Ciberseguridad en el siglo XXI. Un reto al derecho público en Colombia

Cybersecurity in the 21st Century. Challenges to Public Law in Colombia

DOI: https://doi.org/10.18041/0124-0102/a.43.13199

Resumen

Con el uso de la tecnología se ha globalizado el intercambio de información sensible, confidencial y mensajes de comunicación entre los ciudadanos. Existe una sujeción a los cimientos digitales, se adquiere una serie de riesgos en relación con la seguridad. Este artículo pretende analizar la efectividad normativa de la ciberseguridad en el siglo XXI como un reto al derecho público en Colombia. Es un documento académico, que se sustenta principalmente con las opiniones personales de los escritores, siendo este una obra de reflexión acerca de la ciberseguridad. A pesar de ser un contenido de opinión, también se proporciona referencia de contenido académico, legislativo y jurisprudencial que apoya la postura de los autores. Finalmente, se permite inferir los motivos por los cuales se considera que existe falencia en la protección de datos sensibles, porque en los datos de confidencialidad y públicos existe una regulación en aras de la función pública.

Palabras clave:

derecho de cuarta generación, norma, ciberseguridad, dato sensible, confidencial, seguridad digital, transformación digital, protección, derecho público, ciberespacio, dignidad humana, derecho digital.

Abstract

This paper aims to raise awareness about the constant use of technology, which has paved the way for the exchange of sensitive, confidential and personal information among citizens. There is a subjection towards digital means, a series of risks are acquired regarding security; this article also contributes to the analysis of an effective norm about cyber security in the XXI century in the Public Law field in Colombia. This article is merely academic, which mainly describes the opinion of the authors, being this reflective work about cyber security. However, it also provides references of academic, legislative and judicial content, which support the authors' posture. Finally, it allows inferring the reasons for failures regarding protection of sensitive data, due to confidential and public data being regulated for the sake of public service.

Keywords:

security; cyber security; sensitive data; public data; confidentiality; digital transformation; public law; cyber space; digital rights.

Santiago Peñaloza Sosa
Universidad Popular del Cesar, https://orcid.org/0009-0007-1199-4206, penalozasosas@gmail.com.

Rosse Valerie Mena Camelo
Universidad Popular del Cesar, https://orcid.org/0009-0002-2252-8802, rmena@unicesar.edu.co.

Como citar:
Peñalosa, S. S.; Mena, C. R. (2024) Ciberseguridad en el siglo XXI. Un reto al derecho público en Colombia. *Advocatus, 21*(43), 161-170.

Recibido:
15 de enero de 2024
Aceptado:
30 de mayo de 2024
Publicado:
30 de junio de 2024

INTRODUCCIÓN

El fenómeno de la transformación digital permite la automatización para realizar tareas y la gestión de archivo; además, agiliza los procesos administrativos del Estado. Esta digitalización expone la información en el ciberespacio, siendo objetivo de los atacantes para afectar las infraestructuras críticas, en relación con los datos confidenciales y datos públicos. Algunos atacantes no buscan afectar las infraestructuras del Estado, sino los datos sensibles de los ciudadanos, suplantando a la persona y aprovechando su información para obtener un beneficio, afectando directamente a los datos de los ciudadanos que acceden a los derechos de cuarta generación.

En consecuencia, el Estado colombiano protege los datos de los ciudadanos, ante el avance tecnológico, principalmente con base en la Constitución de 1991, la Ley 1266 de 2008, la Ley estatutaria 1581 de 2012 y el Decreto 1377 de 2013. De modo que el Decreto 338 de 2022 establece un lineamiento para la ciberseguridad, como protección de la infraestructura crítica del Estado.

El debate planteado es de carácter reflexivo, sobre la ciberseguridad y la protección de los datos confidenciales, públicos y sensibles. Esto se sustenta en la constante desconfianza en el ciberespacio, aunque muchos autores han abordado la tesis de ciberseguridad, entre los que se encuentran Bellver Capella & Romero Wenz (2023), quienes afirman que la confianza no puede existir en el mundo de lo digital, porque no es una cuestión de fe. De ahí que siempre exista duda sobre la ciberseguridad. Por último, Vargas Montoya & Usma Guzmán (2024) plantean que las estrategias para la prevención de los ciberataques resultan útiles porque se constituyen en una herramienta valiosa para controvertir los hechos repetitivos de cibervictimización por parte de los atacantes en el ciberespacio.

