Revista *Ratio Juris* Vol. 20 N.º 41, 2025, DOI: 10.24142/raju.v20n41a7, pp. 173-194 © UNAULA

ARTÍCULO CIENTÍFICO

HUELLA DIGITAL Y *CIBERBULLYING*: NORMATIVAS LEGALES Y DESAFÍOS EN LA EDUCACIÓN SUPERIOR COLOMBIANA*

DIGITAL FOOTPRINT AND *CYBERBULLYING*: LEGAL REGULATIONS AND CHALLENGES IN COLOMBIAN HIGHER EDUCATION

PEGADA DIGITAL E *CIBERBULLYING*: NORMATIVAS LEGAIS E DESAFIOS NO ENSINO SUPERIOR COLOMBIANO

ÁNGELA MARÍA ARTEAGA FIGUEROA**
DANIELA NARVÁEZ BENAVIDES***

Recibido: 20 de mayo de 2025 - Aceptado: 22 de septiembre de 2025 -
Publicado: 30 de noviembre de 2025
DOI: 10.24142/RAJU.V20N41A7

Cómo citar: Arteaga Figueroa, A. M., & Narváez Benavides, D. (2025). Huella Digital y Ciberbullying: Normativas Legales y Desafíos en la Educación Superior Colombiana. Ratio Juris (UNAULA), 20(41). Recuperado a partir de https://publicaciones.unaula.edu.co/index.php/ratiojuris/article/view/1767, DOI: 10.24142/raju.v20n41a7

* El presente artículo es el resultado de los avances desarrollados en el proyecto de investigación denominado "Apropiación de la huella digital en las plataformas sociales de los estudiantes entre 16 y 20 años de la Universidad cesmag como elemento facilitador del ciberbullying".

** Administradora de sistemas informáticos de la Universidad de Pamplona (Colombia). Magíster en Seguridad Informática, magíster en Tecnología Educativa y Competencias Digitales de la Universidad de La Rioja (España). Doctoranda en Ingeniería Informática de la Universidad Complutense de Madrid (España). Docente e investigadora, integrante del Grupo de Investigación Derecho, Innovación y Desarrollo Social (Categoría C) de la Universidad cesmag. Docente de los programas de posgrado del Centro de Investigaciones Latinoamericanas (ceilat) de la Universidad de Nariño. Correo electrónico: amarteaga@uniceasmag.edu.co, angart01@ucm.es

*** Abogada de la Universidad cesmag. Especialista en Derecho Constitucional de la Universidad Nacional de Colombia. Magíster en Derecho Procesal de la Universidad de Medellín. Doctoranda en Derecho Agrario de la Universidad Federal de Goiás (Brasil). Actualmente es integrante del Grupo de Investigación Derecho, Innovación y Desarrollo Social (Categoría C) de la Universidad cesmag e integrante del gt Clacso: Pensamiento Jurídico Crítico y Conflictos Socio Políticos. Correo electrónico: danielanabe@hotmail.com, dcnarvaez@unicesmag.edu.co

Resumen

Esta investigación tiene como objetivo principal analizar el impacto del *ciberbullying* en la comunidad educativa, identificando principalmente la huella digital que los usuarios generan en las redes sociales y su relación con el acoso cibernético. Partiendo de la premisa de que las conductas agresivas y de acoso han migrado del ámbito presencial al entorno digital, se busca proponer una ruta de prevención que permita generar alertas tempranas, identificar los perfiles de los perpetradores y las víctimas, y remitir los casos a las instancias correspondientes dentro del sistema educativo. El estudio se basa en un enfoque cualitativo y sociocrítico, que integra el análisis normativo y el trabajo de campo con estudiantes de la Universidad CESMAG.

Palabras clave: contextos educativos, huella digital, prevención, *ciberbullying*, protección de datos personales.

Abstract

This research aims to analyze the impact of cyberbullying within the educational community, with special emphasis on identifying the digital footprint that users generate on social networks and its relationship with cyber harassment. Based on the premise that aggressive and harassing behaviors have migrated from face-to-face settings to the digital environment, this study seeks to propose a prevention pathway that enables early alerts, identification of perpetrator and victim pro-

files, and referral of cases to the appropriate instances within the educational system. The study is based on a qualitative and socio-critical approach, integrating normative analysis and fieldwork with students from CESMAG University.

Keywords: educational contexts, digital footprint, prevention, cyberbullying, personal data protection.

Resumo

Esta investigação tem como objetivo principal analisar o impacto do cyberbullying na comunidade educativa, com especial ênfase na identificação da pegada digital que os utilizadores geram nas redes sociais e sua relação com o assédio cibernético. Partindo da premissa de que comportamentos agressivos e de assédio migraram do âmbito presencial para o ambiente digital, procura-se propor uma rota de prevenção que permita gerar alertas precoces, identificar os perfis dos perpetradores e das vítimas, e encaminhar os casos para as instâncias correspondentes no sistema educativo. O estudo baseia-se numa abordagem qualitativa e sociocrítica, integrando análise normativa e trabalho de campo com estudantes da Universidade CESMAG.

Palavras-chave: contextos educativos, pegada digital, prevenção, cyberbullying, proteção de dados pessoais.

