

El uso del doxeo en conflictos digitales en redes sociales y su incidencia en jóvenes

Mariana Marisol Congregado Lezcano[1]

Jorge Daniel Rodriguez Ibarra[2]

Samira Bethania Sosa Vera[3]

Rodrigo Gabriel Vera Gens[4]

El presente artículo de revisión bibliográfica tiene como objetivo analizar el fenómeno del doxeo (doxxing) en el contexto de los conflictos digitales en redes sociales y su incidencia particular en la población joven. A partir de la revisión de fuentes académicas y especializadas, se examinan los tipos de información que se difunden mediante esta práctica, así como los conflictos en línea que impulsan su uso. Los resultados de la revisión evidencian que el doxeo constituye una forma de violencia digital que vulnera la privacidad, la seguridad y la integridad de sus víctimas. Las motivaciones más frecuentes son la venganza, el acoso, el control y las disputas ideológicas. Actualmente se necesita un abordaje educativo, legal y tecnológico coordinado para prevenir y mitigar sus efectos.

Palabras clave: doxeo, conflictos digitales, redes sociales, jóvenes, privacidad, violencia digital, ciberacoso.

ABSTRACT

This bibliographic review article analyzes the phenomenon of doxxing in the context of digital conflicts on social networks and its particular impact on young people. Based on a review of academic and specialized sources, the types of information disseminated through this practice are examined, as well as the online conflicts that drive its use. The results of the review show that doxxing constitutes a form of digital violence that violates the privacy, security, and mental health of its victims, with young people and adolescents being the most exposed. The most frequent motivations are revenge, harassment, control, and ideological disputes. It is concluded that a coordinated educational, legal, and technological approach is urgently needed to prevent and mitigate its effects.

Keywords: doxxing, digital conflicts, social media, youth, privacy, digital violence, cyberbullying.

INTRODUCCIÓN

En la era digital contemporánea, las redes sociales se han convertido en el principal escenario de interacción social para millones de personas en todo el mundo, especialmente para la población joven. Sin embargo, este espacio de comunicación también ha dado lugar a nuevas formas de conflicto y violencia. Una de las más preocupantes es el denominado doxéo o doxxing, práctica que consiste en la recopilación y publicación no autorizada de información privada de una persona con el propósito de dañarla, intimidarla o acosarla (Cambridge Dictionary, citado en National Institutes of Health [NIH], 2019).

El término proviene de la expresión en inglés "dropping dox" (documentos), y su uso se ha extendido de manera alarmante hacia entornos cotidianos, incluidos los conflictos entre jóvenes en plataformas como Instagram, TikTok, X (antes Twitter) y WhatsApp. Aunque inicialmente asociado al mundo de la piratería informática, hoy el doxéo se presenta como un fenómeno transversal que involucra a usuarios comunes, adolescentes y adultos.

La importancia del tema se encuentra en el impacto que el doxéo genera en sus víctimas: consecuencias psicológicas como ansiedad, depresión, desrealización y estrés postraumático, así como daños en la reputación, el rendimiento académico y las relaciones interpersonales (Observatorio de Violencia Digital, 2024).

Este artículo de revisión bibliográfica se plantea responder las siguientes preguntas de investigación: ¿Cómo se presenta el doxéo en los conflictos digitales en redes sociales y qué características tiene su uso entre los jóvenes? ¿Qué tipos de información se difunden mediante el doxéo? ¿Qué conflictos en línea impulsan a los usuarios a practicarlo? Cuáles son las redes sociales más utilizadas para llevar a cabo esta práctica?

En este sentido, el objetivo general de la investigación es analizar cómo se presenta el doxéo en los conflictos digitales en redes sociales y las características que tiene su uso entre los jóvenes. Para alcanzar este propósito, se establecen los siguientes objetivos específicos: identificar los tipos de información que se difunden mediante el doxéo en conflictos digitales en redes sociales por parte de los jóvenes; determinar los conflictos en línea que impulsan a los usuarios a practicar el doxéo en redes sociales; e identificar las redes sociales más utilizadas para la práctica del doxéo entre los jóvenes.

Para ello, se analizan recursos de literatura académica y especializada disponible sobre el tema, con el fin de ofrecer un panorama claro y conciso que sirva de base para futuras investigaciones y contribuya a la comprensión de esta forma de violencia digital en los entornos virtuales contemporáneos.