Partiendo de esta base, se plantea la siguiente interrogante: ¿Cuál es la efectividad de la ciberseguridad en el siglo XXI como un reto al derecho público en Colombia? Para dar respuesta, se presenta el siguiente objetivo: reflexionar sobre la efectividad de la ciberseguridad en el siglo XXI como un reto al derecho público en Colombia. Existen grandes falencias normativas respecto a este tema en el país, a pesar de que existen leyes, decretos y pronunciamientos de la Corte Constitucional referentes a la normativa y su aplicación. Es evidente que el marco jurídico que regula la ciberseguridad en Colombia se ha quedado corto y es poco eficiente al momento de proteger los datos. El panorama es desalentador y se evidencia lo vulnerable que son los derechos de cuarta generación en el país.

Desarrollo. Para empezar, frente a la pregunta planteada, es necesario dirimir tres premisas jurídicas: el régimen normativo de ciberseguridad; las normas de protección y acceso a los datos confidenciales, datos públicos y datos sensibles, y finalmente la aplicación de la seguridad digital en protección a los datos en el ciberespacio.

Ciberseguridad y el régimen normativo. Respecto al primer eje, es necesario determinar la conceptualización de ciberseguridad, como lo determina Candau Romero (2021). La OTAN en 1990 reunió las definiciones de seguridad en las transmisiones, en las redes y en los ordenadores en un grupo de seguridad llamado de la información. El objetivo es proteger la información en tres dimensiones: confidencialidad, integridad y disponibilidad.

Así mismo, Casado Robledo (2020) sostiene que la tendencia de las TIC ha desarrollado un paradigma nuevo por todos los servicios que ofrece esta herramienta tecnológica, que impulsó la transformación de la estructura mundial, llamada el ciberespacio. El entorno ofrece oportunidades económicas y sociológicas. Sin embargo, presenta riesgo debido a la poca prevención de los ciudadanos, aunado al hecho del incremento de los delitos cibernéticos. Desde 1990 se busca proteger el *software* y el *hardware*, tomando en consideración los principios de confidencialidad, integridad y disponibilidad.

Al respecto, autores como Felizia, et al. (2022) consideran que la confiabilidad hace referencia a elegir cómo, cuándo y con quién se puede compartir información personal o comercial. Por su parte, Cerrillo & Martínez (2021) manifiestan que la integridad se refiere a ese principio jurídico que busca garantizar la completitud, la coherencia y rectitud en las actuaciones personales. Mientras que la disponibilidad es contar con esa información para cuando se requiera.

Adicionalmente, existe una realidad que se llama el ciberespacio. En ese sentido, Valencia Corozo (2024) refiere que es el lugar en el que no existen límites fronterizos, es un espacio virtual interconectado que permite el ejercicio de los derechos de cuarta generación, para llevar a cabo las actividades en línea. Por consiguiente, se infiere que no sólo es una protección al *software* y *hardware*, sino que con el ciberespacio se percibe una responsabilidad por parte del Estado. Al respecto, un fragmento del preámbulo de la Constitución de, 1991 otorga unos derechos fundamentales, la democracia y la participación para garantizar orden social justo y comprometido con la integración de la comunidad.

Derecho de cuarta generación. En la constitución política entra "la categoría de los derechos humanos en una cuarta generación, está encaminada a los derechos digitales, bajo el principio de la dignidad humana, bien jurídico tutelado por el Estado" (García, et al., 2022, p. 1).

Por tanto, un principio inspirador es la dignidad humana. La Corte Constitucional fija tres lineamientos: "(i) entendida como autonomía o vivir como quiera. (ii) como ciertas condiciones materiales concretas o vivir bien. (iii) como intangibilidad de los bienes no patrimoniales o vivir sin humillaciones". (T-881, 2002, párr. 1)

Régimen normativo del Estado colombiano para la ciberseguridad. Como respuesta

a la era tecnológica que sorprendió al mundo y sus avances presurosos, los Estados decidieron regular estos hechos, que tienen consecuencias jurídicas y un efecto en la vida de los ciudadanos y en las instituciones. Colombia no fue la excepción, legisla sobre los principios y concepto de las TIC con la Ley 1341 de 2009, que **modificó el Código Penal** Colombiano creando un nuevo bien jurídico denominado "protección de la información y de los datos". Esta ley tipifica delitos como el acceso no autorizado a sistemas informáticos, la interceptación de comunicaciones y el daño informático, entre otros.