Introducción

El *ciberbullying*, entendido como el acoso sistemático a través de los medios digitales, es un fenómeno que está causando una preocupación creciente en Colombia y a nivel global. Este tipo de violencia, que afecta principalmente a los niños, las niñas y los adolescentes, tiene consecuencias devastadoras en la salud mental, emocional y física de las víctimas, incluyendo casos de suicidio, autolesiones y trastornos psicológicos. En el contexto colombiano, el aumento del acceso a internet y el uso masivo de las redes sociales han amplificado este problema, generando nuevos desafíos en materia de seguridad y protección de los datos personales.

El presente estudio se enmarca en el proyecto de investigación "Apropiación de la huella digital en las plataformas sociales de los estudiantes entre 16 y 20 años de la Universidad CESMAG como elemento facilitador del *ciberbullying*", financiado internamente por la Universidad CESMAG. La investigación parte de la premisa de que la huella digital, entendida como el rastro que dejan los usuarios al interactuar en las plataformas digitales, se puede explotar con fines delictivos, incluyendo el *ciberbullying*. Con un enfoque cualitativo y sociocrítico, se busca analizar el marco normativo vigente en Colombia, identificar los mecanismos mediante los cuales la huella digital facilita el acoso cibernético y proponer una ruta de prevención que contemple estrategias de detección temprana e intervención oportuna en el ámbito educativo.

En la era de la información, el uso intensivo de las tecnologías de la información y las comunicaciones (TIC) y de las redes sociales digitales ha transformado las dinámicas de interacción, permitiendo que comportamientos antes limitados al contacto físico se reproduzcan y se amplifiquen en el entorno digital. La huella digital que dejan los usuarios al interactuar en estos medios se ha convertido en un elemento importante que se puede explotar tanto con fines publicitarios como en prácticas delictivas, como el *ciberbullying*. Este fenómeno, caracterizado por conductas de humillación, ridiculización y agresión que impactan la salud mental, física y emocional de las víctimas, adquiere una relevancia especial entre los jóvenes, quienes son los principales actores y, a la vez, los más vulnerables en el contexto digital.

En el presente estudio se analiza el marco normativo vigente en Colombia, en particular la legislación que regula la protección de datos per-

sonales y las medidas preventivas contra el *ciberbullying*. Con un enfoque cualitativo y sociocrítico, se busca identificar los mecanismos mediante los cuales la huella digital puede facilitar la comisión de actos de acoso y proponer una ruta de prevención que contemple estrategias de detección temprana y la intervención oportuna en el ámbito educativo.

En este sentido, la investigación busca aportar elementos prácticos para generar rutas de prevención y construir políticas para proteger la integridad y los derechos fundamentales de los jóvenes. Además, se pretende evaluar la pertinencia de la ruta de prevención del *ciberbullying* en la educación superior y en la población sujeto de estudio, con el fin de contribuir a la creación de un entorno educativo más seguro y respetuoso.

Metodología

El estudio se desarrolló a partir de un enfoque cualitativo con perspectiva sociocrítica, orientado a comprender las interacciones entre la huella digital y la incidencia del *ciberbullying* en el entorno educativo colombiano. Este diseño metodológico permitió integrar el análisis normativo con una intervención directa en la realidad de los estudiantes, favoreciendo así la identificación de estrategias de prevención acordes con el contexto.

Diseño de la investigación

El diseño de la investigación se basó en un enfoque cualitativo que permitió explorar en profundidad las percepciones, las experiencias y los comportamientos de los estudiantes en relación con la huella digital y el *ciberbullying*. Se seleccionó este enfoque debido a que permite captar la complejidad de los fenómenos sociales y generar conocimientos contextualizados que se pueden aplicar en la práctica educativa.

- Enfoque cualitativo: Permitió analizar las interacciones sociales y los significados que los participantes atribuyen a sus experiencias en el entorno digital. Buscó comprender cómo la huella digital influye en la incidencia del *ciberbullying* y cómo las normativas legales se pueden aplicar de manera efectiva en el ámbito educativo.
- Perspectiva sociocrítica: La investigación adoptó una perspectiva sociocrítica, que no solo busca describir y analizar los fenómenos sociales,

sino también proponer soluciones prácticas para transformar las realidades problemáticas. En este caso, se buscó identificar estrategias de prevención y atención del *ciberbullying* que se puedan implementar en una institución educativa.

Muestreo

Se utilizó un muestreo por conveniencia, focalizado en los estudiantes del programa de Derecho de la Universidad CESMAG. Esta selección se fundamenta en la interacción habitual de este grupo con las plataformas digitales, lo que incrementa su vulnerabilidad ante fenómenos como el *ciberbullying*. Además, se consideró que los estudiantes de derecho tienen un mayor conocimiento de las normativas legales, lo que permitió contrastar su comprensión teórica con su aplicación práctica.

- Criterios de inclusión: Se seleccionaron estudiantes de entre dieciséis y veinte años, que fueran usuarios activos de las redes sociales y las plataformas digitales, y que hubieran tenido alguna experiencia relacionada con el *ciberbullying*, ya fuera como víctimas, como testigos o como agresores.
- Tamaño de la muestra: La muestra final la componen ciento treinta estudiantes, cinco docentes y tres miembros del personal administrativo de la Universidad CESMAG. Este tamaño de muestra permitió obtener diversas perspectivas y experiencias, asegurando la saturación de datos en el análisis cualitativo.

Técnicas e instrumentos de recolección de datos

Para recopilar la información necesaria, se utilizaron técnicas e instrumentos de recolección de datos que permitieron obtener una visión amplia del fenómeno del *ciberbullying* y su relación con la huella digital.

