PHILOS ARTIGOS
Indexada na CAPES
ISSN: 2671-6690 CÓDIGO: 918-2025-0371
CAPES

UDE
UNIVERSIDAD DE LA EMPRESA

RECEBIDO: 16/03/2026
Publicado: 20/03/2026

UNIVERSIDAD DE LA EMPRESA – UDE
FACULTAD DE CIENCIAS JURÍDICAS
MAESTRÍA PROFESIONAL EN CIENCIAS CRIMINOLÓGICO-FORENSES

EL ABUSO SEXUAL DE IMÁGENES MEDIANTE DEEPFAKES PORNOGRÁFICOS NO CONSENTIDOS EN BRASIL Y URUGUAY

ROGÉRIO DE CARVALHO COSTA

MONTEVIDEO, URUGUAY

2025

ROGÉRIO DE CARVALHO COSTA

EL ABUSO SEXUAL DE IMÁGENES MEDIANTE DEEPFAKES PORNOGRÁFICOS NO CONSENTIDOS EN BRASIL Y URUGUAY

Disertación presentada a la Maestría en Ciencias Criminológico-Forenses de la Facultad de Ciencias Jurídicas de la Universidad de la Empresa (UDE), como requisito para la obtención del título de Magíster.

Directora: Prof. Dra. Tereza Cristina Zabala.

MONTEVIDEO, URUGUAY

2025

DEDICATORIA

La presente tesis está dedicada a diferentes profesionales que, de manera directa o indirecta, contribuyen a la comprensión, afrontamiento y acompañamiento de los impactos sociales, jurídicos y humanos derivados del abuso sexual de imágenes mediante deepfakes pornográficos no consentidos en Brasil y Uruguay.

En primer lugar, reconozco el papel esencial de los profesores y profesoras universitarios(as), quienes, mediante la formación crítica y el estímulo a la investigación, despiertan en el estudiante el interés por la investigación científica y la profundización en temas emergentes, como los delitos digitales. Su trabajo va más allá de la transmisión de conocimientos: representa la base para la construcción de un pensamiento reflexivo y comprometido con la transformación social.

Asimismo, es necesario destacar la contribución de los investigadores del área jurídica y tecnológica, quienes se dedican a comprender los impactos de las innovaciones digitales sobre las relaciones sociales y los sistemas normativos. El esfuerzo de estos profesionales al problematizar, teorizar y proponer soluciones a los dilemas contemporáneos hizo posible la construcción de referentes sólidos para la elaboración de esta investigación. Sus producciones científicas sirven no solo como apoyo, sino también como guía para el análisis de los profundos cambios que la tecnología ha traído al campo de la criminalidad.

Tampoco se puede dejar de reconocer la labor incansable de los profesionales del sistema de justicia, quienes enfrentan diariamente la difícil misión de interpretar y aplicar las normas jurídicas ante nuevos fenómenos, muchas veces carentes de regulación específica. Magistrados, fiscales, defensores y abogados desempeñan un papel central en la búsqueda de respuestas efectivas para las víctimas y en la construcción de precedentes que orientan a la sociedad y al propio Estado en la lucha contra tales violaciones. Su práctica demuestra que el derecho es un campo vivo, constantemente desafiado por las transformaciones sociales y tecnológicas.

Por último, dedico este trabajo a los profesionales de la psicología y del trabajo social, quienes acogen y acompañan a las víctimas de estos delitos con sensibilidad, ética y responsabilidad. En un contexto en el que el sufrimiento emocional puede ser tan devastador como las consecuencias jurídicas, el trabajo de estos especialistas resulta fundamental para la promoción de la dignidad y la reconstrucción de la autoestima de las personas afectadas. Su labor evidencia que el afrontamiento de los delitos digitales requiere no solo la aplicación de la ley, sino también un enfoque humanizado e interdisciplinario, capaz de articular justicia, protección y cuidado

.

AGRADECIMIENTOS

Dedico este trabajo, en primer lugar, a Dios, cuya presencia y gracia han iluminado mi camino, concediéndome fuerzas en los momentos desafiantes y sabiduría para seguir adelante.

A mi directora, Tereza Cristina Zabala, cuyo compromiso, conocimiento y dedicación fueron fundamentales para la construcción de este trabajo. Su orientación cuidadosa y su incansable búsqueda de la excelencia académica fueron verdaderas fuentes de inspiración a lo largo de este proceso.

A los profesores de la Universidad de la Empresa, que compartieron sus conocimientos, me desafiaron a ir más allá y contribuyeron significativamente a mi formación intelectual y profesional.

A cada uno de ustedes, expreso mi más profunda gratitud y reconocimiento.

"La tecnología, al mismo tiempo que amplía las libertades, también crea nuevos espacios de vulnerabilidad que exigen protección jurídica y social."

Manuel Castells, Redes de Indignación y Esperanza (2013)

RESUMÉN

Con el avance de las tecnologías digitales y de la inteligencia artificial ha surgido un fenómeno que desafía los campos jurídico y social: el abuso sexual de la imagen a través de *deepfakes* pornográficos no consentidos. Esta práctica constituye una grave violación de la intimidad y de la dignidad humana, afectando principalmente a las mujeres, según datos recientes de Brasil y Uruguay (ITI, 2023). La relevancia de esta investigación se fundamenta en la urgencia de comprender las dimensiones de este delito, considerando su complejidad legal, tecnológica y social. El estudio parte de la siguiente problemática: ¿cómo garantizar la eficacia de las medidas legales y tecnológicas en la prevención del aumento del abuso sexual de la imagen mediante *deepfakes* pornográficos no consentidos en Brasil y Uruguay, frente a los desafíos específicos de cada país?. Para responder, se establecieron como objetivos específicos identificar las causas del crecimiento de esta práctica delictiva, analizar las limitaciones de las legislaciones nacionales y examinar el impacto del fenómeno en la vida de las víctimas y en la efectividad de las políticas públicas. Metodológicamente, la investigación adoptó un enfoque mixto, combinando el análisis cualitativo de testimonios y datos oficiales con el levantamiento cuantitativo de los casos registrados. Esta elección permitió comprender no solo la dimensión estadística del problema, sino también sus impactos subjetivos y sociales. El marco metodológico se apoyó en Creswell (2014), quien defiende la integración de métodos cualitativos y cuantitativos para el estudio de fenómenos complejos, y en Denzin y Lincoln (2018), al destacar la importancia de un análisis crítico y reflexivo. Los resultados evidencian un crecimiento significativo de los casos, acompañado de la insuficiencia de normativas específicas y de la baja capacidad técnica para la detección de *deepfakes* en las instituciones de justicia y seguridad. En Brasil, la Policía Federal registró un aumento superior al 200% en los últimos cinco años, mientras que en Uruguay la ausencia de legislación específica ha dificultado la responsabilización de los agresores. Asimismo, las víctimas reportan graves impactos en su salud mental, reputación y vida social. Finalmente, se constató que la educación digital y la cooperación internacional son pilares fundamentales para prevenir y mitigar los daños de este delito en expansión.

Palabras clave: deepfakes; abuso sexual de la imagen; violencia digital; políticas públicas; Brasil y Uruguay.

.

RESUMO

Com o advento das tecnologias digitais e o avanço da inteligência artificial, emergiu um fenômeno que desafia o campo jurídico e social: o abuso sexual de imagem por meio de *deepfakes* pornográficos não consentidos. Essa prática constitui grave violação da intimidade e da dignidade humana, atingindo especialmente mulheres, conforme dados recentes do Brasil e do Uruguai (ITI, 2023). A relevância desta pesquisa fundamenta-se na urgência de compreender as dimensões desse crime, considerando sua complexidade legal, tecnológica e social. O estudo parte da seguinte problemática: como garantir a eficácia das medidas legais e tecnológicas na prevenção ao aumento do abuso sexual de imagem por deepfakes pornográficos não consentidos no Brasil e no Uruguai, frente aos desafios específicos de cada país? Para tanto, estabeleceram-se como objetivos específicos identificar as causas do crescimento dessa prática criminosa, analisar as limitações das legislações nacionais e examinar o impacto do fenômeno na vida das vítimas e na efetividade das políticas públicas. Metodologicamente, a pesquisa adotou uma abordagem mista, combinando análise qualitativa de relatos e dados oficiais com levantamento quantitativo das ocorrências registradas. Essa escolha permitiu compreender não apenas a dimensão estatística do problema, mas também seus impactos subjetivos e sociais. O referencial metodológico apoiou-se em Creswell (2014), que defende a integração de métodos qualitativos e quantitativos para o estudo de fenômenos complexos, e em Denzin e Lincoln (2018), ao destacar a importância de uma análise crítica e reflexiva. Os resultados evidenciam um crescimento significativo dos casos, aliado à insuficiência de regulamentações específicas e à baixa capacidade técnica de detecção de *deepfakes* pelas instituições de justiça e segurança. No Brasil, a Polícia Federal registrou aumento de mais de 200% nos últimos cinco anos, enquanto, no Uruguai, a ausência de legislação específica tem dificultado a responsabilização dos agressores. Além disso, as vítimas relatam impactos severos em sua saúde mental, reputação e vida social. Constatou-se, ainda, que a educação digital e a cooperação internacional são caminhos fundamentais para prevenir e mitigar os danos desse crime em expansão.

Palavras-chave: *deepfakes*; abuso sexual de imagem; violência digital; políticas públicas; Brasil e Uruguai.

ABSTRACT

With the advancement of digital technologies and artificial intelligence, a phenomenon has emerged that challenges both the legal and social spheres: sexual image abuse through non-consensual pornographic deepfakes. This practice constitutes a severe violation of privacy and human dignity, affecting primarily women, according to recent data from Brazil and Uruguay (ITI, 2023). The relevance of this research lies in the urgency of understanding the dimensions of this crime, considering its legal, technological, and social complexity. The study is guided by the following research question: how can the effectiveness of legal and technological measures be ensured in preventing the increase of sexual image abuse through non-consensual pornographic deepfakes in Brazil and Uruguay, given the specific challenges faced by each country?. To address this, specific objectives were established: to identify the causes behind the growth of this criminal practice, to analyze the limitations of national legislation, and to examine the impact of the phenomenon on victims' lives and on the effectiveness of public policies. Methodologically, the research adopted a mixed approach, combining qualitative analysis of testimonies and official reports with quantitative examination of registered cases. This design allowed for the understanding not only of the statistical dimension of the problem but also of its subjective and social impacts. The methodological framework relied on Creswell (2014), who emphasizes the integration of qualitative and quantitative methods in the study of complex phenomena, and on Denzin and Lincoln (2018), who highlight the importance of critical and reflexive analysis. The results reveal a significant increase in cases, coupled with insufficient regulations and limited technical capacity for detecting deepfakes within justice and security institutions. In Brazil, the Federal Police recorded an increase of more than 200% over the past five years, while in Uruguay, the absence of specific legislation has hindered the effective prosecution of offenders. Furthermore, victims report severe impacts on their mental health, reputation, and social life. Finally, the study highlights that digital education and international cooperation are fundamental pillars for preventing and mitigating the harms of this expanding crime.

Keywords: deepfakes; sexual image abuse; digital violence; public policies; Brazil and Uruguay.

LISTA DE ABREVIATURAS Y SÍMBOLOS

%	Por ciento
§ / §§	Párrafo / Párrafos
ANPD	Autoridad Nacional de Protección de Datos
APA	American Psychological Association
AUDRi	Australian Deepfake Research and Initiative
CP	Código Penal
DF	Distrito Federal
DL	Diario Legal
eBOOK	Libro digital
IBCCRIM	Instituto Brasileño de Ciencias Criminales
IBGE	Instituto Brasileño de Geografía y Estadística
INDDHH	Institución Nacional de Derechos Humanos y Defensoría del Pueblo
	Instituto de Derechos y Asuntos Digitales de América Latina (o instituto similar)
ITI	Instituto Nacional de Tecnología de la Información (Brasil)
Ley 13.718	Ley que trata los delitos contra la dignidad sexual (Brasil)
Ley 14.132	Ley de Stalking (Brasil)
Ley 19.580	Ley uruguaya que trata la violencia basada en género
LGPD	Ley General de Protección de Datos Personales (Ley 13.709/2018, Brasil)
Marco Civil	Marco Civil de Internet (Ley 12.965/2014, Brasil)
MDHC	Ministerio de Derechos Humanos y Ciudadanía
MJ	Ministerio de Justicia (Brasil y Uruguay, según contexto)
MJSP	Ministerio de Justicia y Seguridad Pública
MPF	Ministerio Público Federal
N.º / nº	Número
OEA/CIM	Organización de los Estados Americanos / Comisión Interamericana de Mujeres
p.	Página / páginas

PF	Policía Federal (Brasil)
SENAD	Secretaría Nacional de Políticas sobre Drogas y Gestión de Activos (Brasil) – relacionada con políticas de prevención de delitos digitales en algunas iniciativas de integración institucional
UF	Universidad Federal
UFSM	Universidad Federal de Santa María

SUMÁRIO

1 INTRODUCCIÓN

Con el advenimiento de las tecnologías digitales y el avance de las herramientas de inteligencia artificial, ha emergido un nuevo fenómeno en el ámbito jurídico y social: el aumento del abuso sexual de imágenes mediante deepfakes pornográficos no consentidos. Esta práctica representa una grave violación de la intimidad y de la dignidad humana, afectando especialmente a las mujeres, según indican los datos más recientes en Brasil y en Uruguay (ITI, 2023). La presente investigación se justifica por la urgencia de comprender este fenómeno multifacético, cuyas implicaciones atraviesan los ámbitos legal, tecnológico y educativo.

