (2022).

Ahora bien, para hacer frente a las amenazas y a los riesgos derivados de la ciberdelincuencia, se observa el surgimiento de regulaciones desde el derecho penal por medio de las cuales se ha logrado la tipificación de los delitos informáticos. Tal es el caso de Chile, que cuenta con la ley 21459 de 2022 cuya finalidad fue la de adecuar los delitos informáticos de acuerdo con el Convenio de Budapest de 2001 que versa sobre la cibercriminalidad. Así mismo, en el caso de Costa Rica mediante la ley 9048 de 2012 se consagró un total de 11 tipos penales referenciados a delitos informáticos con los que se buscan **proteger la propiedad.**

En México, a través del título IX del Código Penal Federal se busca proteger la **Revelación de secretos y acceso ilícito a sistemas y equipos de informática** y, para tal cometido, consagra los delitos informáticos de aplicación en dicha nación. En el caso Colombiano, se cuenta con la ley 1273 de 2009 con la que se crea un nuevo bien jurídico tutelado denominado: **de la protección de la información y de los datos,** con lo que se tipifican 9 tipos penales constitutivos de delitos informáticos. En referencia a Panamá, se tiene que su código penal en el título VIII estableció los delitos informáticos por medio de los cuales busca amparar la **Seguridad Jurídica de los Medios Electrónicos**.

Por su parte, en el Perú se tiene la ley 30096 que tipifica los delitos informáticos y que según su objeto busca luchar contra la ciber delincuencia; esta consagró una clasificación de los delitos informáticos **de acuerdo con el contexto en el que se produce la lesividad**. En ese sentido, se tienen las siguientes modalidades:

1. Delitos contra datos y sistemas informáticos
2. Delitos informáticos contra la indemnidad y libertad sexuales
3. Delitos informáticos contra la intimidad y el secreto de las comunicaciones
4. Delitos informáticos contra el patrimonio
5. Delitos informáticos contra la fe pública, dentro del cual se tiene la suplantación de identidad

En ese mismo sendero, la República de El Salvador mediante el Decreto 260 de 2016 - *siguiendo el modelo peruano*- consagró un listado de delitos informáticos partiendo de la base del contexto en el que se produce la comisión de la conducta punible, producto de lo cual, el bien jurídico tutelado es: **la información que garantice y proteja el ejercicio de derechos fundamentales como la intimidad, honor, integridad sexual, propiedad, propiedad intelectual, seguridad pública, entre otros**.

Como se observa, existe un ánimo en la región desde la legislación penal comparada para judicializar los delitos informáticos haida cuenta de los estragos de la ciber delincuencia, sin embargo, es evidente que aún no hay un consenso sobre el bien jurídico que debe ser tutelado con la prohibición de tales comportamientos. Con todo, se valora la postura de la legislación Peruana y Salvadoreña, debido a que reconocen la importancia de examinar el contexto en el que ocurre un delito informático para luego verificar el tipo penal en conjunto con el bien jurídico tutelado; situación ésta que reafirma el segundo propósito de este trabajo que es: reconocer la identidad digital como parte del contenido al derecho a la seguridad personal.

Así las cosas, los riesgos derivados de los atentados a la identidad digital producto de la cibercriminalidad, ponen de relieve la necesidad de, por una parte, reconocer que el derecho a la seguridad personal debe ser valorado como un derecho autónomo y relacional para hacer frente a las transformaciones socio tecnológicas contemporáneas, a la par de, precisar las obligaciones de protección en cabeza del Estado frente a las personas que interactúan en el ciber espacio y con la inteligencia artificial y, por la otra parte, que para la protección efectiva de la identidad digital, es menester que el deber de protección respecto de ésta sea parte del contenido del derecho a la seguridad personal y no de otro derecho que no facilite su judicialización por el desconocimiento del contexto en el que se produce la violación del derecho.

Se discute el constructo del derecho a la seguridad personal como derecho autónomo y la protección de la identidad digital como contenido de dicho derecho habida cuenta de los riesgos que corre la persona humana en el ciber espacio.

Referencias Bibliográficas

Corte Constitucional de Colombia. (2018). Sentencia T-411. M.P.: Carlos Bernal Pulido.

Corte Constitucional de Colombia. (2022). Sentencia T-015. M.P.: Gloria Stella Ortiz Delgado.

Corte Constitucional de Colombia. (2021). Sentencia T-239. M.P.: Gloria Stella Ortiz Delgado.

Corte Constitucional de Colombia. (2013). Sentencia T-078. M.P.: Gabriel Eduardo Mendoza Martelo.

Corte Interamericana de Derechos Humanos (2011). Caso Contreras y otros Vs. El Salvador. Fondo, Reparaciones y Costas. Sentencia de 31 de agosto de 2011. Serie C No. 2

Corte Suprema de Justicia. (2019). Sentencia de 1 de octubre, Exp: 679389. M.P.: Patricia Salazar Cuellar.

Escobar, G. (2014). Tipos y estructuras de derechos. Universidad de Alcalá de Henares, Madrid, España.

Gallardo Rodríguez, A. (2023). Identidad digital y responsabilidad civil de las plataformas digitales: de las redes sociales al metaverso.

Kripka, R., Scheller, M., & Bonotto, D. L. (2015). Pesquisa Documental: considerações sobre conceitos e características na Pesquisa Qualitativa. *CIAIQ2015, 2*.

Martínez Molano, V., & Rincón Cárdenas, E. (2021). Problemas y desarrollo de la identidad en el mundo digital. *Revista chilena de derecho y tecnología, 10*(2), 251-276.

Mir, U., Kar, A. K., & Gupta, M. P. (2022). AI-enabled digital identity–inputs for stakeholders and policymakers. *Journal of Science and Technology Policy Management*, *13*(3), 514-541.

Moreno Arvelo, P. M., Paucar Paucar, C. E., & Cajas Parraga, C. M. (2022). Regulación global para evitar la suplantación de identidad digital. *Revista Universidad y Sociedad*, *14*(6), 690-696.

Sabourin, P. (2009). L'analyse de contenu. *Recherche sociale: de la problématique à la collecte des données*, 415-444.

Sule, M. J., Zennaro, M., & Thomas, G. (2021). Cybersecurity through the lens of digital identity and data protection: issues and trends. *Technology in Society*, *67*, 101734.

Tancara, C. (1993). La investigación documental. *Temas sociales*, (17), 91-106.

Tribunal Constitucional del Perú (2004). Caso de Callao Natalia Foronda Crespo y otras EXP. N.° 2333-2004-HC/TC.

Weitzberg, K., Martin, A., & Schoemaker, E. (2022). Chapitre 2: Entre surveillance et identification: Repenser l'identité numérique dans l'humanitaire. In *L'Etat digital: numérisation de l'administration publique et administration publique du numérique* (pp. 145-157).