Entrevistas semiestructuradas

Se llevaron a cabo entrevistas con estudiantes, docentes y personal administrativo para recabar percepciones y experiencias relacionadas con la huella digital y el *ciberbullying*. Las entrevistas se basaron en un guion

predefinido, pero se admitió la flexibilidad para explorar temas emergentes durante la conversación. Las preguntas se centraron en la comprensión de los participantes sobre la huella digital, sus experiencias con el *ciberbullying* y su conocimiento de las normativas legales.

Grupos focales

Se organizaron sesiones de grupos focales con estudiantes y docentes para fomentar el diálogo y la reflexión colectiva sobre las prácticas de seguridad en línea y las medidas preventivas. Estas sesiones permitieron identificar patrones de comportamiento y actitudes comunes entre los participantes, así como explorar las diferencias en las percepciones y las experiencias.

Análisis documental

Se realizó una revisión exhaustiva de la normativa legal vigente en Colombia, incluyendo leyes, decretos y sentencias relacionadas con la protección de datos personales y la prevención del *ciberbullying*. Además, se analizaron documentos institucionales, como manuales de convivencia y protocolos de actuación ante los casos de acoso escolar. Este análisis permitió contextualizar la investigación en el marco jurídico actual y evaluar la aplicabilidad de las normativas en el ámbito educativo.

Observación participante

La observación directa en entornos virtuales y presenciales contribuyó a identificar patrones de comportamiento y dinámicas de interacción entre los usuarios, complementando la información obtenida a través de las entrevistas y los grupos focales.

Tabla 6.1 Relación de actividades, técnicas e instrumentos

Objetivo específico	Actividades	Técnicas	Instrumentos
OE1. Analizar el marco normativo vigente en materia de protección de datos personales y *ciberbullying*	-Revisión y análisis de la literatura jurídica y académica -Estudio documental de leyes, decretos y normativas oficiales	Revisión bibliográfica y análisis documental	Guías de lectura, bases de datos jurídicas, documentos oficiales (leyes, decretos, sentencias)
OE2. Identificar la relación entre la huella digital y la incidencia del *ciberbullying* en los entornos educativos	-Realización de entrevistas semiestructuradas a estudiantes, docentes y expertos -Organización de grupos focales para discutir sobre experiencias y percepciones -Observación participante en contextos digitales y presenciales	Entrevistas semiestructu-radas, grupos focales y observación participante	-Guiones de entrevista -Cuestionarios -Grabadoras -Teléfono móvil -Registro de observaciones
OE3. Proponer una ruta de prevención para mitigar el *ciberbullying* en el ámbito educativo	-Talleres participativos con actores educativos (estudiantes, docentes y personal administrativo) -Análisis y sistematización de la información recolectada -Elaboración de propuestas de intervención y estrategias de prevención	Talleres de discusión y análisis de contenido	-Cuestionarios de evaluación -Actas de talleres -*Software* de análisis cualitativo -Registro de debates y propuestas

Proceso de análisis de datos

Los datos recolectados se sometieron a un análisis de contenido que permitió identificar y categorizar la información en torno a tres ejes principales:

Datos sociodemográficos: Se analizaron las características del perfil de los participantes, incluyendo la edad, el género, las preferencias y el uso de TIC.

Realidad juvenil y uso de TIC: Se exploraron los comportamientos y las actitudes de los jóvenes en el manejo de las plataformas digitales, incluyendo su nivel de conciencia sobre la huella digital y las medidas de seguridad que implementan.

Manifestaciones del *ciberbullying*: Se identificaron las formas de acoso digital más comunes, las plataformas utilizadas para el acoso y las implicaciones del *ciberbullying* en la vida académica y personal de las víctimas.

Para llevar a cabo la codificación y el análisis sistemático de la información, se utilizó el *software* Atlas Ti, que facilitó la organización, el procesamiento y la interpretación de los datos, permitiendo integrar los hallazgos para construir una ruta de prevención efectiva en el ámbito educativo.

Consideraciones éticas

La investigación se llevó a cabo garantizando el anonimato y la confidencialidad de todos los participantes. Se obtuvo el consentimiento informado[1] previo de cada uno, cumpliendo con las normativas éticas y de protección de datos personales[2] vigentes. Además, se garantizó que la participación fuera voluntaria[3] y que los datos se utilizaran exclusivamente con propósitos académicos y en los procesos de investigación institucional.

1 Se explicaron a los participantes los objetivos de la investigación, los procedimientos de recolección de datos y el uso que se daría a la información. Todos los participantes firmaron un formulario de consentimiento informado antes de participar en las entrevistas y los grupos focales.

2 Se tomaron medidas para proteger la identidad de los participantes, utilizando seudónimos y eliminando cualquier información que pudiera identificarlos en los informes finales.

3 Se garantizó que la participación en la investigación fuera completamente voluntaria y que los participantes pudieran retirarse en cualquier momento sin consecuencias negativas.

Limitaciones del estudio

A pesar de los esfuerzos por garantizar la rigurosidad metodológica, el estudio presenta limitaciones que deben considerarse. La selección de participantes se basó en la disponibilidad y la accesibilidad, lo que puede limitar la generalización de los resultados, dejando por fuera a otras poblaciones o contextos educativos. Las entrevistas y los grupos focales dependen de la autoevaluación de los participantes, con lo cual pueden introducir sesgos en la información recopilada. El estudio se realizó en un período específico y esto puede afectar la capacidad para captar cambios o tendencias a largo plazo en el fenómeno del *ciberbullying*.