Regula los aspectos de la competencia, la protección, la cobertura, la calidad del servicio, la inversión en el sector y el desarrollo tecnológico; además, aborda el uso de las redes, el espectro radioeléctrico y las facultades del Estado en planificación, gestión, regulación, control y vigilancia, con el fin de garantizar el acceso libre, sin discriminación, a la sociedad de la información. (Ley 1341 del 2009, artículo 1°)

No obstante, esta ley se quedó corta al llamado de la ciberseguridad, lo cual debería tener el Estado para garantizar la seguridad digital de los ciudadanos. Además, algo a favor de esta ley, en su artículo 2. Numeral 4, es que resalta la protección al usuario y promueve la seguridad de la información.

El Estado cuidará de manera adecuada la protección de los derechos de los usuarios de las Tecnologías de la Información y de las Comunicaciones, así como el estricto cumplimiento de los deberes y derechos procedentes del *Hábeas Data*, relacionados con la prestación del servicio. Por tal motivo, los proveedores u operadores directos tendrán que proponer sus servicios a precio del mercado y una utilidad razonable en los niveles de calidad estipulados en los títulos habilitantes o, en su defecto, enmarcados en los rangos que certifiquen las entidades competentes e idóneas en la materia y con información clara, necesaria, veraz y anterior, consecutiva y de toda forma pertinente para la toma de decisiones de los usuarios. (Ley 1341, 2009, artículo 2°, n°4)

Promover la seguridad informática y de redes para desarrollar las Tecnologías de la Información y las Comunicaciones" (Ley 1341, 2009, artículo 4°, n°11)

Aunque a partir del 8 de marzo de 2022, con el Decreto 338, el Estado colombiano dicta las directrices para reforzar la gobernabilidad de la seguridad digital, es importante tener presente que existe la Ley 1273 de 2009, que "no constituye un Plan Nacional de Ciberseguridad, sino una reforma penal, implementada por el gobierno colombiano para combatir ciberataques y proteger la información de la ciudadanía". (Jiménez Almeira & López, 2023). Con base en lo anterior, el Estado creó un nuevo bien jurídico que es tutelado por la ley penal, está denominado; «de la protección de la información y de los datos». Esta ley no es objeto para el desarrollo de este artículo, ya que esta sólo es la *ius puniendi* del Estado.

Por otra parte, aclarando la idea central del Decreto 338 del 2022, que en el momento es la columna vertebral de la seguridad digital en Colombia, ya que no existe hasta la fecha más normatividad. Sobre este decreto se justifica nuestra teoría en materia de ciberseguridad. Lo anterior, "para asegurar su calidad y aplicabilidad en determinado contexto como lo es la seguridad digital en Colombia, las normas que plantea y en el enfoque que se traduce en mecanismos aplicables en el contexto del ciberespacio. (Gómez Rengifo, 2021, p. 7)

Normas jurídicas que existen en protección y acceso a los datos de los ciudadanos. Para González (2024), el marco legal en Colombia para la protección de datos personales es un derecho fundamental que se encuentra en el artículo 15 de la Constitución Política de Colombia, el cual cuenta con 70 normas promulgadas desde 1951, exceptuando la Ley 1266 de 2008.

El artículo 15 de la Constitución resalta que toda persona tiene derecho a su intimidad personal, familiar, a su buen nombre y el Estado debe protegerlo y crear medidas de protección. En relación con la protección y la intimidad que menciona este artículo, la Corte Constitucional afirma que "Se protege la intimidad como una forma de asegurar la paz y la tranquilidad que exige el desarrollo físico, intelectual y moral de las personas". (T-414, 1992, párr. 1) .

De la misma manera, la Ley 1266 de 2008 dicta las normas generales del **hábeas data** y hace una regulación sobre la información contenida en las bases de datos públicos y sensibles de las entidades públicas y privadas. De igual manera, la Ley 1581 de 2012 y el Decreto 1377 de 2013 implementan el marco legal para la protección de datos personales que reglamenta el tratamiento de esta información por parte de personas naturales y jurídicas. Como parte de este marco legal, la figura de la conducta inequívoca surge como un mecanismo para obtener la autorización del titular de los datos" (González, 2024, p. 4).