MARCO TEÓRICO

Definición y origen del doxéo

El doxéo puede definirse como la práctica de recopilar y publicar, generalmente en línea y sin consentimiento, información personal o identificadora de un individuo con intención maliciosa (NIH, 2019).). El término refiere a la exposición de documentos o información personal para generar un daño deliberado a la trayectoria pública y profesional de una persona. Este concepto se ha expandido más allá de las comunidades

de hackers para convertirse en una herramienta de acoso accesible para cualquier usuario de internet (Studocu, 2023).

Históricamente, el doxeo fue asociado a grupos de hacktivistas como Anonymous, que utilizaron esta práctica para exponer las identidades de miembros de organizaciones extremistas. Sin embargo, con la masificación de las redes sociales, el fenómeno migró hacia conflictos cotidianos, personales e ideológicos entre usuarios anónimos y públicos (Britannica, 2026; Douglas, 2016).

Tipos de doxeo y métodos de recopilación de información

Los métodos empleados para llevar a cabo el doxeo son variados y aprovechan tanto la información públicamente disponible como técnicas más sofisticadas. Entre los principales se identifican: el doxeo por redes sociales (revisión de perfiles públicos), el doxeo de IP/ISP (rastreo de direcciones IP para obtener ubicación geográfica), la utilización de corredores de datos, el phishing e ingeniería social, y el hackeo de cuentas privadas (Studocu, 2023; Gobierno de Argentina, 2026).

En cuanto a las tipologías del comportamiento, la investigación de la NIH (2019) con adolescentes identifica principalmente dos formas: el doxeo social, orientado a obtener información social sobre el objetivo, y el doxeo hostil, dirigido a obtener datos de identificación personal con fines intimidatorios. Este estudio encontró que las mujeres son más propensas a realizar doxeo social, mientras que los hombres tienden al doxeo hostil orientado a la localización física de las víctimas.

El doxeo como violencia digital

El doxeo forma parte de un espectro más amplio de lo que se denomina violencia digital, entendida como toda acción dolosa que cause daño a la intimidad, privacidad o dignidad de las personas a través del uso de tecnologías de la información y la comunicación (Infoem, s.f.). Las Naciones Unidas (ONU Mujeres, s.f.) incluyen al doxeo junto con el ciberacoso, las deepfakes, el grooming y el acoso sexual en línea como formas de violencia digital facilitada por la tecnología.

Desde una perspectiva de género, el doxeo también se manifiesta como violencia de género digital, especialmente cuando afecta a mujeres y niñas, exponiéndolas a represalias que van desde la humillación pública hasta situaciones de riesgo físico (Stop Violencia de Género Digital, 2024). La información difundida en estos casos suele incluir datos de contacto, fotografías íntimas, lugar de trabajo o estudio, e incluso detalles sobre familiares.

Redes sociales y jóvenes: un entorno de riesgo

Las redes sociales constituyen el entorno de socialización primario de la Generación Z y la Generación Alfa. Estudios recientes señalan que casi la mitad de los jóvenes de entre 13 y 17 años en Estados Unidos usa redes sociales de manera casi constante (Pew Research, citado en *Frontiers in Psychiatry*, 2024). Esta exposición permanente incrementa su vulnerabilidad ante prácticas como el doxeo, que puede originarse incluso a partir de un simple desacuerdo en un videojuego en línea (WeLiveSecurity, 2022).

La adolescencia es una etapa de especial vulnerabilidad, marcada por cambios fisiológicos, psicológicos y relacionales intensos. Las redes sociales influyen en la construcción de la identidad de los jóvenes y pueden generar conflictos que conducen a conductas de riesgo (SciELO, 2021). En este contexto, el doxeo actúa como un catalizador de daños que trascienden el espacio digital y afectan la vida cotidiana de las víctimas.

METODOLOGÍA

El presente trabajo adopta un enfoque teórico-documental de tipo cualitativo, basado en la revisión y análisis de fuentes bibliográficas especializadas. Se consultaron artículos académicos indexados en bases de datos como PubMed/NIH, SciELO y revistas de comunicación digital, así como documentos institucionales de organismos gubernamentales (Gobierno de Argentina, Semujeres CDMX) y organizaciones internacionales (ONU Mujeres, Observatorio de Violencia Digital). Igualmente, se utilizaron fuentes de divulgación especializada de alta pertinencia temática.

Los criterios de inclusión fueron: (a) fuentes publicadas entre 2019 y 2026, (b) que abordaran el doxeo desde perspectivas psicológica, social, comunicacional o de ciberseguridad, (c) con foco en población joven o adolescente, o bien en redes sociales como escenario del fenómeno. Se excluyeron fuentes que trataran el doxeo exclusivamente desde una perspectiva técnica de ciberseguridad sin relación con dinámicas sociales.