Resultados

La huella digital está compuesta por una gran cantidad de información que refiere diversos tipos de datos que se conservan de manera integral en los historiales de búsqueda, los historiales de navegación y las publicaciones en redes sociales. Es así como la huella digital ha permitido perfilar a los usuarios de acuerdo con sus gustos y preferencias, e individualizar su experiencia *online*, en principio para ofrecer publicidad personalizada y para obtener una reputación *online*, aunque esta también la pueden utilizar terceros con el fin de recopilar información personal con fines malintencionados, muchas veces sin que los usuarios sean conscientes de estas acciones.

Una de las acciones más frecuentes es el acoso en línea; por lo tanto, es importante reconocer, identificar y ser conscientes de nuestra huella digital, y tomar medidas para prevenir el mal uso de la información personal y proteger aspectos como la privacidad y la integridad de la información.

En la actualidad, el ciberacoso constituye un importante problema asociado a graves consecuencias físicas, mentales y sociales para los niños, las niñas y los adolescentes, y que impacta su rendimiento (Campbell y Bauman, 2018). Los estudios de investigación señalan que generalmente el matoneo se presenta cara a cara y luego se acompaña de otras modalidades, como las llamadas al terminal móvil, los mensajes por WhatsApp y los MMS o los SMS en redes sociales como Facebook e Instagram, o en plataformas como YouTube, o los mensajes instantáneos por Skype y MSN, entre otros (Garmendia *et al.*, 2019).

Compartir contenidos que menoscaban la dignidad de una persona, sean estos reales o manipulados, puede dejar una huella digital, de modo que quien defrauda la confianza puede divulgar en el navegador aquello que había iniciado como un juego interactivo, violando la intimidad de la víctima y dejando secuelas importantes en ella.

Por otra parte, en lo que respecta al ciberacoso y sus modalidades, el engaño es una parte fundamental de este fenómeno. Si bien se puede afirmar que en su mayoría las víctimas son menores de edad, las personas mayores de dieciocho años no están exentas de padecer este tipo de acoso, como señala el Ministerio de las Tecnologías de la Información y las Comunicaciones (Mintic, 2022).

En otras circunstancias los agresores son conocidos, a quienes se teme porque ejercen algún tipo de chantaje contra la persona agredida, por lo que esta no se atreve a denunciarlos. Se requiere analizar el perfil conductual de los agresores, pues generalmente son individuos poco empáticos, con características que les impiden experimentar culpa por su conducta, y que pueden encuadrarse en algunos tipos de personalidad negativos según las concepciones psicológicas.

En muchos países ya se ha intentado regular este fenómeno con el fin de que la sociedad tome conciencia de que se trata de una práctica peligrosa que puede generar consecuencias graves. En la actualidad, antes que castigar, se busca prevenir, como ocurre en Chile, en donde según Guevara *et al.* (2018) se observa que una considerable cantidad de jóvenes han estado inmersos en situaciones de ciberacoso, tanto en calidad de perpetradores como de víctimas, y en 2018 hubo un alza del 64 % en las denuncias con respecto al año inmediatamente anterior. La estrategia aplicada por el Ministerio de Educación de ese país pretende mitigar el ciberacoso mediante una pedagogía difundida en cartillas, con la finalidad de mejorar la formación preventiva que beneficia a los niños, las niñas y los adolescentes. Esta labor realizada por Chile puede adaptarse también para los ámbitos universitarios, dado que este fenómeno social abarca diferentes grupos de edades y esferas sociales.

Alemania también pretende contrarrestar el ciberacoso con educación, aplicando el programa Medienhelden, que tiene como finalidad propender por la alfabetización para prevenir el acoso cibernético. Según Ocaña (2017), se podría identificar a los perpetradores de *ciberbullying* por medio de algoritmos, que sirven para comparar las huellas digitales; de igual forma, las veces que se cliquea en un equipo de cómputo sirven para identificar

o recuperar una huella digital. Como conclusión, es viable la creación de una huella digital resistente a ataques, como indica Cruz (2018), "mejorando la recuperación de la huella digital y la identificación del usuario culpable, ante ataques a la base de datos".

En consecuencia, ante los inconvenientes que ha ido acarreando esta nueva modalidad de delitos informáticos, se suscribe en Budapest, el 23 de noviembre de 2001, el convenio que pretende aminorar la ciberdelincuencia mediante limitaciones y herramientas para establecer una legislación penal y procedimental para sancionar a los infractores de estos delitos cometidos a partir de medios tecnológicos y que han causado daño en las víctimas.

Frente a este panorama mundial, la Convención de Budapest pretende lograr la eficacia en el campo de la investigación y la aplicación de los procedimientos penales aplicables a conductas criminales ejercidas usando los desarrollos tecnológicos y de comunicación, y aplicando el peritaje informático en el recaudo de la evidencia electrónica. El objetivo de la Convención de Budapest es unificar los procedimientos de los países de Europa, Asia y América Latina, los cuales han suscrito este convenio, pues anteriormente cada país tenía una regulación individual para la ciberdelincuencia, lo que generaba un problema a la hora de sancionar estos delitos, ya que cada región gozaba de un ordenamiento jurídico diferente.

Otras naciones, como Brasil e India, no han ratificado aún el convenio, pues los criterios de tipificación de los delitos no se acomodan a las necesidades de estos Estados, donde la pobreza, la cultura y el acceso a internet generan modos, tiempos y circunstancias totalmente diferentes, con lo cual han optado por crear sus limitaciones con base en las necesidades de cada región.