La Ley Estatutaria 1581 de 2012 garantiza la confidencialidad, integridad y disponibilidad de la información, lo cual marca un hito y punto de partida en el ámbito de la protección. Recíprocamente, el Decreto 1377 de 2013 complementa esta ley detallando procedimientos específicos para gestionar, asegurar información, notificar incidentes de seguridad y definir responsabilidades claras para las entidades que manejan datos personales.

Clasificación de los datos. Para desarrollar la clasificación de los datos se exploran las siguientes normas: Ley 1341 de 2009, Ley 1581 de 2012 y el Decreto 1377 de 2013.

Para la Ley 1341 del 2009, el Estado debe garantizar la confidencialidad en las telecomunicaciones, la intimidad, la inviolabilidad y la confidencialidad.

El Decreto 1377 del 2013 precisa el dato público como aquel que no es semiprivado, privado ni sensible, lo cual está relacionado con el es-

tado civil de la persona, profesión, calidad de comerciante o servidores públicos.

La ley define los datos sensibles como aquellos que afectan la intimidad o cuyo uso indebido puede generar afectaciones a los derechos fundamentales.

Interpretar la aplicación de la seguridad digital del Decreto 338 del 2022 y su protección a los datos con la Ley 1581 de 2012 y el Decreto 1377 de 2013. Mediante el Decreto 338 del 2022, el Ministerio de Tecnología da las orientaciones generales para reforzar y fortalecer la gobernanza de la ciberseguridad, de infraestructuras cibernéticas sobre gestión de riesgo y respuesta a incidentes de seguridad digital.

Por lo anterior, es necesario traer a colación el artículo 2.2.21.1.1.3 del decreto 338 del 2022 que trata sobre la gobernanza que el Estado quiere implementar en la ciberseguridad.

En protección del ciberespacio, el Estado dicta un lineamiento, enfatizando con el artículo 2.2.21.1.2.1. Modelo de gobernanza de la seguridad digital, con el fin de fortalecer la seguridad digital, la protección de las redes, las infraestructuras críticas, los servicios esenciales y los sistemas de información.

El artículo 2.2.21.1.4.1 se refiere a las infraestructuras críticas cibernéticas y los servicios esenciales. Para esto, tendrá que determinar los sectores y subsectores que cuentan con infraestructuras débiles cibernéticas o prestan servicios fundamentales para el sostenimiento de las actividades económicas y sociales, para que la autoridad desarrolle y ofrezca una actividad o servicio fundamental para la conservación de actividades sociales o económicas, o cuente con información privilegiada del nivel estratégico del Estado y la seguridad nacional.

El rendimiento de esta actividad o servicio depende de las redes y sistemas de información, o de la aplicación de tecnologías de la información y las comunicaciones. Un ataque en las redes y sistemas de información traería como implicación efectos negativos y considerablemente lesivos para la prestación de dicho servicio.

Efectos del Decreto 338 del 2022 con la confidencialidad. Es importante determinar los datos de confidencialidad protegidos por la ley. La confidencialidad es el estado de secretismo asociado a elementos susceptibles de protección. Por lo tanto, determinar los efectos del Decreto 338, como facilitador de la política de gobierno digital, la cual conduce a la defensa de la confidencialidad, la disponibilidad de la información y la integridad, permitiendo asegurar la privacidad de los datos mediante la implementación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas.

De igual forma, la seguridad digital de la confidencialidad de los datos hace parte de la política del lineamiento para una infraestructura crítica cibernética para la protección de

la actividad del Estado con información privilegiada a nivel estratégico, para mantener su funcionamiento a pesar de los ataques a la información.

Efectos de Decreto 338 del 2022 con los datos públicos. En Colombia, la Ley 1712 de 2014 sobre transparencia y derecho de acceso a la información pública, tiene como función regular el derecho al acceso a los procedimientos para el ejercicio, la información pública y las excepciones a la publicidad de información y garantía del derecho. Esta ley se fundamenta en la política de gobierno digital, cuya intención es promover la transparencia, el acceso a la información pública, la competitividad, el desarrollo económico y la generación de impacto social a través de la apertura, la reutilización de los datos públicos, el uso y apropiación de las TIC.

La Ley de información pública en la reutilización de datos debe ser conocida por todas las personas, también existe una excepción constitucional y legal que trae la misma Ley 1712 de 2014. Artículo 6, que trata sobre la información pública reservada.