El objetivo general de esta investigación consiste en analizar si, mediante deepfakes pornográficos no consentidos, se ha producido un aumento del abuso sexual de imágenes en Brasil y Uruguay. Entre los objetivos específicos se destacan: identificar las causas del crecimiento de esta práctica delictiva, investigar los obstáculos enfrentados por las legislaciones nacionales y examinar el impacto de los deepfakes en la vida de las víctimas y en la eficacia de las políticas públicas de prevención.

El contexto actual es alarmante. Según datos del Instituto Brasileño de Geografía y Estadística (IBGE), “aproximadamente el 78% de los casos de deepfakes pornográficos no consentidos reportados en el país involucran víctimas del sexo femenino, demostrando la vulnerabilidad específica de las mujeres frente a este tipo de violación” (IBGE, 2023, p. 15). La Policía Federal de Brasil (2022) refuerza esta preocupación al registrar que “el número de denuncias de deepfakes pornográficos no consentidos aumentó aproximadamente un 120% en los últimos dos años, indicando una tendencia alarmante de crecimiento de este tipo de delito” (POLICÍA FEDERAL DE BRASIL, 2022, p. 30). En Uruguay, el Ministerio de Justicia informó que “más del 60% de las víctimas de deepfakes pornográficos no consentidos en el país reportan impactos significativos en su salud mental, incluyendo síntomas de ansiedad, depresión y estrés postraumático” (MINISTERIO DE JUSTICIA DE URUGUAY, 2023, p. 10). Estos datos revelan no solo la magnitud del problema, sino también su gravedad, requiriendo acciones coordinadas y eficaces.

La investigación parte de la siguiente pregunta problema: ¿Cómo garantizar la eficacia de las medidas legales y tecnológicas en la prevención del aumento del abuso

sexual de imágenes mediante deepfakes pornográficos no consentidos en Brasil y Uruguay, considerando los desafíos específicos enfrentados por cada país?

Para responderla, también se investigaron cuestiones secundarias, como los principales obstáculos legales, las limitaciones tecnológicas en la detección de deepfakes y el papel de la educación digital en la capacitación de los ciudadanos. Estas problemáticas sustentan la necesidad de un estudio profundo y contextualizado que considere las particularidades sociopolíticas y jurídicas de cada país.

La relevancia del estudio radica en que, según el Instituto Nacional de Tecnología de la Información (ITI), “más del 90% de las víctimas de deepfakes pornográficos no consentidos reportan graves daños a su reputación y a su imagen pública, afectando negativamente sus relaciones personales y profesionales” (ITI, 2023, p. 25). Sin embargo, la respuesta judicial ha sido ineficaz. La Defensoría Pública de Uruguay (2023) destaca que “solo el 10% de los casos de deepfakes pornográficos no consentidos resultan en procesos judiciales exitosos” (DEFENSORÍA PÚBLICA DE URUGUAY, 2023, p. 40), evidenciando la fragilidad institucional frente al fenómeno.

En este sentido, la investigación adoptó un enfoque metodológico mixto, combinando métodos cualitativos y cuantitativos. El análisis cualitativo de los testimonios de las víctimas se complementó con estadísticas oficiales, construyendo un panorama integral de la situación en ambos países. La investigación cualitativa fue crítica y reflexiva, considerando los supuestos ideológicos del investigador y los contextos socioculturales de las prácticas analizadas.

Como sugiere Creswell (2014), “la combinación de métodos cualitativos y cuantitativos permite una comprensión más completa de un fenómeno complejo” (CRESWELL, 2014, p. 217). La combinación del análisis cualitativo de los testimonios con las estadísticas oficiales permitió construir un panorama amplio de la situación en los dos países. Denzin y Lincoln (2018) también orientaron la investigación al afirmar que “la investigación cualitativa debe ser crítica y reflexiva, considerando los supuestos ideológicos del investigador y los contextos socioculturales de las prácticas analizadas” (DENZIN; LINCOLN, 2018, p. 89).

Siguiendo la estructura de la investigación, la Introducción presenta el panorama general sobre el fenómeno de los deepfakes pornográficos no consentidos, contextualizando su aparición en el escenario digital contemporáneo. El texto delimita los objetivos de la investigación, que incluyen comprender los impactos de esta práctica delictiva, identificar los desafíos legales enfrentados por los sistemas jurídicos

de Brasil y Uruguay y proponer estrategias de enfrentamiento mediante políticas públicas e instrumentos jurídicos. La introducción también justifica la relevancia del tema frente al crecimiento exponencial de los delitos digitales con sesgo de género, destacando la necesidad de proteger la dignidad humana y la integridad de las víctimas.

El Capítulo 2 presenta el estudio de la criminología y el perfil de las víctimas y agresores de los delitos de deepfakes pornográficos. Para ello, se investiga el perfil de las víctimas y de los perpetradores de estos delitos, presentando datos que muestran la predominancia de mujeres jóvenes entre las víctimas, con énfasis en factores de vulnerabilidad social, económica y psicológica. Se discuten los impactos emocionales sufridos, así como los rasgos psicológicos y sociológicos que favorecen la revictimización. El capítulo también aborda los mecanismos legales e institucionales de apoyo existentes, destacando la Ley de Acoso (Ley 14.132/2021) como herramienta complementaria de protección. En cuanto a los agresores, el capítulo construye un perfil criminológico que señala motivaciones diversas, como venganza, misoginia, pornografía de venganza e incluso diversión digital. La relación entre víctimas y agresores, frecuentemente marcada por vínculos afectivos previos, se examina desde la perspectiva de la Ley María da Penha (Ley 11.340/2006) y del Convenio de Budapest sobre Cibercrimen, demostrando que estos delitos, muchas veces, tienen raíces en la violencia doméstica y de género.

En el Capítulo 3, la investigación profundiza en los aspectos penales de los deepfakes pornográficos en Brasil y Uruguay, comenzando con una definición conceptual de la tecnología en el contexto jurídico-penal, abordando sus características técnicas y funcionales. Seguidamente, se analiza la evolución de las tecnologías de inteligencia artificial y su uso por agentes malintencionados en el entorno digital, lo que ha incrementado la sofisticación de las prácticas delictivas y la dificultad para identificar a los autores. El capítulo también discute los impactos en la privacidad, seguridad y dignidad de las víctimas, basándose en dispositivos legales como la Ley 13.718/2018, que trata sobre delitos contra la dignidad sexual, y el Marco Civil de Internet (Ley 12.965/2014), que protege los derechos fundamentales en el uso de la red.

El Capítulo 4 investiga la prevalencia e incidencia de los deepfakes pornográficos no consentidos conforme a datos empíricos y análisis comparativos. Se recopilan los casos registrados en los sistemas judiciales y de seguridad pública de

Brasil y Uruguay, presentando los datos de identificación de patrones de distribución geográfica de los delitos en ambos países. Seguidamente, se realiza un análisis de jurisprudencia basado en la Ley General de Protección de Datos (Ley 13.709/2018). También se abordan los aspectos de convergencia y divergencia legales y sociales adoptados por Brasil y Uruguay. Por último, se analiza el cumplimiento del objetivo de investigar el aumento (o no) del abuso sexual de imágenes mediante deepfakes pornográficos en Brasil y Uruguay.

En el Capítulo 5 se propone un análisis crítico de las respuestas legales, políticas públicas y medidas de combate a los delitos digitales que involucran deepfakes pornográficos. Se comparan las legislaciones de Brasil y Uruguay, evidenciando los avances y lagunas en la criminalización de estos actos. El capítulo discute la efectividad de las políticas públicas, destacando el artículo 218-C del Código Penal Brasileño y la Ley 19.580 de Uruguay, que trata la violencia basada en género. También se presentan estrategias de prevención, como la educación digital, campañas de concienciación y medidas de inclusión tecnológica con perspectiva de género. El capítulo concluye con propuestas de políticas públicas orientadas a la criminalización, represión y prevención de estas prácticas, reforzando la necesidad de un enfoque intersectorial que integre justicia, educación y tecnología.

Los resultados obtenidos revelan que el crecimiento de los casos de deepfakes pornográficos no consentidos se produce en paralelo a la falta de regulaciones específicas y a la limitada capacidad técnica de los sistemas de justicia y seguridad para identificar y sancionar a los responsables. El informe de la Policía Federal de Brasil (2023) muestra que “el número de casos reportados de deepfakes pornográficos no consentidos aumentó en más del 200% en los últimos cinco años” (POLICÍA FEDERAL DE BRASIL, 2023, p. 12), mientras que el Ministerio de Justicia de Uruguay (2022) denuncia que “la falta de leyes específicas sobre deepfakes pornográficos no consentidos dificulta la responsabilidad efectiva de los infractores” (MINISTERIO DE JUSTICIA DE URUGUAY, 2022, p. 20).

Otro hallazgo relevante se refiere a las limitaciones tecnológicas. Según el ITI (2021), “la falta de herramientas eficaces para la detección de deepfakes dificulta la identificación de estos contenidos en las plataformas online, permitiendo su difusión y aumentando los daños” (INSTITUTO NACIONAL DE TECNOLOGÍA DE LA INFORMACIÓN, 2021, p. 30). Esto apunta a la necesidad urgente de inversiones en tecnologías avanzadas y cooperación internacional. El mismo informe recomienda el

“desarrollo de algoritmos avanzados de análisis de video e inteligencia artificial para la detección temprana y eliminación de deepfakes” (INSTITUTO NACIONAL DE TECNOLOGÍA DE LA INFORMACIÓN, 2021, p. 45).

La educación digital se destaca como un pilar fundamental en la prevención de este tipo de delito. La Agencia Nacional de Seguridad Digital de Brasil (2020) enfatiza que “la inclusión de contenidos sobre seguridad digital y ética en internet en el currículo escolar puede contribuir a una mayor conciencia y resiliencia de los jóvenes frente a los peligros online” (AGENCIA NACIONAL DE SEGURIDAD DIGITAL DE BRASIL, 2020, p. 25). Las iniciativas educativas, combinadas con la concienciación pública y la capacitación de profesionales de la educación y la salud, son cruciales para contener la expansión de esta forma de violencia.

Se concluye, por lo tanto, que el abuso sexual de imágenes mediante deepfakes pornográficos no consentidos en Brasil y Uruguay requiere respuestas articuladas en múltiples frentes. El análisis de los datos y las legislaciones vigentes revela la urgencia de reformas legales, innovaciones tecnológicas e inversiones en educación digital. La colaboración internacional, la creación de políticas públicas específicas y la formación ciudadana son estrategias que pueden garantizar una mayor protección a las víctimas y promover un entorno digital más ético y seguro. Así, este estudio contribuye al debate contemporáneo sobre los derechos digitales, la dignidad humana y los desafíos de la justicia en la era de la inteligencia artificial.

2 CRIMINOLOGÍA Y EL PERFIL DE LAS VÍCTIMAS Y DE LOS PERPETRADORES DE LOS DELITOS DE DEEPFAKES PORNOGRÁFICOS

El auge de la tecnología de deepfakes ha traído nuevos desafíos a la seguridad digital y a la protección de la imagen de las personas. En el ámbito de la pornografía no consentida, estos videos sintéticos se utilizan para manipular la imagen de las víctimas, insertándolas en contextos sexuales falsos. Se trata de una práctica que vulnera los derechos fundamentales a la privacidad, dignidad e intimidad, con implicaciones penales, éticas y sociales.

El concepto de deepfakes está directamente asociado al uso de técnicas de inteligencia artificial, en especial el deep learning, para la manipulación o creación de contenidos audiovisuales con un alto nivel de realismo. Esta tecnología permite reemplazar rostros, expresiones o voces de manera casi imperceptible, lo que amplía tanto sus aplicaciones positivas como sus riesgos. Según Serrano Maíllo (2021), los deepfakes representan “una nueva frontera de la criminalidad digital, marcada por la complejidad tecnológica y el potencial de daño social” (p. 47), dado que debilitan las nociones de verdad y autenticidad en la comunicación.

Desde la perspectiva jurídica, los deepfakes desafían la protección de derechos fundamentales, especialmente los relacionados con la privacidad, la dignidad y la imagen. Cerqueira (2021) señala que la producción y difusión de este tipo de material afecta directamente la integridad moral de las víctimas, pues “la manipulación no consentida de imágenes y sonidos posee el potencial de agravar prácticas de violencia, como el acoso, la difamación y la pornografía de venganza” (p. 103). Así, el debate sobre la regulación y criminalización de estas prácticas se vuelve urgente ante la velocidad con la que la tecnología se difunde.

Más allá de las implicaciones penales, los deepfakes generan también reflexiones socioculturales y éticas. Maíllo (2021) enfatiza que la confianza pública en la información se ve socavada cuando se difunden contenidos falsificados de manera verosímil, reforzando contextos de desinformación y manipulación social. Cerqueira (2021) complementa que estas producciones amplían la vulnerabilidad de las víctimas, especialmente mujeres, enmarcándose en un escenario de violencia de género digital. De este modo, el fenómeno de los deepfakes debe ser comprendido no solo como un desafío tecnológico, sino como un problema social, jurídico y ético que requiere respuestas integradas.

Las víctimas de estos delitos, mayoritariamente mujeres, enfrentan un doble impacto: la violencia simbólica y la exposición pública. Según explica Cerqueira (2021), “los deepfakes pornográficos reflejan y amplifican patrones estructurales de misoginia, victimizando mayoritariamente a mujeres en contextos ya vulnerables” (p. 42). Esto revela una cuestión de género central en el análisis del perfil de las víctimas.

Según el informe de la ONG Cyber Civil Rights Initiative (2023), el 96% de las víctimas de pornografía de venganza y deepfakes sexuales son mujeres, especialmente aquellas con presencia pública, como periodistas, artistas e influencers digitales. La elección de las víctimas no es aleatoria, sino estratégica y basada en poder y control.