Entre los avances legislativos en Colombia, según Novoa *et al.* (2016), la Ley 1341 de 2009 se constituyó en un paso importante para que el país entre a formar parte de la sociedad de la información y del conocimiento. Sin embargo, esta norma se modificó en la Ley 2108 de 2021, "Ley de Internet como servicio público esencial y universal", que modifica la Ley 1341 de 2009, tendiente a lograr un servicio de internet permanente para favorecer la conectividad, "en especial, de la población que, en razón a su condición social o étnica, se encuentre en situación de vulnerabilidad o en zonas rurales y apartadas" (Congreso de la República de Colombia, 2021).

En el año 2007 surge el Proyecto de Ley 123, que propone la creación de una nueva tipificación de este delito para proteger la información que cir-

cula en la red, y finalmente se introduce en la Ley 1273 del 2009 (Congreso de la República de Colombia, 2009). Más adelante, a través de la Ley 1928 de 2018 (Congreso de la República de Colombia, 2018), se aprueba el Convenio sobre la Ciberdelincuencia, que nace en Budapest.

Colombia vio la necesidad de proteger la seguridad informática debido al gran incremento de las TIC, pues como afirma Molina (2021), se hizo necesario el fortalecimiento de la seguridad interna con relación a los datos inmersos en el ámbito digital, usados por los nacionales en su diario vivir y, en consecuencia, la población se volvió más vulnerable frente a los ataques cibernéticos.

La seguridad informática y la protección de los datos personales sensibles son parte de la agenda del Estado colombiano, bajo el concepto de "Gobierno Digital" (Mintic, 2020); por tanto, la ratificación del convenio de Budapest ha resultado de gran relevancia para prevenir los ataques cibernéticos, mejorar la seguridad de la información en los hogares y en las empresas privadas y públicas, y empezar a concientizar a la sociedad de que no debe brindar información que genere consecuencias como las amenazas, los hurtos ni la divulgación de información íntima, de modo que se hace necesario resguardar la información, pues "los delitos no solamente ocurren en la vida real, la virtualidad es un nuevo escenario, los ciberdelincuentes están a la orden del día" (Arteaga, 2018).

En este sentido, es importante manifestar que dentro del marco constitucional colombiano se pueden resaltar dos tipologías de derechos que son relevantes con respecto al uso de las plataformas digitales y su incidencia en materia de *ciberbullying*. Conforme a los artículos 15, 20, 21 y 28 superiores se encuentran derechos fundamentales que hacen referencia a la protección individual y personalísima, y que establecen que todas las personas tienen derecho a la intimidad personal, al buen nombre y a actualizar y rectificar cualquier tipo de dato que se haya recogido a través de cualquier medio, incluyendo los informáticos. Así mismo, el artículo 20 constitucional señala que toda persona tiene derecho a expresarse libremente y que se debe garantizar este derecho como la libertad de buscar, recibir y difundir información e ideas. Por tal razón, "el derecho a la información debe ser respetado y garantizado por el Estado, siempre y cuando no afecte valores sustanciales, como los derechos al buen nombre, a la honra o a la intimidad" (Corte Constitucional de Colombia, Sentencia C-488 de 1993). En concordancia con lo anterior, el artículo 21 de la carta magna reconoce categóricamente

dos derechos, a la honra y al buen nombre, ya que recogen la protección a la reputación y el valor de la vida privada de las personas.

Ahora bien, en la sección de los derechos sociales, se han identificado aquellos establecidos en los artículos 44, 45 y 67, los cuales respectivamente resignifican los derechos fundamentales de los niños, las niñas y los adolescentes, y en concordancia con ello, se asocian con el interés superior y la paridad de salvaguardar la dignidad humana de los y las jóvenes del país, especialmente cuando se trata de su protección y de su formación integral en el campo de los contextos educativos, como en el caso particular de la población objeto de estudio, que se alinea con los propósitos educativos de la Universidad CESMAG, reconociendo que el Estado, la sociedad y la familia son responsables de garantizar el derecho a la educación libre de acoso, discriminación o de cualquier tipo de afectación en el desarrollo de su formación académica.

En este sentido, los criterios constitucionales con los que se relaciona la presente investigación se encuentran dentro del ordenamiento jurídico conforme lo dictan leyes como la 1620 de 2013, la 115 del 1994 y la 1098 de 2006. A continuación, se hace referencia a los criterios legislativos que operan en el caso puntual de identificar el uso inadecuado de las plataformas sociales y que buscan regular la violencia cibernética, el ciberacoso y los discursos de odio, siendo estas las actividades que afectan con mayor intensidad a la población joven, que llevan a tomar decisiones como el suicidio y que pueden generar enfermedades mentales, agresiones, autolaceraciones, entre otras prácticas.

Los artículos 6, 8 y 16 de la Ley 1620 de 2013 señalan lo siguiente:

> El Sistema Nacional de Convivencia Escolar y Formación para los Derechos Humanos, la Educación para la Sexualidad y la Prevención y Mitigación de la Violencia Escolar tendrá una estructura constituida por instancias en tres niveles: nacional, territorial y escolar, liderados por el sector educativo:
>
> - Nacional: Integrado por el Comité Nacional de Convivencia Escolar.
> - Territorial: Integrado por los comités municipales, distritales y departamentales de convivencia escolar, según corresponda.
> - Escolar: Integrado por el comité de convivencia del respectivo establecimiento educativo.