La información recopilada fue organizada en categorías temáticas: definición y caracterización del doxeo; tipos de información difundida; motivaciones y conflictos desencadenantes; e impactos en la población joven. Este proceso permitió una síntesis que responde a las preguntas de investigación planteadas.

A partir del análisis de la información recopilada, los resultados se presentan en tres ejes: tipos de información difundida mediante el doxeo entre jóvenes, conflictos en línea que lo impulsan e impactos en la población joven. Esta organización permite comprender el fenómeno desde sus principales características, causas y consecuencias.

RESULTADOS

Tipos de información difundida mediante el doxeo entre jóvenes

La investigación bibliográfica permite identificar un conjunto recurrente de categorías de información que los perpetradores recopilan y publican al llevar a cabo el doxeo. Según el Gobierno de Argentina (2026), la información más frecuentemente expuesta incluye: datos de contacto (números de teléfono, correos electrónicos), dirección física o lugar de trabajo o estudio, nombres reales cuando se usan seudónimos en línea, fotografías y videos privados o íntimos, e información financiera.

El estudio de la NIH (2019) con adolescentes identifica que el objetivo varía según el tipo de doxeo: en el doxeo social, la información buscada es de tipo relacional (dónde está la persona, con quién se relaciona); mientras que en el doxeo hostil, la información objetivo es de identificación personal, incluyendo datos domiciliarios que permiten localizar físicamente a la víctima. Esta distinción es clave para entender los niveles de riesgo diferenciados que enfrentan las víctimas jóvenes.

Especial preocupación merece la difusión de fotografías y videos sin consentimiento, práctica que en el contexto de la violencia de género digital se denomina también image-based sexual abuse o pornovenganza. Investigaciones con adolescentes edocumentan esta modalidad como una forma específica de doxéo vinculada a la violencia de género (Revista Prisma Social, 2024). El estudio de la NIH (2023) con estudiantes secundarios de Hong Kong confirmó que la exposición de fotografías y videos personales genera consecuencias emocionales severas.

Conflictos en línea que impulsan el doxéo entre jóvenes

Los conflictos que precipitan el doxéo en entornos juveniles son de naturaleza diversa. Las fuentes revisadas permiten clasificarlos en las siguientes categorías:

En primer lugar, los conflictos interpersonales y disputas de carácter personal constituyen el detonante más frecuente. Brave Up (2022) señala que las personas recurren al doxéo cuando sienten que han sido atacadas o insultadas, buscando venganza como respuesta. Estos conflictos incluyen rupturas sentimentales, peleas entre grupos de pares, y rivalidades escolares trasladadas al entorno digital.

En segundo lugar, los conflictos ideológicos y de opinión son especialmente frecuentes en plataformas como X (Twitter) o foros de debate. Cuando el tema de disputa tiene visiones muy polarizadas, el doxéo se usa como herramienta para silenciar, intimidar o desacreditar a quienes sostienen posiciones contrarias (Brave Up, 2022; Wikipedia, 2026). Entre jóvenes, esto incluye debates sobre feminismo, política, género, identidad cultural y preferencias en comunidades de videojuegos o fandoms.

En tercer lugar, los conflictos en videojuegos en línea representan un escenario específico y creciente. WeLiveSecurity (2022) documenta cómo el doxéo puede comenzar a raíz de simples desacuerdos o rivalidades en videojuegos, derivando en cargas emocionales importantes para las víctimas, principalmente cuando se trata de menores de edad.

En cuarto lugar, el acoso sistemático o ciberbullying constituye tanto un antecedente como una consecuencia del doxéo. La investigación de la NIH (2019) establece que los estudiantes que habían perpetrado actos de doxéo tenían mayor

probabilidad de haber experimentado también situaciones de divulgación de información como víctimas, perpetradores u observadores, lo que evidencia un ciclo de violencia digital retroalimentado.

Finalmente, el activismo digital mal encauzado y la llamada "justicia vigilante" motivan casos en los que usuarios colectivamente deciden exponer a alguien a quien consideran culpable de alguna conducta reprobable, sin pasar por mecanismos institucionales. Este fenómeno, documentado históricamente con grupos como Anonymous, se replica hoy a menor escala en dinámicas juveniles de redes sociales (Britannica, 2026; Douglas, 2016).