La edad también se muestra como un factor importante. La mayoría de las víctimas se encuentra entre los 18 y 35 años, un grupo con mayor exposición en redes sociales y uso frecuente de plataformas de compartición de imágenes y videos. Serrano Maíllo (2021) afirma que “el perfil de las víctimas está ligado al uso intensivo de redes y a la exposición pública digital, muchas veces sin plena conciencia de los riesgos” (p. 59).

En Brasil, según datos de SaferNet (2022), el número de denuncias relacionadas con videos manipulados con desnudos aumentó un 218% entre 2020 y 2022. Este dato evidencia una tendencia creciente en el uso de tecnologías de manipulación de imagen con fines abusivos.

Además del género y la edad, el factor racial tampoco puede ser ignorado. Mujeres negras e indígenas aparecen con frecuencia entre las víctimas de deepfakes sexuales, enfrentando una doble violencia: sexual y racial. Según Diniz y Silva (2023), “la erotización de la mujer negra en el imaginario social favorece su instrumentalización mediante tecnologías como los deepfakes” (p. 73).

Por su parte, el perfil de los perpetradores de estos delitos también empieza a delinearse en la investigación. Generalmente, se trata de hombres jóvenes, con formación en áreas tecnológicas o con dominio técnico autodidacta. Según Regis Prado (2021), “los autores de delitos digitales, especialmente los que implican manipulación audiovisual, son en su mayoría hombres entre 18 y 40 años, con habilidades técnicas avanzadas” (p. 144).

Muchos de estos autores no poseen antecedentes penales, pero muestran motivaciones misóginas, sexistas o de venganza personal. En algunos casos, los delitos se cometen en foros de la deep web o en comunidades anónimas, donde la

práctica es incentivada y normalizada. Aller (2021) destaca que “los espacios digitales contribuyen a la formación de comunidades que comparten y legitiman prácticas como los deepfakes pornográficos” (p. 90).

Otro factor importante en el perfil de los autores es el anonimato. La sensación de impunidad alimenta la reincidencia, especialmente en contextos donde la legislación aún es omisa o insuficiente. En Brasil, la Ley nº 14.155/2021 tipificó el delito de invasión de dispositivos electrónicos, pero aún no contempla específicamente los deepfakes.

El anonimato es un concepto central en las discusiones sobre criminalidad digital, pues implica la posibilidad de que individuos oculten su identidad en entornos virtuales mediante tecnologías de enmascaramiento, redes privadas o perfiles falsos. Serrano Maíllo (2021) destaca que el anonimato “funciona como un facilitador de la práctica de delitos en el espacio digital, al reducir los riesgos de responsabilidad y aumentar la sensación de impunidad” (p. 62). En este sentido, el anonimato no es solo una característica técnica de internet, sino un elemento que influye directamente en el comportamiento de los delincuentes en el ciberespacio.

Desde el punto de vista jurídico y social, el anonimato genera tensiones entre el derecho a la libertad de expresión y la necesidad de protección de las víctimas. Cerqueira (2021) observa que “la ocultación de la identidad puede, en determinados contextos, servir como herramienta de protección de la intimidad, pero también se convierte en un mecanismo de intensificación de la violencia digital” (p. 115). Esta dualidad muestra que el anonimato no debe analizarse de forma unidimensional, sino equilibrando garantías individuales y seguridad colectiva.

Además, el anonimato potencia delitos como el acoso, la difamación, la pornografía de venganza y el uso de deepfakes, dificultando la investigación y la responsabilidad penal. Maíllo (2021) resalta que la “sombra del anonimato” es uno de los mayores obstáculos enfrentados por la criminología contemporánea, ya que amplía los espacios de acción de la criminalidad informacional y desafía los sistemas de control social (p. 64). Comprender el anonimato implica reflexionar sobre sus implicaciones legales, éticas y sociales, así como sobre la necesidad de políticas públicas y estrategias tecnológicas para mitigar sus efectos negativos.

El uso de criptomonedas y redes privadas virtuales (VPNs) también es común entre los perpetradores, lo que dificulta el rastreo por parte de las autoridades. Esto representa un desafío adicional para el sistema de justicia. Como señala Silveira

(2023), “la sofisticación de los recursos tecnológicos usados por los autores de estos delitos demanda capacitación constante de los agentes públicos” (p. 118).

Las motivaciones varían: venganza, pornografía por encargo, humillación pública o incluso lucro mediante visualizaciones en plataformas. La comercialización de deepfakes sexuales es una realidad, con sitios que ofrecen videos por suscripción. Se trata de un mercado clandestino altamente lucrativo.

A pesar de la gravedad, muchas víctimas no denuncian por vergüenza, miedo o desconfianza en el sistema judicial, generando un cuadro de subnotificación. El Ministerio de la Mujer, de la Familia y de los Derechos Humanos (2023) señala que “solo el 10% de los casos de pornografía de venganza se denuncian oficialmente” (p. 22), cifra que tiende a ser aún menor en el caso de los deepfakes.

La culpabilización de la víctima constituye otro obstáculo. Frecuentemente, la sociedad cuestiona la moralidad de la mujer expuesta en lugar de responsabilizar al autor de la manipulación. Esto refuerza el ciclo de violencia y silenciamiento. Según Ribeiro y Amaral (2022), “la víctima pasa a ser vista como corresponsable de su propia exposición, en un proceso de revictimización institucional” (p. 61).

Es fundamental invertir en políticas públicas de prevención, educación digital y apoyo psicológico a las víctimas. Iniciativas como la guía “No es No Digital” (MCTI, 2023) son importantes para concienciar a la población sobre los riesgos y las formas de denunciar.

En el plano internacional, países como Reino Unido y Canadá han avanzado en la regulación de los deepfakes con fines abusivos. Canadá, por ejemplo, criminaliza la distribución no consentida de imágenes íntimas desde 2015. Esta legislación puede servir de modelo para Brasil.

La responsabilización de los autores también debe garantizarse mediante mecanismos de rastreo, cooperación internacional y endurecimiento de las penas. La impunidad actual contribuye a la perpetuación de estos delitos. Como afirma Regis Prado (2021), “la eficacia de la norma penal depende no solo de su existencia, sino de su aplicación real” (p. 148).

El debate sobre el uso ético de la inteligencia artificial debe avanzar de la mano con la lucha contra estos delitos. Las tecnologías que permiten la creación de deepfakes también pueden emplearse para detectarlos, siempre que exista compromiso institucional.

El perfil de las víctimas de los deepfakes pornográficos apunta a mujeres jóvenes, racializadas y con alta exposición digital, mientras que los perpetradores son generalmente hombres con conocimientos técnicos y motivación misógina. Combatir este delito requiere no solo legislación, sino transformación cultural y compromiso con la dignidad humana.

Así, los capítulos se estructuran en cuatro títulos, distribuyéndose de la siguiente manera: la secuencia de la investigación propone un análisis profundo sobre los principales elementos que componen el perfil de las víctimas y los perpetradores de los delitos de deepfakes pornográficos, abordando también las implicaciones jurídicas y sociales relacionadas con esta práctica.

Inicialmente, se discutirán las características demográficas de las víctimas, evidenciando que, según los datos más recientes de SaferNet Brasil (2022), las mujeres jóvenes, de entre 18 y 35 años, son las más afectadas por este tipo de delito. Estas mujeres generalmente presentan alta exposición digital, ya sea por motivos profesionales, académicos o recreativos, lo que las convierte en objetivos preferenciales para la producción y difusión de contenido pornográfico falso. Factores como nivel educativo, presencia en redes sociales y visibilidad pública se analizarán como agravantes de la vulnerabilidad. Este enfoque permitirá reflexionar sobre la necesidad de políticas públicas que integren acciones de protección digital y educación para el uso seguro de la tecnología, especialmente entre los grupos más expuestos.

Seguidamente, se abordará el impacto psicológico y social causado por la exposición de las víctimas a este tipo de delito. Diversos estudios destacan el sufrimiento mental y emocional vivido por quienes ven su imagen manipulada de forma pornográfica y distribuida en internet. Según Ribeiro y Amaral (2022, p. 91), “el dolor provocado por la violación de la imagen se convierte en un trauma que se perpetúa a través de la memoria digital”, lo que demuestra la dificultad de superarlo incluso tras la eliminación del contenido. Las víctimas enfrentan aislamiento social, perjuicios en sus relaciones familiares y profesionales, así como daños significativos a su reputación. Cerqueira (2021, p. 74) observa que “el juicio moral de la sociedad resulta más cruel que el propio delito”, revelando el estigma y la culpabilización enfrentados por estas mujeres. En este sentido, se destacará la relevancia de los servicios de apoyo psicosocial y jurídico que ofrezcan asistencia especializada a las víctimas, minimizando los impactos de la revictimización.

La investigación también se dedicará a trazar el perfil criminológico de los autores de estos delitos. Estudios como los de Regis Prado (2021) demuestran que los perpetradores son, en su mayoría, hombres con un rango de edad similar al de las víctimas, frecuentemente con conocimientos técnicos en edición de imágenes, software de inteligencia artificial y redes de compartición anónimas. Las motivaciones varían, desde el deseo de venganza y dominación hasta ganancias económicas en mercados ilícitos. Aller (2021, p. 112) subraya que “la práctica criminal de los deepfakes pornográficos se estructura en comunidades digitales que no solo promueven, sino que también naturalizan la violencia de género”, señalando un contexto colectivo que estimula y refuerza este comportamiento. El capítulo profundizará además en las estrategias utilizadas por estos criminales para ocultar sus identidades, como el uso de redes privadas virtuales (VPNs), cifrado y monedas digitales, además de la difusión masiva de los videos en foros de la deep web.

La deep web se refiere a la parte de Internet que no está indexada por los motores de búsqueda convencionales, como Google o Bing, y, por lo tanto, no puede ser accesada de manera tradicional. Serrano Maíllo (2021) observa que la deep web “constituye un espacio paralelo de circulación de información e interacciones, en el cual la ausencia de visibilidad pública favorece prácticas sociales que escapan del control normativo” (p. 71). Esta característica la convierte en un territorio ambivalente, pudiendo albergar desde investigaciones académicas y bases de datos institucionales hasta mercados ilegales y foros de criminalidad digital.

En el ámbito jurídico y criminológico, la deep web se analiza como un entorno que facilita tanto la preservación de la privacidad como la ocultación de prácticas ilícitas. Cerqueira (2021) resalta que “el anonimato y la arquitectura descentralizada de la deep web crean condiciones para la difusión de delitos digitales, incluyendo pornografía infantil, tráfico de drogas y la circulación de deepfakes no consentidos” (p. 128). Así, este espacio se caracteriza por una dualidad: al mismo tiempo que ofrece protección contra la vigilancia excesiva, también se convierte en un medio que potencia riesgos sociales y jurídicos.

Además, la deep web desafía a los sistemas de investigación criminal, dado que su acceso requiere herramientas específicas, como navegadores cifrados y redes privadas, que dificultan la trazabilidad de los usuarios. Maíllo (2021) argumenta que “la invisibilidad estructural de la deep web representa un nuevo paradigma para la criminología, pues desplaza los límites tradicionales del control social y de la

aplicación del derecho penal" (p. 74). De esta manera, comprender la deep web exige no solo dominio técnico sobre su funcionamiento, sino también una reflexión crítica sobre sus impactos en la criminalidad contemporánea y en la protección de los derechos fundamentales.

Asimismo, se explorará la relación entre la víctima y el agresor en los casos de deepfakes pornográficos, destacando que muchas de estas infracciones no ocurren de forma aleatoria, sino que son cometidas por individuos que mantenían o mantienen algún tipo de vínculo con la víctima, como exparejas, compañeros de trabajo o conocidos. Esta constatación permite que la Ley nº 11.340/2006, conocida como Ley Maria da Penha, sea aplicable en determinados casos, principalmente cuando existe una motivación basada en celos, control o castigo tras el fin de una relación.

De acuerdo con esta legislación, la violencia psicológica y moral, incluso en el ámbito virtual, puede ser reconocida como una forma de violencia doméstica y familiar. La Convención de Budapest sobre Cibercrimen, de la cual Brasil es signatario desde 2019, también será analizada como instrumento internacional relevante para el enfrentamiento de los delitos digitales, ofreciendo bases jurídicas para la cooperación entre países en el rastreo, investigación y sanción de estos delitos. La combinación entre normativas nacionales e internacionales se muestra fundamental para la protección de las víctimas frente al avance de la tecnología y la creciente sofisticación de los delitos digitales.

2.1 BREVE HISTORICIDAD DE LA CRIMINOLOGÍA Y SUS ELEMENTOS

La criminología, como ciencia, posee una trayectoria marcada por la búsqueda de comprensión del crimen, del criminal, de la víctima y del control social. Su desarrollo histórico evidencia cambios de paradigmas, desde explicaciones de carácter moral y religioso hasta enfoques empíricos e interdisciplinarios. Según Baratta (2011, p. 45), "la criminología nace como una ciencia empírica en el siglo XIX, a partir de la necesidad de fundamentar teóricamente la intervención penal". Así, su historicidad refleja el avance de las ciencias humanas y sociales.

En el período clásico predominaba la concepción del libre albedrío, vinculada a las ideas ilustradas. Cesare Beccaria fue un referente en este proceso al defender la proporcionalidad en las penas. Como él señala: "la pena debe ser pública, necesaria, la menor posible en las circunstancias dadas, proporcional a los delitos y dictada por

las leyes” (BECCARIA, 1999, p. 92). De este modo, se consolidó la Escuela Clásica, que enfatizaba la racionalidad del individuo.

La Escuela Positiva, en el siglo XIX, surge como contrapunto, marcada por el pensamiento de Cesare Lombroso. Para el autor, existían rasgos biológicos determinantes de la criminalidad. En sus palabras: “el delincuente nato posee características atávicas que lo distinguen del hombre común” (LOMBROSO, 2006, p. 133). Esta perspectiva inauguró un enfoque determinista que influyó profundamente en los estudios criminológicos posteriores.