> Las organizaciones privadas con o sin ánimo de lucro podrán hacer parte de las estrategias, programas y actividades que, en desarrollo de esta ley, sean implementadas por los comités municipales, distritales o departamentales de convivencia escolar (Congreso de la República de Colombia, 2013).

El Sistema Nacional de Convivencia Escolar ha planteado la necesidad de sentar una ruta de formación en materia de derechos humanos y de la educación para la sexualidad, la prevención y la mitigación de la violencia escolar. Por tal razón, en analogía con los contextos universitarios, se considera que las instituciones de educación superior tienen el deber de establecer y promover una formación ciudadana para el desarrollo constructivo de una sociedad democrática que busque superar y minimizar cualquier tipo de violencia mediante el uso de los ambientes virtuales.

Además, se establece que una de las funciones del Comité Nacional de Convivencia Escolar es "coordinar la creación de mecanismos de denuncia y seguimiento en internet, redes sociales y demás tecnologías de información a los casos de *ciberbullying*" (Congreso de la República de Colombia, 2013, artículo 8, numeral 9). Por tal motivo, dentro del Sistema Nacional de Educación se plantea la necesidad de promover el desarrollo de la prevención del acoso escolar o de formas de intimidación con el uso deliberado de las tecnologías de la información.

Finalmente, en lo que respecta a esta norma, se observa que existe una serie de responsabilidades institucionales en los contextos escolares, por lo que se insiste en la promoción del "desarrollo de las competencias ciudadanas, el ejercicio de los derechos humanos, sexuales y reproductivos, el fomento de estilos de vida saludable y la prevención del acoso escolar y el *ciberbullying* en las jornadas escolares complementarias" (Congreso de la República de Colombia, 2013, artículo 16, numeral 6).

En virtud de lo anterior, se contempla lo incorporado por la Ley 115 de 1994, la cual tiene por objeto reconocer que la educación es un proceso de formación permanente que se desarrolla bajo la concepción integral de la persona humana, su dignidad y, en general, sus derechos. En este sentido, en el artículo 87 se plantea la necesidad de una regulación interna e institucional que, además de estipular una organización administrativa en materia de educación, exija la existencia de un reglamento o un manual de convivencia en el que se definan los derechos y los deberes de los estudiantes.

Igualmente, la Ley 1098 de 2006, conocida también como Código de la Infancia y la Adolescencia, reconoce que el Estado colombiano debe garantizar un proceso de desarrollo integral de educación que pueda "prevenir y atender en forma prevalente las diferentes formas de violencia y todo tipo de accidentes que atenten contra el derecho a la vida y la calidad de vida de los niños, las niñas y los adolescentes" (Congreso de la República de Colombia, 2006, artículo 41, numeral 16). Ello permite evidenciar que en el contexto de la Universidad CESMAG debe haber un mayor control frente a cualquier forma de ciberacoso o intimidación a través de las tecnologías digitales.

Relación entre la huella digital y el *ciberbullying* en los contextos educativos

La combinación de las entrevistas semiestructuradas, los grupos focales y la observación participante permitió profundizar en la manera en que la huella digital actúa como un factor facilitador en la incidencia del *ciberbullying* en los entornos educativos.

La mayoría de los participantes (estudiantes, docentes y expertos) reconocen que la huella digital deja un rastro permanente en las plataformas digitales. Muchos expresaron que a pesar de que están al tanto de la existencia de este rastro, su comprensión de las implicaciones en la privacidad y en la seguridad de su información es realmente limitada, y que debido a la falta de educación digital y de estrategias de prevención se puede incrementar la vulnerabilidad de los jóvenes frente a los ataques cibernéticos.

Tabla 6.2 Comparación de los resultados obtenidos

	Programa de Derecho	Programa de Psicología	Análisis
Conocimiento del *ciberbullying*	84 % sabe, 9,6 % no sabe, 6,4 % no está seguro	90,2 % sabe, 8,2 % no sabe, 1,6 % no está seguro	Los estudiantes de Psicología muestran mayor familiaridad con el concepto, posiblemente por su formación en temas de comportamiento y violencia digital

Continuación.Tabla 6.2 Comparación de los resultados obtenidos

	Programa de Derecho	Programa de Psicología	Análisis
Conocimiento de las normas	83 % no conoce, 10,6 % conoce, 6,4 % no está seguro	86,9 % no conoce, 9,8 % conoce, 3,3 % no está seguro	Existe un gran desconocimiento de las normativas en ambos grupos, que indica la necesidad de mejorar la comunicación sobre las políticas y las regulaciones
Capacitación	88,3 % no ha asistido, 8,5 % ha asistido, 3,2 % no está seguro	77 % no ha asistido, 14,8 % ha asistido, 8,2 % no está seguro	Aunque la formación es escasa en ambos grupos, los estudiantes de Psicología han participado en capacitaciones en mayor proporción
Campañas publicitarias	73,4 % no ha visto, 13,8 % ha visto, 12,8 % no recuerda	67,2 % no ha visto, 18 % ha visto, 14,8 % no recuerda	La percepción de la visibilidad de las campañas es similar; se requiere incrementar la frecuencia y el alcance de estas iniciativas
Rutas de atención	83 % no conoce, 11,7 % conoce, 5,3 % no está seguro	82 % no conoce, 11,5 % conoce, 6,5 % no está seguro	El gran desconocimiento de las rutas de atención destaca la necesidad de divulgar y facilitar el acceso a estos recursos en la universidad
Identificación de casos	56,4 % puede, 26,6 % no está seguro, 17 % no puede	67,2 % puede, 26,2 % tal vez pueda, 6,6 % no puede	Los estudiantes de Psicología tienen una mayor capacidad para identificar los casos de *ciberbullying*, coherente con su formación en análisis del comportamiento