En síntesis, los datos públicos pueden ser conocidos por todos los interesados. Por otra parte, existe una excepción a la cual se debe su protección, en referencia a la Ley 1581 del 2012, acogiendo la misma tesis de los datos de las personas mayores y menores de edad, siempre que sean de naturaleza pública.

Ahora, los efectos del Decreto 338 del 2022 no son taxativos sobre los datos públicos, pero en la interpretación sobre los lineamientos para la ciberseguridad existen datos públicos que tienen limitaciones para ser conocidos por todas las personas. El decreto para garantizar y proteger la información de las infraestructuras críticas, al momento de ser divulgada, genera un riesgo para la seguridad digital del Estado.

Respecto a lo anterior, el decreto fortalece los lineamientos de la gobernanza en la seguridad digital con los datos públicos, específicamente en los que recaen las limitaciones legales y constitucionales, específicamente en la zona de la tecnología de la información y comunicación.

El Decreto 338 del 2022 en relación con los datos sensibles. En primer lugar, es importante tener presente que los datos sensibles están siendo perseguidos constantemente para suplantarlos. Desde luego, la poca higiene cibernética de las personas genera brechas entre la seguridad y la protección de datos sensibles.

Estos datos son el blanco diario para los ciberataques, facilitando el engaño en las entidades públicas y privadas para obtener un beneficio a costa de la identidad de las personas naturales o jurídicas.

Para conservar los datos sensibles de las personas, con su debida autorización, en aras de la protección y la seguridad jurídica para su

manejo en las bases de datos de las empresas públicas o privadas se crearon la Ley 1581 de 2012 y el Decreto 1377 de 2013, que establecen un marco legal para la protección de datos personales, regulando el tratamiento de esta información por parte de las personas naturales y jurídicas.

Por lo tanto, el Decreto 338 dicta unos lineamientos de gobernanza de la seguridad digital en el sector de la tecnología de la información y fortalece la coordinación en las entidades públicas, pero no regula frente a los datos sensibles de los ciudadanos. No existe una prevención.

Cabe recordar que en el ordenamiento jurídico colombiano se encuentra la Ley 1273 de 2009 en la *ius puniendi* del Estado, que pretende luchar contra el cibercrimen y la protección de la privacidad, la honestidad y los mismos sistemas informáticos. No se deben desconocer la ley ni las entidades investigativas, así como también, el soporte tecnológico de las diversas áreas de los sistemas electrónicos. Con la entrada en vigencia de la Ley 1273 de 2009 se dispone de herramientas jurídicas con sanciones rigurosas y seguras para castigar la ciberdelincuencia y reducir las actividades delictivas realizadas a través de los medios informáticos

Aunque el decreto no dicta las guías para el amparo cibernético de los datos sensibles de los ciudadanos, el ordenamiento jurídico contiene una sanción para quien pretenda cometer el delito. Aunque el Estado no es preventivo, contiene las normas necesarias para castigar.

En conclusión, este artículo lleva a reflexionar sobre el reto que tiene el derecho público en Colombia en temas de ciberseguridad en el siglo XXI. A través de este bosquejo se notan las falencias normativas que existen en este tema, a pesar de que existen leyes, decretos y pronunciamientos de la Corte Constitucional referente a la normativa y su aplicación.

Es notorio evidenciar que a pesar del marco jurídico que regula la ciberseguridad en los derechos de cuarta generación en Colombia, éste se ha quedado corto y no ha sido efectivo al momento de brindar protección. El panorama es un poco desalentador y es evidente lo vulnerable que siguen siendo los datos públicos y los datos sensibles, que afectan los derechos de cuarta generación del titular afectado y de la función pública. Aunque tenga una regulación más amplia se ha visto inmerso en la vulneración de las bases de datos (datos públicos y sensibles).

Los ataques cibernéticos a los datos públicos y sensibles le llevan una ventaja amplia a la ciberseguridad del Estado colombiano, lo que impide que el marco legal sea eficiente y proactivo al momento de su protección, poniendo en tela de juicio la efectividad, aplicación y la poca política del Estado en lo concerniente a la ciberseguridad y la protección de los derechos de cuarta generación, dejando así el sin sabor y la preocupación de la inminente amenaza que existe y los desafiantes retos que tiene el

derecho público para encontrar un equilibrio, proteger estos derechos y salvaguardar la ciberseguridad del Estado colombiano.

REFERENCIAS

Bellver Capella, V., & Romero-Wenz, L. (2023). Byung-Chul Han: la sociedad transparente digital o el infierno de lo igual. *Scio*, (23), 151-184. https://riucv.ucv.es/handle/20.500.12466/2869.