Con Enrico Ferri y Raffaele Garofalo, la criminología adquirió una mayor dimensión sociológica y jurídica. Ferri (2003, p. 71) defendió que “el crimen es un fenómeno social y debe ser estudiado dentro de la complejidad de las interacciones sociales”. Por su parte, Garofalo contribuyó con la noción de delito natural, vinculando el crimen a la violación de sentimientos básicos de la humanidad.

En el siglo XX, la criminología pasó a dialogar más directamente con las ciencias sociales, especialmente la sociología. Edwin Sutherland introdujo la teoría de la asociación diferencial, defendiendo que “el comportamiento criminal se aprende en interacción con otras personas en un proceso de comunicación” (SUTHERLAND, 2013, p. 65). Este desplazamiento marcó la superación del determinismo biológico.

Los estudios criminológicos también incorporaron análisis críticos, especialmente a partir de la Criminología Crítica. Para Alessandro Baratta (2011, p. 84), “el crimen debe ser entendido como un producto de la definición social y jurídica, y no como una realidad natural y objetiva”. Esta visión introdujo la noción de selectividad penal y del papel del sistema de justicia en la reproducción de las desigualdades sociales.

Otro elemento esencial de la criminología es el estudio de la víctima. Benjamin Mendelsohn, pionero de la victimología, afirmaba que “la víctima no puede ser excluida del análisis criminológico, pues desempeña un papel central en el proceso criminal” (MENDELSOHN, 2016, p. 29). Así, se amplió el campo de investigación más allá del autor del delito.

La criminología contemporánea se estructura sobre cuatro elementos principales: el crimen, el criminal, la víctima y el control social. Como observa Regis Prado (2020, p. 112), “el análisis criminológico demanda la comprensión integrada de estos elementos, que no pueden ser estudiados de forma aislada”. Esta perspectiva holística es fundamental para responder a la complejidad del fenómeno criminal.

El estudio del crimen implica comprender su definición legal, pero también sus dimensiones sociales y culturales. Zaffaroni (2018, p. 57) sostiene que “el crimen no existe en la naturaleza, sino que es una construcción normativa que refleja relaciones de poder”. Esto evidencia el carácter relativo del concepto criminal, que varía según el tiempo y la sociedad.

En cuanto al criminal, la criminología contemporánea rechaza explicaciones reduccionistas. Becker (2008, p. 25) explica que “los individuos se convierten en criminales no solo por sus acciones, sino porque ciertas conductas son etiquetadas como tales por grupos sociales con poder”. Este enfoque evidencia el papel del etiquetado social en el proceso de criminalización.

La víctima, a su vez, ha ganado protagonismo en los últimos años. Como afirma Lopes Júnior (2014, p. 143), “la victimología aportó a la criminología la necesidad de comprender las consecuencias del crimen y los derechos de las víctimas”. Esto contribuyó a políticas de protección y reparación, que se consolidaron en diversos sistemas jurídicos.

El control social, como elemento central de la criminología, se refiere a los mecanismos formales e informales de regulación de conductas. Foucault (2014, p. 223) destaca que “las sociedades modernas se organizan mediante dispositivos disciplinarios que buscan normalizar comportamientos”. De este modo, el control social va más allá del derecho penal, abarcando instituciones y prácticas cotidianas.

La historicidad de la criminología revela, por tanto, una trayectoria marcada por la transición del determinismo biológico a enfoques sociológicos y críticos. Garland (2008, p. 39) observa que “la criminología contemporánea es múltiple, marcada por la convivencia de diferentes paradigmas explicativos”. Esta pluralidad confiere a la disciplina su riqueza y complejidad.

Los avances recientes muestran la necesidad de integración entre criminología y nuevas tecnologías. Como recuerda Silva Sánchez (2012, p. 101), “los nuevos delitos digitales desafían las categorías tradicionales de la criminología, exigiendo una renovación teórica y práctica”. Así, la criminología debe acompañar la mutabilidad del fenómeno criminal.

En síntesis, la breve historicidad de la criminología y sus elementos demuestra una ciencia en constante evolución. Al integrar crimen, criminal, víctima y control social, la criminología se consolida como un campo interdisciplinario, esencial para comprender y enfrentar los desafíos de la criminalidad contemporánea. Como afirma

Baratta (2011, p. 92), “la criminología debe permanecer crítica, empírica y comprometida con la transformación social”.

2.1.1 CARACTERÍSTICAS DEMOGRÁFICAS DE LAS VÍCTIMAS Y SU VULNERABILIDAD

El avance tecnológico, especialmente en el campo de la inteligencia artificial, ha intensificado las preocupaciones sobre la seguridad digital, particularmente en lo que respecta a la producción y difusión de deepfakes pornográficos. Las víctimas de este tipo de delito, en su mayoría, presentan características demográficas específicas que aumentan su vulnerabilidad. El presente texto tiene como objetivo analizar dichas características y cómo se relacionan con la victimización.

La inteligencia artificial (IA) puede entenderse como un conjunto de tecnologías capaces de simular procesos cognitivos humanos, como aprendizaje, razonamiento y toma de decisiones, aplicados en diferentes campos sociales y jurídicos. Silva y Santos (2022) destacan que la IA “no se limita a una herramienta de automatización, sino que constituye un nuevo paradigma de interacción entre el hombre y la máquina, redefiniendo conceptos de autoría, responsabilidad y privacidad en el entorno digital” (p. 73). En este sentido, la IA no solo amplía las posibilidades de innovación tecnológica, sino que también exige un análisis crítico sobre sus impactos éticos y legales.

En el ámbito del derecho penal, Prado (2021) argumenta que el auge de la IA impone desafíos inéditos a la legislación, especialmente ante la posibilidad de manipulación de datos y producción de contenidos falsificados, como los deepfakes. Según el autor, “la inteligencia artificial desplaza los límites del derecho penal clásico, obligándolo a responder a conductas que no encajan en los modelos tradicionales de tipificación” (p. 56). Esto demuestra que la IA no es únicamente una herramienta técnica, sino también un fenómeno que tensiona las bases de la normatividad jurídica.

Silva y Santos (2022) refuerzan que la IA debe entenderse como un instrumento ambivalente: mientras puede ampliar derechos, como el acceso a la información y la protección de datos, también puede ser utilizada de manera abusiva, resultando en violaciones graves. En este punto, Prado (2021) agrega que el papel del derecho es fundamental para equilibrar innovación y control, garantizando que el desarrollo

tecnológico se realice en consonancia con la dignidad humana y los derechos fundamentales.

Las víctimas de deepfakes pornográficos son mayoritariamente mujeres jóvenes, con edades entre 18 y 35 años, hecho que refleja no solo la hipersexualización femenina, sino también la desigualdad de género en la sociedad digital. Según Prado (2021), “las víctimas son casi siempre mujeres, víctimas de una objetificación que se perpetúa a través de las tecnologías digitales” (p. 45).

La juventud aparece como un factor de riesgo central, ya que los jóvenes son generalmente más activos en las redes sociales, compartiendo imágenes y videos que pueden ser utilizados indebidamente. De acuerdo con Maíllo (2021), “la exposición constante en las redes sociales crea un ambiente propicio para la recolección de imágenes con fines de manipulación digital” (p. 78).

Además, la mayoría de las víctimas posee un alto nivel educativo, con formación universitaria o en proceso de formación. Este dato parece paradójico, pero refleja un grupo que, al ser más activo en el ámbito digital, termina más expuesto. Como destaca Aller (2021), “la educación formal no protege necesariamente contra la victimización digital, ya que el comportamiento en línea sigue siendo el principal factor de riesgo” (p. 62).

Otro factor relevante es la profesión de las víctimas. Muchas son influenciadoras digitales, actrices, periodistas o académicas —perfiles con alta visibilidad y, por lo tanto, objetivos preferenciales. Según Silva y Santos (2022), “el público objetivo tiende a ser mujeres de relevancia pública, lo que intensifica el impacto social y psicológico del delito” (p. 91).

También se observa que el color de la piel y la clase social no son barreras para el delito, aunque hay mayor incidencia de casos que involucran mujeres blancas de clase media y alta. Según Gomes (2023), “la mayor representación de mujeres blancas entre las víctimas puede estar relacionada con la disponibilidad de datos gráficos accesibles en internet” (p. 105).

Por otro lado, las mujeres negras enfrentan una doble vulnerabilidad: además de ser víctimas de deepfakes, son más frecuentemente objeto de representaciones pornográficas con sesgo racista. Como relata Costa (2023), “los deepfakes con mujeres negras frecuentemente explotan estereotipos hipersexualizados históricamente impuestos a esta población” (p. 122).

La vulnerabilidad de las víctimas también está relacionada con la escasa protección legal y la dificultad para denunciar. Muchas mujeres reportan miedo a la exposición, vergüenza y revictimización. Según Prado (2021), “existe una sensación de impotencia generalizada entre las víctimas, que se sienten desprotegidas ante la lentitud del sistema judicial” (p. 48).

Otro grupo vulnerable son las personas trans y no binarias, quienes se encuentran entre las víctimas más invisibilizadas en los informes oficiales. Como apunta Maia (2022), “existe un borrado deliberado de las identidades trans en los registros, lo que contribuye a la perpetuación de la violencia” (p. 59).

La nacionalidad y el contexto cultural también influyen en la exposición al riesgo. En países con legislación más laxa o inexistente sobre delitos digitales, como Brasil hasta hace poco, el número de casos tiende a ser mayor. Según Marques (2022), “la falta de tipificación penal adecuada permite que el delito de deepfake pornográfico permanezca impune” (p. 66).

Dentro del contexto brasileño, se observa que la mayoría de las víctimas reside en áreas urbanas, donde el acceso a la tecnología e internet es más intenso. Según el IBGE (2023), “las mujeres urbanas son quienes más utilizan redes sociales y, por lo tanto, más susceptibles al robo y manipulación de imágenes” (p. 134).

Otro aspecto importante es la ausencia de protocolos eficaces para protección y denuncia en las plataformas digitales. Como afirma Lima (2023), “las grandes empresas de tecnología aún no han implementado mecanismos efectivos para la identificación y eliminación de deepfakes pornográficos” (p. 118).

Las víctimas frecuentemente enfrentan consecuencias psicológicas severas, como depresión, ansiedad y tendencias suicidas. Como apunta Aller (2021), “el impacto emocional de la exposición no consentida puede ser devastador y duradero” (p. 64).

La culpabilización de las víctimas también contribuye a su invisibilidad y silenciamiento. Muchas son acusadas de “permitir” que sus imágenes fueran utilizadas, lo que refuerza la cultura de la violación digital. Según Silva y Santos (2022), “existe una perversión en la asignación de responsabilidad, que traslada la culpa a quien fue violada” (p. 93).

La impunidad alimenta la reincidencia de los perpetradores, quienes se aprovechan de la ineficacia de las investigaciones. Como observa Prado (2021), “los

autores de deepfakes rara vez enfrentan consecuencias legales, lo que crea un ambiente de permisividad" (p. 50).

Aunque existen proyectos de ley en trámite en Brasil para criminalizar específicamente los deepfakes, aún hay vacíos en la tipificación penal. Según Maia (2022), "la ausencia de un marco legal claro dificulta la responsabilización y reparación de las víctimas" (p. 61).

En Brasil, el ordenamiento jurídico presenta normas relevantes que tocan la cuestión de los deepfakes, aunque aún no existe una ley específica que los criminalice de forma directa. La Ley nº 13.709/2018 —Ley General de Protección de Datos (LGPD)— regula el tratamiento de datos personales, estableciendo reglas para la recolección, uso y almacenamiento, aplicables a casos de manipulación digital. Asimismo, la Ley nº 14.132/2021, que tipifica el delito de acoso (stalking), puede utilizarse cuando la producción y difusión de deepfakes genere persecución y daños psicológicos a las víctimas. No obstante, estas legislaciones no abarcan de manera explícita la manipulación de imágenes y videos falsificados mediante IA.

El Proyecto de Ley nº 4.391/2021, en trámite en el Congreso Nacional, busca incluir los deepfakes en la legislación penal brasileña. Propone modificaciones al Código Penal para tipificar como delito la producción, difusión o almacenamiento de contenido manipulado por inteligencia artificial con el objetivo de difamar, calumniar o violar la dignidad de las personas. Aunque representa un avance, aún no ha sido aprobado, manteniendo un vacío legislativo. Como observa Maia (2022), "la ausencia de un marco legal claro dificulta la responsabilización y reparación de las víctimas" (p. 61).

A nivel internacional, Uruguay posee dispositivos más avanzados para enfrentar la violencia digital. La Ley nº 19.580/2017, que aborda la violencia de género contra las mujeres, incluye la violencia simbólica y digital, permitiendo encuadrar prácticas como la difusión de deepfakes pornográficos no consentidos. Además, la Ley nº 18.331/2008, sobre protección de datos personales, proporciona bases jurídicas para impugnar el uso indebido de información digital y solicitar reparación. Estos instrumentos, aunque no mencionen específicamente los deepfakes, amplían las posibilidades de responsabilización, mostrando un escenario más protector en comparación con Brasil.

Por lo tanto, es fundamental reconocer que las características demográficas de las víctimas no determinan su responsabilidad, sino que evidencian fallas sistémicas

en su protección. La responsabilidad debe recaer sobre los autores y sobre los sistemas que permiten la continuidad de la violencia.

En conclusión, las víctimas de deepfakes pornográficos son mayoritariamente mujeres jóvenes, blancas, instruidas y con exposición pública. Su vulnerabilidad está directamente relacionada con la desigualdad de género, la falta de legislación eficaz y el comportamiento permisivo de las plataformas digitales. Solo con medidas integradas de educación, legislación y responsabilización será posible reducir este tipo de delitos.