Continuación.Tabla 6.2 Comparación de los resultados obtenidos

	Programa de Derecho	Programa de Psicología	Análisis
Conocimiento de las víctimas	76,6 % no conoce, 23,4 % conoce	86,9 % no conoce, 13,1 % conoce	La mayoría no conoce a víctimas, siendo el desconocimiento aún mayor en Psicología, lo que podría reflejar la reticencia a compartir las experiencias personales
Acción frente a los casos	57,4 % no sabe cómo actuar, 29,8 % sabe cómo actuar, 12,8 % no está seguro	44,3 % no sabe cómo actuar, 29,5 % sabe cómo actuar, 26,2 % tal vez sepa	Existe una considerable inseguridad en la actuación ante los casos; se hace imprescindible desarrollar y comunicar los protocolos de acción claros
Importancia del fenómeno	89,4 % considera importante, 10,6 % no está seguro	90,2 % considera importante, 8,2 % no está seguro	Ambos grupos reconocen la relevancia del *ciberbullying* como problema social, lo que favorece la implementación de medidas preventivas
Impacto a futuro	95,7 % cree que tendrá un gran impacto, 4,3 % no está seguro	95,1 % cree que tendrá un gran impacto, 4,9 % no está seguro	Existe un consenso general sobre el potencial impacto negativo del *ciberbullying*, lo que resalta la urgencia de intervenir de manera integral

Fuente: elaboración propia.

Los testimonios recogidos evidencian que, si bien la mayoría reconoce el término, la comprensión de sus implicaciones varía, lo que indica que es necesario profundizar en la formación sobre *ciberbullying* en los diferentes programas académicos. Pese a que existe un marco normativo formal (como la Ley 1620 de 2013 y la Ley 1273 de 2009), su operacionalización

en el ámbito universitario es insuficiente. También se identifica una brecha entre el conocimiento teórico y la aplicación práctica de las normativas, lo que afecta la eficacia de los mecanismos de atención y prevención.

Durante la realización de los grupos focales se enfatizó la necesidad de incrementar la capacitación y mejorar la comunicación institucional sobre el tema para crear una conciencia real sobre esta problemática. De igual forma, los relatos de las entrevistas indican que la inseguridad en la acción responde a la ausencia de protocolos claros y del manejo de las situaciones de *ciberbullying*.

Con base en la integración de los hallazgos anteriores, se da inicio a una propuesta de ruta de prevención orientada hacia la detección temprana para implementar sistemas de alerta y protocolos que permitan identificar conductas sospechosas y protocolos de intervención con directrices para la actuación ante los casos de *ciberbullying*.

Entre los hallazgos normativos en materia de *ciberbullying* en Colombia, se tiene que en el contexto nacional se ha estimado la necesidad de controlar y prevenir diferentes formas de violencia que pueden ser el resultado del uso de nuevas tecnologías y ambientes virtuales.

Conclusiones

En Colombia existen diversas normativas que conforman un marco legal que regula el tratamiento y la protección de datos personales, y que establece las condiciones para la recolección, el almacenamiento, el uso y la circulación de información personal. En cuanto al caso particular de la regulación del *cyberbullying*, se debe señalar que la Ley 1620 de 2013 busca prevenir y erradicar el acoso escolar y otros tipos de violencia en los establecimientos educativos; en su artículo 75 establece que las instituciones educativas deben promover la convivencia pacífica y el respeto por los derechos humanos, así como establecer mecanismos para prevenir y atender los casos de violencia escolar. Sin embargo, los resultados indican que en el entorno universitario existe un alto nivel de desconocimiento respecto a estas regulaciones, lo que pone en evidencia una brecha significativa entre la teoría normativa y su aplicación práctica. Es necesario que las instituciones refuercen la difusión y el conocimiento de estas leyes, para que sean efectivamente operacionales en la vida diaria de los estudiantes.

También se determinó que en Colombia el código penal establece que el acoso cibernético es un delito y se puede castigar con pena de prisión. Sumado a esto, la Fiscalía General de la Nación cuenta con la unidad de Cibercrimen, que se encarga de investigar y perseguir los delitos cometidos a través de internet y utilizando medios digitales. Aunque los estudiantes de Derecho acceden al conocimiento básico sobre la legislación, la falta de conocimiento específico sobre las normas que regulan el *ciberbullying* y las rutas de atención revela que la formación académica actual no aborda de manera suficiente la dimensión digital de la problemática. Asimismo, los estudiantes de Psicología, a pesar de su formación en análisis del comportamiento, requieren una profundización en la normativa que respalde la protección de los datos personales y la respuesta a los incidentes. Esto indica la urgencia de integrar módulos de formación sobre la legislación digital, la protección de datos y los protocolos de acción en el currículo universitario.