Cerrillo-i-Martínez, A. (2021). La integridad como instrumento para la prevención de los conflictos de intereses en la contratación pública (Integrity as a Tool to Prevent Conflict of Interest in Public Procurement). *Revista digital de derecho administrativo*, (25). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3749387.

Constitución Política de Colombia. http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html.

Corte Constitucional. Sentencia T-414-92. https://www.corteconstitucional.gov.co/relatoria/1992/t-414-92.htm.

Corte constitucional. Sentencia T-881-02. https://www.corteconstitucional.gov.co/relatoria/2002/t-881-02.htm.

Corozo, E. H. V. (2024). Implicaciones y desafíos del ciberespacio para la aplicación del Derecho Internacional. *Revista Política Internacional*, *6*(1), 219-233. https://core.ac.uk/reader/596250910.

Felizia, S. M., Molina-Jiménez, C., Frantz, R. Z., Reina-Quintero, A. M., Valente, A. D., & Navarro, E. (2022). Fortalecimiento del derecho a la confidencialidad en la gobernanza algorítmica. *Actas de las XVII Jornadas de Ingeniería de Ciencia e Ingeniería de Servicios (JCIS 2022). Sistedes*. https://www.cl.cam.ac.uk/~cm770/spanishpage/fortalecimientoconfidencialidad_jcis2022.pdf.

Función pública. Ley 1341 del 30 de julio de 2009. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=36913.

Función pública. Ley 1266 de 2008. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488.

Función pública. Decreto 1377 del 2013. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646.

Función pública. Ley 1712 de 6 de marzo del 2014. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882.

Gómez Rengifo, J. N. La ciberseguridad en el Estado colombiano. https://repository.umng.edu.co/server/api/core/bitstreams/3f6dc747-7e55-4cde-8969-0cbca7ed9be/content.

Hincapié, C. L. G. Implementación de política de protección de datos para la fundación escuela contra la pobreza-consultoría empresarial. https://repositorio.autonoma.edu.co/items/ea86608c-4b27-4fd1-88ac-212f5574f141.

Jiménez-Almeira, G. A., & López, D. E. (2023). Ciberseguridad y Seguridad Integral: un análisis reflexivo sobre el avance normativo en Colombia. *Revista Ibérica de Sistemas e Tecnologias de Informação*, (E62), 16-31. https://www.proquest.com/openview/9ec42ec894a0cf7606f7a0fbedcdfac4/1?pq-origsite=gscholar&cbl=1006393.

Romero, J. C. (2021). Ciberseguridad: Evolución y tendencias. *bie3: Boletín IEEE*, (23), 460-494. https://dialnet.unirioja.es/servlet/articulo?codigo=8175398.

Robledo, M. J. C. (2020). Proteger la información ha sido una constante a lo largo de la historia. *Revista española de control externo*, 22(64), 88-101. https://dialnet.unirioja.es/servlet/articulo?codigo=7774286.

San José, D. G., Alonso, F. L., & Delgado, C. V. (2022). La sociedad de los algoritmos y el derecho digital. *IUS ET SCIENTIA*, *8*(1), 5-7. https://scholar.google.com/scholar?hl=es&as_sdt=0%2C5&scioq=HINCAPI%C3%89%2C+CHRISTIAN+LEONARDO+GONZ%C3%81LEZ.+%22IMPLEMENTACI%C3%93N+DE+POL%C3%8DTICA+DE+PROTECCI%C3%93N+DE+DATOS+PARA+LA+FUNDACI%C3%93N+ESCUELA+CONTRA+LA+POBREZA-CONSULTORIA+EMPRESARIAL.%22&q=San+Jos%C3%A9%2C+D.+G.%2C+Alonso%2C+F.+L.%2C+%26+Delgado%2C+C.+V.+%282022%29.+La+sociedad+de+los+algoritmos+y+el+derecho+digital.+IUS+ET+SCIENTIA%2C+8%281%29%2C+5-7.&btnG=.

Vargas Montoya, H. F., & Usma Guzmán, F. A. (2024). Gamificación: Estrategia preventiva de ciberseguridad para sexting y grooming. *Revista Logos Ciencia & Tecnología*, *16*(2), 95-117. http://www.scielo.org.co/scielo.php?pid=S2422-42002024000200095&script=sci_arttext.