2.2 LA CRIMINOLOGÍA Y LAS VÍCTIMAS DE DEEPFAKES: PREDOMINANCIA DE MUJERES JÓVENES, CON ÉNFASIS EN FACTORES DE VULNERABILIDAD SOCIAL

Las consecuencias de la victimización por deepfakes pornográficos van más allá del daño a la imagen y la reputación, afectando profundamente el bienestar psicológico de las personas involucradas. El impacto emocional generado por esta forma de violencia es intenso, duradero y frecuentemente ignorado por las instituciones. Como relata Aller (2021), “las víctimas sufren traumas equivalentes a los de las violencias sexuales presenciales, aun cuando el contacto físico no ocurre” (p. 71).

La ansiedad generalizada es una de las reacciones más comunes tras la divulgación de deepfakes. Las víctimas reportan miedo constante a la exposición, vigilancia excesiva de su imagen en línea y sensación de inseguridad permanente. Para Prado (2021), “la ansiedad se deriva del sentimiento de pérdida de control sobre el propio cuerpo e identidad” (p. 53), lo que agrava los síntomas de angustia y estrés.

Además de la ansiedad, muchas víctimas desarrollan cuadros de depresión profunda, resultado de la vergüenza, la revictimización y la soledad que acompañan el proceso de exposición pública. Maíllo (2021) destaca que “la depresión entre víctimas de deepfakes se ve agravada por el juicio social y la lentitud judicial” (p. 82), impidiendo la recuperación emocional adecuada.

Otro efecto recurrente es la ideación suicida, que se manifiesta como respuesta al sentimiento de impotencia frente a la exposición y la ausencia de apoyo institucional. Como observa Maia (2022), “las víctimas frecuentemente consideran el suicidio como

única salida ante el intenso sufrimiento psíquico" (p. 67), lo que exige atención prioritaria de los servicios de salud mental.

En el ámbito social, se produce una ruptura de los lazos afectivos y comunitarios. Muchas víctimas pierden el apoyo de familiares, amigos o parejas, que, en lugar de ofrecer soporte, juzgan o se alejan. Según Silva y Santos (2022), "la soledad impuesta por el estigma agrava el sufrimiento psicológico y aumenta el riesgo de enfermedad mental" (p. 96), ampliando el aislamiento social.

El juicio moral de la sociedad sobre las víctimas es un factor de revictimización. La culpabilización, muchas veces basada en comportamientos considerados "inadecuados" en las redes, recae sobre quien tuvo su imagen manipulada, no sobre los autores del delito. Como afirma Costa (2023), "la cultura del juicio transfiere la responsabilidad a la víctima y legitima la violencia" (p. 129).

El miedo a no ser tomada en serio por las autoridades también impide que muchas víctimas denuncien el delito. En los relatos de mujeres afectadas, existe una constante minimización de lo ocurrido por parte de policías y jueces. Según Marques (2022), "las víctimas sienten que deben probar su inocencia, aun frente a evidencias claras de manipulación digital" (p. 70).

El impacto en las relaciones profesionales también es devastador. Muchas mujeres pierden sus empleos o sufren represalias debido al contenido falso, aunque se trate de deepfakes. De acuerdo con Lima (2023), "la reputación digital de las víctimas frecuentemente se confunde con su conducta real, generando perjuicios irreversibles a la carrera" (p. 121).

Las víctimas también enfrentan humillación pública constante, ya que los videos manipulados se difunden ampliamente en sitios pornográficos y redes sociales. Esta exposición continua prolonga el sufrimiento psicológico y dificulta la rehabilitación de la imagen personal. Para Gomes (2023), "la permanencia del contenido en línea perpetúa el trauma y la sensación de impotencia" (p. 107).

La recuperación emocional se ve dificultada por la ausencia de políticas públicas orientadas a la salud mental de las víctimas de delitos digitales. No existen programas específicos que ofrezcan acompañamiento psicológico, obligando a muchas mujeres a buscar ayuda por cuenta propia, generalmente sin recursos financieros. Según IBGE (2023), "solo el 18% de las víctimas logra acceso continuo a soporte psicológico tras el delito" (p. 137).

Las redes de apoyo entre víctimas han demostrado ser un factor importante en la superación del trauma. Grupos virtuales y colectivos feministas han sido fundamentales para el acompañamiento y el intercambio de experiencias. Como relata Costa (2023), “la solidaridad entre mujeres ha sido uno de los pocos refugios seguros frente a la negligencia institucional” (p. 133).

La experiencia con el delito también genera efectos duraderos en la autoestima y la autoimagen. Muchas víctimas reportan vergüenza de su propio cuerpo y dificultad para verse como sujetos de deseo fuera del contexto violento. Prado (2021) afirma que “el cuerpo pasa a ser visto como un campo de batalla, no como un espacio de autonomía” (p. 56), lo que impacta directamente en las relaciones íntimas.

El trauma sexual simbólico generado por los deepfakes incluso interfiere en la vida sexual de las víctimas. Muchas desarrollan aversión al contacto o a la intimidad, asociando el placer al dolor y al juicio. Según Maia (2022), “la vida sexual de las víctimas se desestructura por la experiencia de violación, incluso si es digital” (p. 70).

Existen también implicaciones pedagógicas y educativas, especialmente en víctimas que son estudiantes. El miedo a la exposición lleva al abandono escolar o al aislamiento en entornos educativos. Según Silva y Santos (2022), “muchas jóvenes abandonan la universidad tras sufrir deepfakes, debido al acoso institucionalizado” (p. 98).

Las plataformas digitales contribuyen a mantener el sufrimiento al no eliminar prontamente los contenidos falsificados. La ausencia de una respuesta rápida prolonga la exposición, dificultando aún más la recuperación. Según Lima (2023), “la demora de las plataformas en actuar contribuye directamente al agravamiento del estado emocional de las víctimas” (p. 123).

En el ámbito jurídico, la lentitud de los procesos constituye otra forma de violencia. Muchas víctimas esperan años por una respuesta del sistema judicial, lo que impide el cierre del ciclo traumático. Según Maíllo (2021), “la justicia tardía es otra capa de dolor para quien ya ha sido violentada” (p. 85).

La criminalización de la pornografía deepfake aún encuentra resistencia en diversos sectores, dejando a las víctimas en una zona gris legal. La falta de claridad jurídica contribuye a la sensación de impunidad y abandono. Como relata Marques (2022), “sin una legislación firme, las víctimas continúan sin el mínimo de protección” (p. 72).

Es urgente que la sociedad, el Estado y las plataformas asuman la responsabilidad de la protección emocional y social de las víctimas de deepfakes pornográficos. Esto implica no solo sancionar a los autores, sino garantizar soporte psicológico, jurídico y social para las personas afectadas. Sin esta red de apoyo, la violencia se perpetúa y se intensifica tanto en el entorno digital como fuera de él.

2.2.1 LOS IMPACTOS EMOCIONALES SUFRIDOS

El avance tecnológico, aunque ha proporcionado innumerables beneficios sociales, también ha traído consigo nuevas formas de violencia que afectan profundamente la vida emocional de las víctimas. En el caso del uso de deepfakes pornográficas no consentidas, tanto en Brasil como en Uruguay, se observa una grave violación de la dignidad humana. “Las víctimas relatan ansiedad intensa y sentimiento de vulnerabilidad extrema” (SILVA, 2024, p. 45), revelando que la primera reacción es la ruptura de la sensación de seguridad.

Este impacto inicial desencadena un segundo efecto: la vergüenza. La exposición pública de imágenes íntimas manipuladas coloca a la víctima en un estado de humillación continua. “La vergüenza se centra en la percepción de exposición pública y juicio social” (GONZÁLEZ, 2023, p. 78). En Brasil, esta vergüenza se amplifica por la rapidez de la circulación digital, mientras que en Uruguay se intensifica debido a la proximidad social en comunidades más pequeñas, reforzando el dolor emocional.

La vergüenza, a su vez, repercute directamente en la autoestima. La víctima internaliza la idea de haber perdido el control sobre su propia imagen e identidad. “Las víctimas sienten que su valor personal se reduce a meros objetos de voyeurismo” (SANTOS, 2022, p. 112). Este proceso conduce a un sentimiento de desvalorización que, en muchos casos, da lugar a cuadros de depresión.

Al mismo tiempo, se instala un miedo persistente. La incertidumbre sobre la reaparición del material manipulado en plataformas digitales profundiza la sensación de inseguridad. Como afirma Pérez (2024), “el miedo a que las imágenes vuelvan a circular en cualquier momento causa estrés crónico” (p. 30). De este modo, la ansiedad se perpetúa, manteniendo a las víctimas en un estado de alerta constante.

El miedo se asocia además con el sentimiento de impotencia frente al delito. La imposibilidad de controlar la circulación del contenido genera frustración y

desorientación. “Muchos relatan sensación de impotencia por no tener control sobre sus propias imágenes” (RODRIGUEZ, 2023, p. 55). Esta impotencia suele derivar en aislamiento social, afectando no solo la vida individual, sino también la dinámica familiar.

Dicho aislamiento se ve agravado por las reacciones de personas cercanas, que no siempre brindan apoyo adecuado. En algunos casos, parejas y familiares reproducen el juicio social, profundizando el sufrimiento de la víctima. “La reacción negativa de personas cercanas refuerza la sensación de abandono emocional” (ALMEIDA, 2022, p. 90). Así, la ausencia de una red de apoyo sólida incrementa la vulnerabilidad emocional.

Este cuadro de abandono y aislamiento tiene impactos directos en la salud mental. Estudios recientes muestran que las víctimas de este tipo de abuso presentan niveles elevados de ansiedad y depresión. “Más del 60 % de las víctimas presentan síntomas clínicos de depresión tras la exposición a deepfakes” (FERNANDEZ, 2024, p. 105). Cuando no se tratan, estas condiciones pueden evolucionar hacia enfermedades graves, incluida la ideación suicida.

Además de la depresión, surge el sentimiento de culpa, incluso sin fundamento. Muchas víctimas se responsabilizan de manera irracional por lo ocurrido, internalizando la violencia sufrida. “La culpa irracional se presenta incluso cuando hay total ausencia de responsabilidad personal” (CASTRO, 2023, p. 66). Esta percepción es una de las barreras más difíciles de superar, ya que mantiene a la víctima atrapada en un ciclo de auto-penalización.

Este ciclo se intensifica con el llamado trauma digital, concepto que describe la imposibilidad de borrar definitivamente la experiencia en línea. “El trauma digital consiste en la dificultad para recuperar la privacidad en entornos online” (LIMA, 2024, p. 23). La permanencia virtual del contenido manipulado prolonga el dolor, haciendo que la recuperación emocional sea un proceso aún más desafiante.

Frente a esto, la búsqueda de apoyo psicológico especializado se muestra indispensable. La superación no puede limitarse a enfoques tradicionales, siendo necesaria una escucha centrada en la reconstrucción de la confianza. “Las víctimas necesitan enfoques terapéuticos centrados en la reconstrucción de la confianza” (MENDES, 2022, p. 38). Este apoyo, sin embargo, sigue siendo desigual entre Brasil y Uruguay, restringiéndose a grandes centros urbanos.

Mientras buscan soporte psicológico, muchas víctimas enfrentan además la batalla judicial. La lentitud del sistema de justicia prolonga el sufrimiento y genera revictimización. “La demora en la respuesta judicial amplía el sentimiento de desamparo y revictimización” (MARTINEZ, 2023, p. 77). La morosidad procesal convierte lo que debería ser reparación en una fuente adicional de desgaste emocional.

En este contexto, las campañas de concientización se vuelven fundamentales. Cuando se conducen adecuadamente, estas iniciativas reducen el estigma e incentivan la empatía social. “Las campañas de concientización tienen potencial para humanizar a las víctimas y reducir el estigma” (OLIVEIRA, 2024, p. 50). Sin embargo, si están mal estructuradas, pueden reforzar prejuicios y culpar aún más a las víctimas.

Las redes sociales, sin embargo, permanecen como el espacio donde los impactos emocionales se intensifican. Comentarios ofensivos y compartidos sucesivos revictimizan a la persona expuesta. “La exposición continua en las redes sociales impide el fin del dolor emocional” (RAMOS, 2023, p. 120). Así, el entorno que podría servir para apoyo y denuncia se transforma en un campo de prolongación de la violencia.

Esta prolongación se vuelve aún más cruel para víctimas que viven en regiones periféricas o alejadas de los centros urbanos. En estas localidades, el acceso a apoyo psicológico, jurídico y social es limitado, aumentando la sensación de abandono. “El aislamiento cultural amplía la sensación de no pertenencia y abandono” (VÁZQUEZ, 2022, p. 88). La desigualdad territorial, por tanto, agrava los impactos emocionales del abuso.

Así, los impactos emocionales de los deepfakes pornográficos no consentidos son múltiples e interrelacionados, desde la ansiedad y vergüenza hasta el aislamiento social, la depresión y el trauma digital. En Brasil y Uruguay, enfrentar este fenómeno requiere estrategias integradas que combinen apoyo psicológico, respuestas judiciales rápidas y políticas de concientización. Solo mediante este enfoque multidimensional será posible rescatar la dignidad y ofrecer a las víctimas condiciones para reconstruir su vida emocional

2.2.2 RASTROS PSICOLÓGICOS Y SOCIOLÓGICOS DE LA REVICTIMIZACIÓN

El avance de las tecnologías de manipulación de imágenes y videos ha permitido la proliferación de deepfakes pornográficos, cuyos autores presentan

perfiles cada vez más específicos y complejos. La comprensión criminológica de estos perpetradores es fundamental para la creación de políticas públicas eficaces y estrategias de prevención. Diversos documentos oficiales señalan patrones de comportamiento y motivaciones recurrentes en quienes cometen estos delitos digitales.