Impactos del doxeo en la población joven

Los efectos del doxeo sobre las víctimas jóvenes son de carácter multidimensional. A nivel psicológico, el estudio de la NIH (2023) con 2.120 estudiantes de secundaria en Hong Kong concluye que prácticamente todos los tipos de información personal divulgada generan sentimientos negativos en las víctimas, incluyendo depresión, ansiedad, pánico, paranoia y estrés. Las asociaciones más significativas se encontraron entre la exposición de números de teléfono y fotografías personales con la aparición de ansiedad y depresión clínica.

A nivel social y académico, el Observatorio de Violencia Digital (2024) documenta que el doxeo puede socavar la confianza en uno mismo y en los demás, alterar las relaciones personales y afectar negativamente el rendimiento académico. Las víctimas frecuentemente modifican sus hábitos en línea y pueden llegar a la autoexclusión digital como mecanismo de protección.

A nivel físico y de seguridad, la exposición de datos domiciliarios o de geolocalización puede derivar en acoso presencial, situaciones de riesgo físico e incluso violencia. ONU Mujeres (s.f.) advierte que el doxeo puede conducir a consecuencias en la vida real tales como el seguimiento, las amenazas y la violencia física. Esta dimensión hace del doxeo un fenómeno que no puede ser reducido a una problemática exclusivamente virtual.

DISCUSIÓN

Los hallazgos de esta revisión permiten comprender el doxeo como un fenómeno complejo que opera en la intersección entre la violencia digital, la privacidad, la identidad en línea y las dinámicas relacionales de la juventud actual. Su análisis revela al menos tres ejes fundamentales que merecen atención investigativa y política.

La primera tensión se refiere a la frontera entre información pública y privada en la era de las redes sociales. Los jóvenes comparten grandes volúmenes de información en sus perfiles digitales, con frecuencia sin dimensionar los riesgos que esto conlleva. La sobreexposición voluntaria en redes sociales, documentada por múltiples estudios, convierte al entorno digital en un espacio propicio para la recopilación de datos con fines maliciosos (WeLiveSecurity, 2022; BBVA, 2021). Esta situación exige repensar la educación digital orientada no solo al uso responsable, sino a la comprensión crítica de la privacidad como derecho.

La segunda tensión concierne a la desproporción de género en el doxeo. La investigación evidencia que las chicas son víctimas de doxeo con mayor frecuencia que los chicos (NIH, 2023), y que el doxeo vinculado a la divulgación de contenido íntimo afecta desproporcionadamente a las mujeres. Esto ubica al fenómeno dentro de patrones más amplios de violencia de género digital que requieren respuestas específicas desde los sistemas de protección y justicia.

La tercera tensión se relaciona con el ciclo de victimización-perpetración. Los datos sugieren que quienes han sido víctimas de doxeo tienen mayor probabilidad de convertirse en perpetradores (NIH, 2019), lo que revela un ciclo de violencia que se autoalimenta en las comunidades digitales juveniles. Intervenir en este ciclo requiere estrategias que aborden simultáneamente la prevención, la atención a víctimas y la rehabilitación de quienes perpetran estas conductas.

Finalmente, cabe señalar una limitación relevante del presente trabajo: la mayoría de estudios disponibles provienen de contextos anglosajones y asiáticos (Estados Unidos, Reino Unido, Hong Kong), por lo que la transferibilidad de sus hallazgos a contextos latinoamericanos requiere cuidado. Se identifican vacíos investigativos

importantes en la región, especialmente en relación con el doxeo en conflictos entre jóvenes en redes sociales de América Latina.

CONCLUSIONES

El doxeo se ha consolidado como una de las manifestaciones más graves de la violencia digital en el contexto de las redes sociales, con una incidencia preocupante en la población joven. La revisión bibliográfica realizada permite extraer las siguientes conclusiones principales:

Primero, el doxeo entre jóvenes involucra la difusión de información altamente sensible, incluyendo datos de contacto, ubicación física, fotografías y videos personales, e información de identidad real. El tipo de información difundida varía según el tipo de doxeo (social u hostil) y la naturaleza del conflicto que lo motiva.

Segundo, los conflictos en línea más frecuentes que impulsan el doxeo son: disputas interpersonales y de venganza, conflictos ideológicos en entornos polarizados, rivalidades en videojuegos, ciberbullying sistemático y dinámicas de justicia vigilante digital. Todos ellos comparten el rasgo de utilizar la información privada de la víctima como arma de intimidación, control o humillación pública.