Debido a que la huella digital es una parte inevitable de nuestra presencia en internet, es importante que los usuarios, en este caso estudiantes, conozcan sus derechos y denuncien cualquier situación de acoso o violencia en línea. Es vital que las instituciones educativas actualicen sus protocolos de atención y realicen campañas informativas constantes que difundan el contenido y la importancia de las normativas relativas al *ciberbullying* y la protección de datos personales. La creación de comités interdisciplinarios y la definición de canales claros de denuncia y atención contribuirán a que las normativas se conviertan en herramientas operativas que aseguren una respuesta rápida y efectiva ante los casos de *ciberbullying*.

Referencias

Arteaga, Á. (2018). Seguridad de la información. Un recorrido bajo la perspectiva de Marc Goodman. *Estudios Latinoamericanos*, (42-43), 83-88. https://doi.org/10.22267/rceilat.184243.20.

Campbell, M. y Bauman, S. (2018). *Reducing cyberbullying in schools: international evidence-based best practices*. Academic Press. https://books.google.com.co/books?id=8QIxDwAAQBAJ&printsec=frontcover&hl=es#v=onep age&q&f=false.

Congreso de la República de Colombia (1994). Ley 115 de 1994. Por la cual se expide la Ley General de Educación. https://www.mineducacion.gov.co/1621/articles-85906_archivo_pdf.pdf.

Congreso de la República de Colombia (2006). Ley 1098 de 2006. Por la cual se expide el Código de la Infancia y la Adolescencia. http://www.secretariasenado.gov.co/senado/basedoc/ley_1098_2006.html#41.

Congreso de la República de Colombia (2009). Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado —denominado "de la protección de la información y de los datos"— y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. http://secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html.

Congreso de la República de Colombia (2013). Ley 1620 de 2013. Por la cual se crea el Sistema Nacional de Convivencia Escolar y Formación para el Ejercicio de los Derechos Humanos, la Educación para la Sexualidad y la Prevención y Mitigación de la Violencia Escolar. https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1685356.

Congreso de la República de Colombia (2018). Ley 1928 de 2018. Por medio de la cual se aprueba el Convenio sobre la Ciberdelincuencia, adoptado el 23 de noviembre de 2001, en Budapest. https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=147939.

Corte Constitucional de Colombia (1993). Sentencia C-488 de 1993. https://www.corteconstitucional.gov.co/relatoria/1993/C-488-93.htm.

Cruz, D. (2018). *Esquema de huella digital para datos relacionales con baja distorsión y resistente a ataques de colusión*. [Tesis de maestría]. Instituto Nacional de Astrofísica, Óptica y Electrónica (INAOE). https://inaoe.repositorioinstitucional.mx/jspui/bitstream/1009/1608/1/CruzPD.pdf.

Garmendia, M., Jiménez, E. y Larrañaga, N. (2019). Bullying y ciberbullying: victimización, acoso y daño. Necesidad de intervenir en el entorno escolar. *Revista Española de Pedagogía*, *77*(273), 295-311. https://dialnet.unirioja.es/servlet/articulo?codigo=6941197.

Goodman, M. (2015). *Los delitos del futuro*. Ariel.

Guevara, J., Sthioul, A., Rivera, M. y Barrientos, F. (2018). Ciberacoso: una revisión internacional y nacional de estudios y programas. *Evidencias*, *43*. https://centroestudios.mineduc.cl/wp- content/uploads/sites/100/2018/11/EVIDENCIAS-43.pdf.

Ministerio de Tecnologías de la Información y las Comunicaciones (Mintic). (2020). *Marco de la transformación digital para el Estado colombiano*. https://gobiernodigital.mintic.gov.co/692/articles-149178_recurso_1.pdf.

Mintic le dice no al acoso escolar y reafirma su compromiso para prevenir el *ciberbullying* (2 de mayo de 2022). *Ministerio de Tecnologías de la Información y las Comunicaciones (Mintic)*. https://mintic.gov.co/chicassteam/801/w3-article-210272.html.

Molina, C. D. (2021). *El Convenio de Budapest: un análisis desde el ordenamiento jurídico colombiano*. [Tesis de grado]. Universidad Pontificia Bolivariana. https://repository.upb.edu.co/bitstream/handle/20.500.11912/9409/Convenio_Budapest.pdf?sequence=1&isAllowed=y.

Petro, G. (2022). *Colombia Humana hacia una era de paz. Programa de gobierno del candidato presidencial Gustavo Francisco Petro Urrego para el período 2018-2022*. https://imagenes.canalrcn.com/ImgNoticias/programa-gobierno-colombia-humana.pdf?uAYrFBW7Pm.MYgKwlM6Nf1sxojON6b5t.

Objetivos de Desarrollo Sostenible (2019). *Departamento Nacional de Planeación (DNP)*. https://sinergia.dnp.gov.co/ods.

Ocaña, M. (2017). *Algoritmos de* matching *entre huellas dactilares*. [Tesis de grado]. Universidad Politécnica de Madrid. https://oa.upm.es/47958/1/TFG_MANUEL_OCANA_DIEZ_DE_LA_TORRE.pdf.

República de Colombia (1991). Constitución Política de Colombia. https://pdba.georgetown.edu/Constitutions/Colombia/colombia91.pdf.

Rincón, A. I. y Ávila, W. D. (2014). Simbiosis vital para describir el *ciberbullying* en Colombia. *Revista Científica General José María Córdova*, *12*(14), 149-164. http://www.scielo.org.co/pdf/recig/v12n14/v12n14a09.pdf.

Rubiano, I., Moreno, I. M. y Plazas, J. A. (2016). *Me cuido, te cuido en la red*. [Tesis de maestría]. Universidad de La Sabana.