En primer lugar, se destaca el perfil masculino de los perpetradores. La mayoría de los delitos relacionados con deepfakes pornográficos son cometidos por hombres, generalmente entre los 18 y 40 años. Según el Informe de Europol sobre Criminalidad Cibernética (2023), “los perpetradores son predominantemente de sexo masculino, con conocimientos técnicos medianos o avanzados” (p. 19), reforzando la desigualdad de género en el uso de la tecnología con fines delictivos.

Además, muchos de los autores de estos delitos tienen formación en áreas de tecnología de la información, ingeniería o son autodidactas con amplia experiencia en entornos digitales. El Manual de Capacitación del Ministerio de Justicia de Brasil sobre Delitos Cibernéticos (MJSP, 2022) afirma que “los autores demuestran dominio técnico, utilizando softwares accesibles en foros de internet y redes anónimas” (p. 32), lo que amplía la diseminación de este tipo de materiales.

El anonimato en Internet es una motivación central para la comisión de estos delitos, ya que permite al infractor actuar con una falsa sensación de impunidad. Según la Guía de Seguridad Digital de SaferNet Brasil (2023), “la ocultación de la identidad real en la red facilita la práctica de delitos de odio y violencia sexual, como en el caso de los deepfakes” (p. 41), lo que revela la importancia de regular el uso de tecnologías anónimas.

Entre los principales motivadores se encuentran la venganza, el deseo de control y dominación y, en muchos casos, la obtención de lucro mediante la comercialización de los videos falsificados. El Informe de la Oficina de las Naciones Unidas sobre Drogas y Crimen (UNODC, 2022) destaca que “el objetivo puede variar entre entretenimiento, humillación pública y ganancias financieras, especialmente cuando los videos se venden en plataformas ilegales” (p. 64).

La pornografía de venganza, que motiva muchos de estos ataques, es frecuentemente consecuencia de relaciones interpersonales rotas. El Informe del Consejo Nacional de Justicia (CNJ, 2023) señala que “ex-parejas son responsables de gran parte de las denuncias que implican manipulación de imágenes íntimas para

avergonzar a las víctimas” (p. 52), revelando un patrón de violencia basado en género y poder.

La misoginia digital es una característica notable entre los agresores. La violencia simbólica contra las mujeres en internet se ve reforzada por el uso de deepfakes como mecanismo de humillación. Según el Informe Anual de la Comisión de Derechos Humanos del Senado Federal (2022), “hay evidencia de que los autores de estos delitos operan desde una cultura de odio de género que se reproduce en comunidades online” (p. 37).

La misoginia puede entenderse como un fenómeno estructural que atraviesa las relaciones sociales y jurídicas, reflejándose en prácticas de violencia contra las mujeres tanto en el espacio físico como digital. Para Silva y Santos (2022, p. 91), la misoginia, mediada por la tecnología, se intensifica mediante conductas como la producción y circulación de deepfakes no consensuados, revelando “la vulnerabilidad de las mujeres frente a un mercado digital que explota la intimidad como mercancía”. Esto evidencia que la misoginia no se limita a manifestaciones culturales, sino que constituye también una forma de violencia que requiere respuestas legales.

En este sentido, Prado (2021, p. 47) observa que el derecho penal brasileño aún enfrenta desafíos para acompañar las nuevas modalidades de delitos de odio y de género, destacando que “la legislación necesita evolucionar para dar cuenta de las transformaciones introducidas por las tecnologías digitales, especialmente en lo que respecta a las ofensas sistemáticas dirigidas a las mujeres”. El análisis del autor refuerza que la misoginia digital se vuelve más compleja, combinando aspectos psicológicos, sociales y tecnológicos, lo que exige un enfoque interdisciplinario.

Como respuesta legislativa, la Ley nº 13.718/2018 representó un avance al criminalizar la divulgación no autorizada de imágenes íntimas, reconociendo jurídicamente la gravedad de la violencia contra las mujeres en entornos digitales. Sin embargo, como argumentan Silva y Santos (2022), estas medidas siguen siendo insuficientes ante la sofisticación de las prácticas de misoginia online, que incluyen desde el acoso sistemático hasta la creación de contenidos manipulados mediante inteligencia artificial. De esta manera, la misoginia debe abordarse como un problema estructural y digital, requiriendo tanto marcos legales más específicos como políticas públicas.

Otro elemento relevante es la inserción de los delincuentes en foros de la deep web, donde intercambian técnicas, scripts y videos manipulados. El Informe de

Monitoreo del NIC.br sobre Seguridad en Internet (2023) señala que “estas comunidades funcionan como verdaderos laboratorios de crimen digital, donde se estimulan el anonimato y la impunidad” (p. 28).

Es importante destacar que muchos perpetradores no reconocen la gravedad de sus actos. El MJSP (2022) explica que “los autores suelen relativizar el impacto de sus acciones, alegando que se trata de ‘una broma’ o ‘libertad de expresión’” (p. 35), evidenciando ausencia de empatía y comprensión de las consecuencias legales y sociales.

El perfil psicológico de estos criminales también muestra rasgos preocupantes. El Manual Técnico de Psicología Forense del CNMP (2022) sugiere que “algunos infractores demuestran rasgos de narcisismo, obsesividad y placer sádico asociados a la exposición y humillación ajena” (p. 58), indicando la presencia de trastornos conductuales en ciertos casos.

Aunque muchos infractores actúan individualmente, existen registros de acciones colectivas organizadas, especialmente en grupos de intercambio masivo. Según el Informe de la Policía Federal sobre Delitos en Internet (2023), “hay una estructuración en redes con división de tareas entre creadores, divulgadores y monetizadores de los contenidos manipulados” (p. 46), revelando la complejidad de las acciones criminales.

Las motivaciones también pueden tener carácter ideológico, como en el caso de grupos extremistas que usan deepfakes para atacar figuras públicas, feministas o activistas. El UNODC (2022) advierte que “la tecnología se instrumentaliza como arma de guerra simbólica, con el objetivo de desacreditar liderazgos y defender agendas discriminatorias” (p. 69).

Los delitos digitales con deepfakes también se utilizan como instrumentos de chantaje. Muchos infractores exigen dinero o favores sexuales a cambio de no divulgar el material. Según la Guía de Enfrentamiento a la Violencia Online del Ministerio de Derechos Humanos (2023), “la extorsión con material íntimo manipulado es una nueva forma de violencia sexual, agravada por la verosimilitud de los videos” (p. 24).

Algunos infractores son adolescentes que, impulsados por curiosidad, desafío o inserción en grupos de pares, se involucran en prácticas delictivas sin pleno entendimiento de la ilegalidad. El CNJ (2023) advierte que “aumenta el número de jóvenes involucrados en la creación y difusión de deepfakes, muchas veces sin discernimiento sobre los daños causados” (p. 55).

La impunidad percibida también es un factor motivacional. Muchos perpetradores consideran que las investigaciones son lentas o inexistentes, lo que los anima a reincidir. El NIC.br (2023) destaca que “la baja tasa de identificación de los autores y la ausencia de responsabilidad efectiva generan un entorno fértil para la repetición de conductas” (p. 31).

El uso de inteligencia artificial accesible contribuye a la popularización de este tipo de delitos. Softwares gratuitos, tutoriales en línea y comunidades de apoyo técnico facilitan la incorporación de nuevos agresores. Según Europol (2023), “la democratización de las herramientas de edición y la ausencia de barreras éticas amplían el espectro de usuarios que se convierten en criminales” (p. 21).

Cabe destacar que la mayoría de los infractores no presenta antecedentes penales, lo que dificulta su detección mediante métodos tradicionales. Según el MJSP (2022), “la ausencia de historial penal y el perfil aparentemente ‘normal’ dificultan el rastreo de estos criminales” (p. 39), reforzando la necesidad de vigilancia digital proactiva.

En síntesis, el perfil criminológico de los perpetradores de deepfakes pornográficos revela individuos técnicamente capacitados, mayoritariamente hombres, motivados por deseos de venganza, dominación, lucro o ideología. La falta de legislación específica, combinada con el anonimato y la facilidad de acceso a la tecnología, favorece la continuidad de estos delitos.

La respuesta institucional debe considerar las motivaciones de los autores y sus particularidades, garantizando la responsabilidad penal y previniendo la reincidencia. Programas de monitoreo, educación digital y endurecimiento de las sanciones son caminos urgentes para contener la creciente ola de violencia simbólica y sexual alimentada por las tecnologías emergentes.

2.2. LEY DEL STALKING (LEY 14.132/2021)

La promulgación de la Ley nº 14.132/2021 representó un hito en el ordenamiento jurídico brasileño, al tipificar el delito de persecución, conocido popularmente como *stalking*. Esta práctica, antes tratada de manera difusa, pasó a contar con una previsión legal específica. Como destaca Gomes (2022), “la ley responde a una demanda social urgente, brindando mayor seguridad a las víctimas de persecución sistemática” (p. 41).

La legislación define el delito de *stalking* como la acción de perseguir a alguien de manera reiterada, por cualquier medio, amenazando su integridad física o psicológica. Esta definición incluye comportamientos digitales, como el envío excesivo de mensajes, y presenciales, como persecuciones físicas. Según Silva (2023), “el carácter reiterado es lo que distingue el *stalking* de meras molestias ocasionales” (p. 77).

Antes de la ley, muchos casos de persecución se trataban como contravenciones penales, resultando en sanciones leves. Con la nueva tipificación, el legislador buscó ampliar la protección: “El cambio legislativo elevó la gravedad de la conducta, reconociéndola como delito y no como mera contravención” (MEDEIROS, 2022, p. 59), fortaleciendo así la red de protección jurídica.

Uno de los puntos centrales de la ley es el reconocimiento de los impactos psicológicos que sufren las víctimas. Las persecuciones constantes generan ansiedad, miedo y restricción de libertad. “El *stalking* no solo daña el cuerpo, sino principalmente la mente de la víctima” (ALVES, 2021, p. 34). Esto evidencia que el legislador consideró el sufrimiento emocional como un componente esencial del delito.

En el ámbito digital, el *stalking* adquiere contornos aún más preocupantes. Las plataformas de redes sociales amplían el alcance de la persecución, haciéndola persistente e invasiva. “El *stalking* virtual permite que la víctima sea vigilada en tiempo completo, incluso en entornos íntimos” (OLIVEIRA, 2023, p. 112), mostrando cómo el fenómeno está estrechamente ligado a las transformaciones tecnológicas recientes.

A pesar de los avances, la aplicación práctica de la ley aún enfrenta desafíos. La dificultad de recopilar pruebas digitales es un obstáculo recurrente. “La recolección de evidencias en delitos de *stalking* digital depende de pericia técnica compleja y no siempre accesible” (PEREIRA, 2022, p. 89), lo que evidencia la necesidad de capacitación continua de las autoridades.

Otro tema de debate es la compatibilidad de la ley con la libertad de expresión. Existen situaciones en que manifestaciones insistentes pueden confundirse con persecución. Como observa Rocha (2023), “el desafío consiste en equilibrar la protección de la víctima sin restringir indebidamente derechos fundamentales” (p. 58). El tema requiere interpretación cuidadosa por parte de los tribunales.

La pena prevista para el delito es de reclusión de 6 meses a 2 años y multa, pudiendo aumentar si existen agravantes, como víctima menor de edad o relación íntima con el agresor. “El aumento de la pena en situaciones de vulnerabilidad refleja

la preocupación del legislador por la protección de grupos específicos" (Martins, 2022, p. 101), mostrando la sensibilidad social de la norma.

Las mujeres, en particular, son las principales víctimas de *stalking*, frecuentemente en contextos de violencia doméstica. "La persecución es una extensión de la violencia de género, sirviendo como mecanismo de control e intimidación" (CARVALHO, 2021, p. 66). En este sentido, la ley dialoga con políticas más amplias de enfrentamiento a la violencia contra la mujer.

La experiencia internacional muestra que legislaciones similares ya estaban consolidadas en otros países. En Uruguay, por ejemplo, la persecución sistemática fue reconocida como forma de violencia psicológica en 2018. "Brasil tardó en acompañar la tendencia mundial, pero la Ley 14.132/2021 corrigió esa laguna" (FERNÁNDEZ, 2022, p. 25), revelando la importancia de la integración regional en la lucha contra el delito.

En la práctica forense, sin embargo, aún hay subregistro. Muchas víctimas no reconocen la persecución como delito o temen represalias. "El miedo a la reacción del agresor hace que diversas víctimas guarden silencio frente al *stalking*" (LIMA, 2023, p. 72), evidenciando la necesidad de ampliar campañas de concienciación.

Además de la concienciación, es fundamental contar con un abordaje multidisciplinario. Psicólogos, asistentes sociales y abogados deben actuar en conjunto para apoyar a las víctimas. "El tratamiento del *stalking* requiere un enfoque integrado, que vaya más allá del ámbito penal" (SOUZA, 2022, p. 119). Así, la ley debe aplicarse en sinergia con políticas de apoyo social.

Un punto innovador es el reconocimiento del *stalking* como práctica que limita la libertad de la víctima. El derecho a ir y venir se ve comprometido por el miedo. "La restricción de la libertad, aunque invisible, es una de las mayores violencias causadas por la persecución" (DIAS, 2021, p. 55), ampliando la comprensión de la gravedad del delito.

A pesar de críticas y limitaciones, la Ley nº 14.132/2021 representa un avance significativo para el ordenamiento jurídico brasileño. Inserta el *stalking* en un nivel de mayor gravedad, equiparándolo con otros delitos que afectan directamente la dignidad humana. "La legislación inauguró un nuevo capítulo en el enfrentamiento a la violencia psicológica" (MOURA, 2023, p. 80).

De este modo, la Ley del *Stalking* fortalece la protección de las víctimas y da visibilidad a un delito que, durante mucho tiempo, fue negligenciado. Sin embargo, su

eficacia depende de la concienciación social, la capacitación de profesionales y la cooperación entre distintas áreas del conocimiento. Solo así será posible consolidar la ley como instrumento efectivo de protección. “El desafío ahora es transformar la previsión legal en una realidad cotidiana” (BARBOSA, 2022, p. 64).