Tercero, los impactos del doxeo en jóvenes son severos y multidimensionales: afectan la salud mental (ansiedad, depresión, estrés), la seguridad física, el rendimiento académico y las relaciones sociales. Las víctimas más vulnerables son las adolescentes, quienes enfrentan formas específicas de violencia de género digital asociadas al doxeo.

A partir de estas conclusiones, se recomienda avanzar en tres direcciones: (a) el desarrollo de programas de educación digital que incluyan la protección de la privacidad y las consecuencias del doxeo, dirigidos especialmente a adolescentes y jóvenes; (b) el fortalecimiento de marcos legales que tipifiquen el doxeo como una forma de violencia digital y garanticen la protección de las víctimas; y (c) la realización de investigaciones empíricas en contextos latinoamericanos que permitan caracterizar el fenómeno con mayor precisión y pertinencia cultural.

REFERENCIAS

Brave Up. (2022, 15 de diciembre). Otro tipo de violencia cibernética: el doxing. <https://blog.braveup.com/otro-tipo-de-violencia-cibernetica-el-doxing/>

BBVA. (2021, 16 de marzo). Qué es el doxing. <https://www.bbva.es/finanzas-vistazo/ciberseguridad/ataques-informaticos/que-es-el-doxing.html>

Gobierno de Argentina. (2026, marzo). ¿Qué es el doxing y cómo podemos cuidarnos? Ministerio de Justicia. <https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-el-doxing-y-como-podemos-cuidarnos>

Instituto de Acceso a la Información del Estado de México [Infoem]. (s.f.). Violencia digital. <https://www.infoem.org.mx/es/iniciativas/micrositio/violencia-digital>

Kwan, I., Dickson, K., Richardson, M., MacDowall, W., Burchett, H., Stansfield, C., Brunton, G., Sutcliffe, K., & Thomas, J. (2020). Cyberbullying and children and young people's mental health: A systematic map of systematic reviews. *Cyberpsychology, Behavior, and Social Networking*, 23(2), 72–82. <https://doi.org/10.1089/cyber.2019.0370>

Lahti, H., Kokkonen, M., Hietajärvi, L., Lyyra, N., & Paakkari, L. (2024). Social media threats and health among adolescents: evidence from the health behaviour in school-aged children study. *Child and Adolescent Psychiatry and Mental Health*, 18, Article 60. <https://doi.org/10.1186/s13034-024-00754-8>

National Institutes of Health [NIH]. (2019). Doxing: What adolescents look for and their intentions. PubMed Central. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6352099/>

National Institutes of Health [NIH]. (2023). Doxing victimization and emotional problems among secondary school students in Hong Kong. PubMed Central. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6313484/>

Observatorio de Violencia Digital. (2024, 12 de marzo). Stalking y doxing en la era digital. <https://observatoriodeviolenciadigital.com/stalking-y-doxing-en-la-era-digital/>

ONU Mujeres. (s.f.). FAQs: Digital abuse, trolling, stalking, and other forms of technology-facilitated violence against women and girls. <https://www.unwomen.org/en/articles/faqs/digital-abuse-trolling-stalking-and-other-forms-of-technology-facilitated-violence-against-women>

Secretaría de las Mujeres de la Ciudad de México [Semujeres]. (s.f.). Prevención y visibilización de la violencia cibernética contra las mujeres y niñas. <https://www.semujeres.cdmx.gob.mx/violencia-cibernetica-contramujeres>

Stop Violencia de Género Digital. (2024, 12 de marzo). Doxing: Una forma de violencia de género digital. <https://stopviolenciadegenerodigital.com/2024/03/12/doxing-una-forma-de-violencia-de-genero-digital/>

Tarullo, R., & Frezzotti, Y. (2024). La difusión digital de contenidos íntimos como forma de violencia de género: Un estudio cualitativo con adolescentes de Argentina. Revista Prisma Social, 47. <https://revistaprismasocial.es/ps/article/view/5532>

WeLiveSecurity. (2022, 16 de septiembre). Qué es el doxing y qué podemos hacer para prevenirlo. <https://www.welivesecurity.com/la-es/2022/09/16/que-es-doxing/>

Britannica. (2026, 26 de febrero). Doxing. Encyclopaedia Britannica.
<https://www.britannica.com/topic/doxing>

Douglas, D. M. (2016). Doxing: A conceptual analysis. *Ethics and Information Technology*, 18(3), 199–210. <https://doi.org/10.1007/s10676-016-9406-0>