2.2.4 LOS PROGRAMAS DE ACOGIDA, REDES DE APOYO PSICOLÓGICO Y JURÍDICO

Los programas de acogida surgen como instrumentos esenciales en la lucha contra las violencias digitales y presenciales, ofreciendo un soporte integral a las víctimas. Estos programas tienen como objetivo reducir el sufrimiento emocional y orientar jurídicamente. Como resalta Souza (2022), “el tratamiento del stalking exige un enfoque integrado que vaya más allá del ámbito penal” (p. 119). Tal afirmación refuerza la necesidad de articulación entre psicología, derecho y políticas públicas.

La red de apoyo psicológico se ha mostrado fundamental para la reconstrucción de la autoestima de las víctimas. Al ofrecer una escucha cualificada, los profesionales ayudan a reducir los daños emocionales resultantes del delito. “Las víctimas necesitan enfoques terapéuticos centrados en la reconstrucción de la confianza” (MENDES, 2022, p. 38). Así, la psicoterapia especializada actúa como pilar central de los programas de acogida.

Los programas de acogida no se limitan a la asistencia psicológica, sino que también brindan apoyo jurídico, permitiendo que las víctimas comprendan sus derechos y sigan los procesos legales. “La demora en la respuesta judicial amplía el sentimiento de desamparo y revictimización” (MARTINEZ, 2023, p. 77). Por ello, el soporte jurídico inmediato evita que la víctima se sienta abandonada por el sistema.

En este sentido, es importante considerar que la red de acogida debe estar disponible desde el primer contacto con la víctima, asegurando protección contra nuevas violaciones. “El miedo a la reacción del agresor hace que diversas víctimas guarden silencio frente al stalking” (LIMA, 2023, p. 72). La acogida inicial, por tanto, funciona como herramienta para romper el silencio e incentivar denuncias.

Además de la orientación jurídica, los programas deben actuar en el fortalecimiento social de las víctimas. La falta de apoyo comunitario muchas veces agrava la situación. “La reacción negativa de personas cercanas refuerza la sensación de abandono emocional” (ALMEIDA, 2022, p. 90). De esta manera, las redes de

acogida que involucran a familiares y comunidad pueden minimizar el impacto de la estigmatización.

La interdisciplinariedad es un aspecto fundamental. La integración entre psicólogos, trabajadores sociales y abogados permite una respuesta más completa. “El tratamiento del stalking exige un enfoque integrado que vaya más allá del ámbito penal” (SOUZA, 2022, p. 119). Esta articulación garantiza que las víctimas no necesiten buscar ayuda aisladamente, evitando desgaste emocional.

En el ámbito psicológico, la creación de grupos de apoyo ha sido eficaz. Compartir experiencias fortalece la resiliencia de las víctimas. “Más del 60 % de las víctimas presentan síntomas clínicos de depresión tras la exposición a deepfakes” (FERNANDEZ, 2024, p. 105). El apoyo colectivo reduce la sensación de soledad y legitima el sufrimiento, creando vínculos de confianza.

En el campo jurídico, las redes de apoyo desempeñan un papel fundamental en el acompañamiento procesal. Ayudan en la recopilación de pruebas y en la formalización de denuncias. “La recolección de evidencias en delitos de stalking digital depende de pericia técnica compleja y no siempre accesible” (PEREIRA, 2022, p. 89). Este apoyo especializado aumenta las posibilidades de responsabilización del agresor.

La presencia de abogados especializados también contribuye a la aplicación efectiva de la Ley nº 14.132/2021. “La ley responde a una demanda social urgente, proporcionando mayor seguridad a las víctimas de persecución sistemática” (GOMES, 2022, p. 41). De esta manera, los programas de acogida garantizan que la legislación se utilice de manera eficaz, evitando la impunidad.

Otro aspecto esencial es el apoyo a las víctimas en casos de violencia de género, donde el stalking y el abuso de imagen digital están frecuentemente presentes. “La persecución es una prolongación de la violencia de género, sirviendo como mecanismo de control e intimidación” (CARVALHO, 2021, p. 66). La red de acogida, en estos casos, actúa como instrumento de protección de la autonomía femenina.

Las campañas de concientización también forman parte de las redes de apoyo, en la medida en que reducen el estigma social e incentivan denuncias. “Las campañas de concientización tienen el potencial de humanizar a las víctimas y reducir el estigma” (OLIVEIRA, 2024, p. 50). Esta función pedagógica de la red amplía su actuación, no solo en la acogida, sino también en la prevención.

No obstante, el alcance de los programas aún enfrenta desigualdades regionales. En las áreas más remotas, el acceso a la acogida es limitado. “El

aislamiento cultural amplía la sensación de no pertenencia y abandono" (VÁZQUEZ, 2022, p. 88). Esto revela la importancia de políticas públicas que garanticen la universalización de las redes de apoyo.

La cooperación internacional también es relevante. Uruguay, por ejemplo, ya reconocía la persecución sistemática como violencia psicológica antes que Brasil. "Brasil tardó en seguir la tendencia mundial, pero la Ley 14.132/2021 corrigió esa laguna" (FERNÁNDEZ, 2022, p. 25). En este sentido, el intercambio de experiencias puede fortalecer los programas de acogida regionales.

A pesar de los desafíos, los programas de acogida han contribuido significativamente a la reducción de los impactos emocionales. "Ansiedad intensa y sentimiento de vulnerabilidad extrema" (SILVA, 2024, p. 45) son sentimientos reportados que encuentran alivio en los espacios de apoyo. Así, estas iniciativas desempeñan un papel crucial en la reconstrucción de la dignidad de las víctimas.

En conclusión, los programas de acogida y las redes de apoyo psicológico y jurídico se configuran como instrumentos indispensables en la lucha contra la violencia digital y el stalking. Ofrecen soporte emocional, orientación legal y fortalecimiento social. "El desafío ahora es transformar la previsión legal en realidad cotidiana" (BARBOSA, 2022, p. 64). Para ello, es necesario aumentar la inversión, capacitar profesionales y consolidar una cultura de acogida y empatía.

2.2.5 LA CREACIÓN DE CANALES DE DENUNCIA

La creación de canales de denuncia representa uno de los pilares fundamentales en el enfrentamiento de la violencia digital, especialmente en el caso de las deepfakes pornográficas no consentidas. Según Oliveira (2023, p. 141), "la existencia de medios accesibles y seguros de denuncia aumenta la confianza de las víctimas en la posibilidad de responsabilización de los agresores". Esta confianza es esencial para estimular que mujeres y hombres afectados busquen protección y justicia.

En Brasil, diversas iniciativas han buscado ampliar los mecanismos de denuncia, como el Disque 100 y el Ligue 180, adaptados también para casos de violencia en línea. Souza y Pereira (2022, p. 87) destacan que "la disponibilidad de canales específicos para denuncias digitales contribuye a reducir la subnotificación de

los delitos, permitiendo una mayor visibilidad del fenómeno". Esto refuerza la necesidad de actualización constante de estas estructuras.

No obstante, crear canales por sí solo no garantiza eficacia sin inversión en difusión. Como resalta Costa (2024, p. 210), "muchas víctimas desconocen los canales de denuncia disponibles, lo que dificulta la movilización social y la protección efectiva". Por ello, las campañas públicas son indispensables para que estos instrumentos sean realmente accesibles.

En Uruguay, se han implementado experiencias similares con enfoque en la lucha contra la violencia digital. Fernández (2023, p. 95) señala que "la creación de líneas de denuncia especializadas en delitos digitales ha generado avances importantes en la confianza de las víctimas en el sistema de justicia". Este ejemplo internacional sirve de referencia para que Brasil mejore su propia estructura.

La denuncia también debe ser recibida con sensibilidad. Para Santos (2022, p. 132), "no basta con abrir canales de comunicación; es necesario garantizar que la víctima sea tratada con respeto y tenga un acompañamiento adecuado". Esto significa que los canales no deben ser meramente burocráticos, sino espacios de escucha activa.

Además, la integración entre los canales de denuncia y los programas de acogida psicológica y jurídica es esencial. Según Oliveira (2023, p. 147), "el vínculo entre denuncia y acogida permite que la víctima se sienta protegida y amparada desde el primer contacto con las autoridades". Este modelo integrado fortalece la confianza en el proceso de denuncia.

Otro aspecto relevante es la anonimización. De acuerdo con Souza y Pereira (2022, p. 94), "la posibilidad de realizar denuncias anónimas anima a víctimas y testigos a reportar casos, disminuyendo el miedo a represalias". Esta medida es fundamental en la lucha contra las deepfakes, donde la exposición de la identidad ya forma parte de la violencia sufrida.

No obstante, aún persisten desafíos respecto a la respuesta del sistema tras la denuncia. Costa (2024, p. 215) advierte que "cuando no hay retorno ni medidas concretas tras la denuncia, se crea un ciclo de desconfianza que desincentiva nuevas notificaciones". Por ello, es esencial garantizar agilidad y efectividad en el procesamiento de los casos.

Las plataformas digitales también tienen responsabilidad en este proceso. Fernández (2023, p. 102) enfatiza que "la creación de botones de denuncia dentro de

las propias redes sociales y sitios pornográficos es un paso relevante, pero aún insuficiente sin mecanismos rápidos de retiro del contenido". Esto muestra que la cooperación internacional es imprescindible.

Desde esta perspectiva, se observa que el fortalecimiento de los canales de denuncia debe ir de la mano con políticas públicas de protección. Para Santos (2022, p. 138), "el Estado necesita asumir un papel protagónico, ofreciendo canales que no solo reciban denuncias, sino que también aseguren medidas protectoras inmediatas". Así se evita que la víctima continúe expuesta.

Otro punto a destacar es la necesidad de accesibilidad digital. Oliveira (2023, p. 153) señala que "sin plataformas accesibles para personas con discapacidad, el derecho a denunciar se vuelve desigual". Por lo tanto, la inclusión debe ser un principio central en la creación de cualquier mecanismo de comunicación oficial.

Asimismo, la cooperación con organizaciones de la sociedad civil fortalece los canales existentes. Souza y Pereira (2022, p. 98) afirman que "las ONG no solo ofrecen canales paralelos de denuncia, sino también apoyo psicosocial inmediato, convirtiéndose en aliadas estratégicas del Estado". Esta colaboración amplía la cobertura de las acciones de enfrentamiento.

En el contexto de las deepfakes, la urgencia de la denuncia es aún más evidente. Costa (2024, p. 223) subraya que "cuanto más rápido se denuncie el contenido, mayor es la posibilidad de removerlo antes de que se difunda masivamente". Esto refuerza la necesidad de canales ágiles y monitoreados permanentemente.

En Uruguay, los canales digitales se han fortalecido mediante legislaciones específicas. Fernández (2023, p. 110) destaca que "la legislación uruguaya prevé la creación de sistemas de denuncia integrados al Ministerio del Interior, con respuestas rápidas y protocolos claros". Esta práctica puede servir de inspiración para Brasil.

De este modo, la creación de canales de denuncia eficaces debe considerarse no solo como una herramienta burocrática, sino como una política pública esencial en el enfrentamiento de las deepfakes pornográficas no consentidas. Según Santos (2022, p. 144), "la denuncia es el primer paso para romper el silencio y permitir que la víctima inicie su proceso de reparación". Por lo tanto, la efectividad de estos canales puede determinar el éxito o fracaso de las políticas de combate a este tipo de violencia.

2.3 LA CRIMINOLOGÍA Y LOS AGRESORES: PERFIL CRIMINOLÓGICO Y MOTIVACIONES PARA LA CONDUCTA DELICTIVA

El análisis criminológico de los agresores de *deepfakes* pornográficas y *stalking* permite comprender los factores que motivan la conducta delictiva. Souza y Pereira (2022, p. 92) afirman que “entender el perfil psicológico del agresor es esencial para el desarrollo de políticas preventivas eficaces”. Tal enfoque ayuda en la construcción de estrategias integradas de prevención e intervención.

Generalmente, los agresores presentan características de búsqueda de control y poder sobre la víctima, siendo común la presencia de conductas obsesivas. Oliveira (2023, p. 145) observa que “el agresor digital frecuentemente actúa con el propósito de dominación y humillación, reflejando necesidades de afirmación personal”. Esta motivación está estrechamente ligada al contexto social y psicológico del infractor.

En muchos casos, la impunidad percibida alimenta la repetición del comportamiento delictivo. Costa (2024, p. 218) destaca que “cuando el agresor cree que no habrá consecuencias legales, la conducta tiende a intensificarse, ampliando los daños a la víctima”. Así, la percepción del riesgo legal actúa como factor modulador del comportamiento criminal.

La criminología señala también que el anonimato proporcionado por internet facilita la práctica de los delitos digitales. Fernandez (2023, p. 99) afirma que “la sensación de invisibilidad digital alienta a los individuos a perpetrar delitos sin considerar responsabilidades sociales o legales”. El anonimato crea un ambiente propicio para conductas depredadoras y repetitivas.

Otro factor es la normalización cultural de prácticas abusivas. Santos (2022, p. 136) resalta que “en contextos donde la cosificación y la sexualización de la imagen ajena son comunes, el agresor se siente legitimado para actuar sin restricciones”. Esta percepción social contribuye al mantenimiento de conductas delictivas en línea.

El perfil criminológico también evidencia que muchos agresores presentan rasgos de impulsividad y dificultades de empatía. Gomes (2022, p. 44) señala que “la incapacidad de comprender el sufrimiento de la víctima caracteriza al agresor digital e influye directamente en la persistencia del delito”. El aspecto psicológico, por lo tanto, es determinante en la conducta criminal.

La literatura destaca además la presencia de motivaciones de venganza o resentimiento personal. Silva (2024, p. 48) observa que “una parte significativa de los

agresores actúa motivada por resentimientos o conflictos personales, transformando disputas privadas en violencia pública digital". Esta motivación demuestra que el delito puede tener raíces en relaciones interpersonales previas.

La búsqueda de estatus y reconocimiento en grupos virtuales también influye en el comportamiento. Oliveira (2023, p. 148) relata que "algunos infractores comparten imágenes o informaciones con el objetivo de ganar notoriedad dentro de redes sociales, reforzando su poder simbólico". Esta motivación evidencia la dimensión social del delito digital.

Otro elemento relevante es el impacto de la educación y la socialización familiar. Souza y Pereira (2022, p. 95) afirman que "los individuos con antecedentes de negligencia familiar o poca educación emocional tienen mayor probabilidad de reproducir conductas abusivas en línea". Esta constatación refuerza la necesidad de prevención desde la infancia.

La criminología también sugiere que la tecnología actúa como amplificador de las conductas delictivas. Costa (2024, p. 221) destaca que "las herramientas digitales permiten multiplicar y acelerar la difusión de contenido abusivo, aumentando el alcance y el impacto de la agresión". Así, el perfil del agresor está estrechamente vinculado al uso estratégico de recursos tecnológicos.

La relación entre el delito de *stalking* y las *deepfakes* muestra que el agresor frecuentemente combina conductas obsesivas con explotación digital. Fernandez (2023, p. 104) observa que "la confluencia de *stalking* y manipulación digital evidencia una estrategia planificada de intimidación y control". Esta constatación refuerza la complejidad criminológica del fenómeno.

En el contexto de género, se verifica predominancia de agresores hombres, aunque no exclusiva. Santos (2022, p. 139) afirma que "los análisis indican mayor incidencia masculina en delitos de persecución y abuso de imagen, aunque los casos femeninos no son inexistentes". Esta información es importante para la orientación de políticas de prevención.

La criminología contemporánea enfatiza que la comprensión de las motivaciones permite delinear estrategias de reeducación y responsabilización del agresor. Gomes (2022, p. 46) subraya que "los programas de intervención deben considerar factores psicológicos, sociales y tecnológicos para reducir la reincidencia". Así, el enfoque preventivo se muestra complementario al represivo.

Otro punto es que el estudio del perfil criminológico ayuda en la creación de políticas públicas más eficaces. Silva (2024, p. 50) destaca que “el conocimiento de las características del agresor orienta medidas preventivas, desde campañas educativas hasta el perfeccionamiento de la legislación”. Esta articulación evidencia la importancia de la criminología aplicada.

Comprender el perfil criminológico y las motivaciones de los agresores es fundamental para la prevención y el enfrentamiento del *stalking* y de las *deepfakes* pornográficas no consentidas. Oliveira (2023, p. 151) concluye que “el análisis criminológico proporciona insumos para políticas integradas, capaces de proteger a las víctimas y reducir la ocurrencia de nuevos delitos”. De esta forma, la criminología actúa como herramienta estratégica en la construcción de respuestas efectivas.

2.4 LA RELACIÓN ENTRE VÍCTIMAS Y AGRESORES

La relación entre víctimas y agresores de *deepfakes* pornográficas y *stalking* presenta dinámicas complejas, frecuentemente marcadas por desequilibrio de poder. Souza y Pereira (2022, p. 93) destacan que “la relación entre víctima y agresor es muchas veces caracterizada por control, intimidación y violación de la autonomía personal”. Este desequilibrio es uno de los principales factores que intensifican el sufrimiento emocional.

En casos de *stalking*, el agresor suele ser alguien cercano a la víctima, como exparejas o conocidos, lo que agrava la sensación de traición y vulnerabilidad. Oliveira (2023, p. 146) observa que “la proximidad emocional o social entre víctima y agresor aumenta el impacto psicológico, dificultando la ruptura del ciclo de violencia”. Esto demuestra la necesidad de políticas que contemplen los vínculos interpersonales.

Incluso en situaciones digitales, la relación puede ser directa o indirecta. Costa (2024, p. 220) señala que “muchos agresores utilizan informaciones obtenidas de redes sociales y entornos virtuales para perseguir o chantajear a las víctimas”. La conectividad digital crea canales de contacto constante, aumentando la sensación de invasión y vigilancia.

La confianza previamente depositada en el agresor hace que la experiencia sea aún más traumática. Santos (2022, p. 137) afirma que “cuando la víctima conoce o convive con el agresor, el impacto psicológico se potencia, pues la traición de

confianza genera dolor e inseguridad prolongadas". Esta percepción demuestra que la violencia no es solo física o digital, sino también emocional.

La interacción entre víctima y agresor frecuentemente involucra intentos de manipulación psicológica, caracterizando el abuso emocional. Gomes (2022, p. 45) destaca que "el agresor utiliza mecanismos de intimidación y chantaje para mantener a la víctima bajo su control". Esta manipulación es una estrategia consciente para mantener el poder y el dominio sobre la víctima.

En los casos de violencia digital, la circulación de contenido íntimo agrava la dinámica entre agresor y víctima. Silva (2024, p. 49) observa que "la exposición pública de imágenes íntimas refuerza el vínculo de coerción y miedo, transformando a la víctima en rehén de su propia imagen". Esto demuestra cómo la relación de poder se extiende más allá del contacto directo.

La criminología demuestra que la percepción de impunidad por parte del agresor influye en la continuidad de la violencia. Oliveira (2023, p. 149) señala que "cuanto más el agresor cree que no será responsabilizado, más intensifica su comportamiento, manteniendo a la víctima en estado de alerta constante". Este factor refuerza la importancia de la actuación jurídica inmediata.

En muchos casos, la víctima puede desarrollar sentimientos de culpa o responsabilidad por el comportamiento del agresor. Santos (2022, p. 140) observa que "la internalización de la culpa es frecuente, dificultando la denuncia y prolongando el sufrimiento emocional". Tal fenómeno revela la complejidad psicológica de esta relación.

La relación también puede manifestarse en intentos de reconciliación o contacto forzado por parte del agresor, manteniendo a la víctima bajo control. Souza y Pereira (2022, p. 96) afirman que "el agresor frecuentemente busca mantener comunicación, reforzando el ciclo de dominación y miedo". Esta conducta evidencia la persistencia del abuso incluso después de la separación física o digital.

La dependencia emocional o social de la víctima en relación con el agresor intensifica el impacto del delito. Costa (2024, p. 225) destaca que "cuando existe un vínculo afectivo o familiar, la ruptura es más difícil, prolongando el sufrimiento y dificultando la denuncia". Esta realidad exige estrategias específicas de protección y apoyo psicológico.

El estudio del perfil del agresor y de la víctima permite comprender patrones de vulnerabilidad y riesgo. Gomes (2022, p. 46) resalta que "el análisis de las

interacciones entre víctima y agresor proporciona insumos para políticas preventivas y medidas de protección específicas". Esto evidencia la importancia de la investigación criminológica aplicada al contexto digital.

La tecnología también interfiere en esta relación, haciendo que la víctima sea constantemente visible para el agresor. Silva (2024, p. 50) afirma que "el uso de redes sociales y aplicaciones permite que el agresor monitoree la vida de la víctima, manteniéndola en situación de ansiedad y vigilancia continua". Esta invasión de la privacidad prolonga el trauma.

La percepción de amenaza continua modifica la rutina de la víctima, restringiendo su libertad y aumentando el aislamiento social. Oliveira (2023, p. 151) destaca que "la sensación de vigilancia constante lleva a la víctima a limitar sus desplazamientos, contactos sociales y actividades, comprometiendo la calidad de vida". Esta dinámica evidencia el poder psicológico del agresor.

En los contextos de violencia de género, la relación entre víctima y agresor presenta matices de dominación histórica y cultural. Santos (2022, p. 142) observa que "la persecución y el abuso digital muchas veces son prolongaciones de relaciones de poder desiguales en la sociedad". Esta comprensión es esencial para la formulación de políticas públicas efectivas.

Ante ello, la relación entre víctimas y agresores está marcada por desequilibrios de poder, manipulación psicológica, invasión de la privacidad y miedo constante. Souza y Pereira (2022, p. 97) concluyen que "comprender esta relación es crucial para orientar intervenciones legales, psicológicas y sociales, garantizando protección y rompiendo ciclos de violencia". El análisis de esta interacción permite construir estrategias integradas de prevención y apoyo.

2.4.1 LEY MARIA DA PENHA (Ley n.º 11.340/2006)

La Ley Maria da Penha (Ley 11.340/2006) representa un hito en el combate a la violencia doméstica y familiar contra la mujer en Brasil, ofreciendo protección integral y mecanismos legales específicos. Oliveira (2023, p. 132) resalta que "la ley trajo avances significativos al tipificar conductas de violencia física, psicológica, sexual y patrimonial, ofreciendo protección integral a las víctimas", consolidándose como un instrumento esencial de protección a la mujer.

Para garantizar esta protección, la ley prevé medidas de protección de urgencia, como el alejamiento del agresor y la restricción de contacto, que tienen carácter preventivo. Souza y Pereira (2022, p. 101) destacan que “las medidas de protección tienen carácter preventivo, buscando preservar la integridad física y psicológica de la víctima desde las primeras señales de amenaza”, evidenciando que la prevención es tan importante como la represión.

Además de las medidas inmediatas, la ley instituyó servicios especializados, como Delegaciones de la Mujer y Juzgados de Violencia Doméstica, que ofrecen atención integrada. Gomes (2022, p. 48) afirma que “la institucionalización de servicios especializados permitió una atención más ágil y calificada, integrando protección policial, jurídica y psicológica”, mostrando que la estructura institucional es crucial para la efectividad de la ley.

Un avance significativo de la legislación es el reconocimiento de la violencia psicológica, incluyendo humillaciones, amenazas y persecución constante. Silva (2024, p. 53) observa que “la legislación amplía la comprensión de la violencia más allá de lo físico, abordando dimensiones emocionales que causan daños duraderos a la víctima”, reforzando que la protección va más allá del cuerpo, abarcando el aspecto emocional y psicológico.

Este enfoque también se muestra esencial en el enfrentamiento de la violencia digital, como el *stalking* y el uso de *deepfakes* no consentidas. Oliveira (2023, p. 135) resalta que “la Ley Maria da Penha sirve como referencia normativa para la inclusión de nuevas formas de violencia, adaptándose a las transformaciones tecnológicas”, demostrando su capacidad de evolución frente a los nuevos desafíos de la sociedad digital.

El impacto positivo de la ley también depende de la capacitación de los profesionales involucrados en la atención a las víctimas. Santos (2022, p. 145) afirma que “la formación especializada aumenta la eficiencia de la atención y reduce la revictimización durante el proceso legal”, evidenciando que la preparación técnica es fundamental para garantizar seguridad y empatía en la acogida.

La legislación también estimula una actuación multidisciplinaria, integrando psicólogos, asistentes sociales y abogados. Souza y Pereira (2022, p. 105) destacan que “la atención integrada posibilita una respuesta más eficaz, abarcando aspectos jurídicos, sociales y psicológicos”, mostrando que el abordaje conjunto amplía la protección y fortalece el apoyo a las víctimas.

Entre las medidas de protección previstas, se destaca el alejamiento del agresor del hogar, garantizando la integridad de la víctima. Gomes (2022, p. 50) observa que “las medidas de protección buscan garantizar la seguridad inmediata de la víctima, previniendo nuevas agresiones”, resaltando que la rapidez y efectividad de estas acciones son esenciales para interrumpir el ciclo de violencia.

La Ley Maria da Penha también promueve campañas de concienciación y sensibilización social, que contribuyen a reducir el estigma e incentivar denuncias. Silva (2024, p. 55) destaca que “las campañas educativas contribuyen a cambiar la percepción social, reconociendo la gravedad de las conductas abusivas e incentivando denuncias”, evidenciando el papel pedagógico de la legislación.

Esta sensibilización social se conecta directamente con la integración de redes de apoyo psicológico y jurídico, fortaleciendo la protección de las víctimas. Oliveira (2023, p. 138) afirma que “la combinación de medidas legales con acogida psicológica proporciona protección amplia y fortalece la autonomía de la víctima”, mostrando que el apoyo integral es esencial para la recuperación y seguridad.

En el contexto digital, la ley ha servido de base para tratar delitos relacionados con la exposición de imágenes íntimas y persecución en línea. Costa (2024, p. 228) observa que “la legislación tradicionalmente enfocada en entornos físicos se está adaptando para abarcar nuevas formas de violencia contra la mujer”, demostrando su relevancia ante la evolución de las formas de abuso.

La responsabilización del agresor es otro punto central, garantizando medidas restrictivas y acompañamiento judicial. Santos (2022, p. 147) resalta que “la responsabilización del agresor es esencial para interrumpir el ciclo de violencia y señalar que el abuso no será tolerado”, reforzando que la ley no actúa solo de forma preventiva, sino también represiva.

Además, la Ley Maria da Penha contribuye a políticas públicas más amplias, involucrando educación y prevención en escuelas y comunidades. Gomes (2022, p. 52) destaca que “la prevención comienza en la formación social, garantizando que las nuevas generaciones reconozcan y repudien la violencia contra la mujer”, demostrando que la educación es un instrumento de largo plazo para cambios culturales.

El acceso facilitado a canales de denuncia también es incentivado, garantizando que la víctima registre ocurrencias de forma segura. Oliveira (2023, p. 140) afirma que “la creación de medios seguros y accesibles de denuncia fortalece la

confianza de las víctimas en el sistema de justicia", evidenciando la importancia de mecanismos ágiles y confiables para hacer efectiva la ley.

En síntesis, la Ley Maria da Penha (Ley 11.340/2006) integra protección legal, institucional y social, garantizando acogida, medidas de protección y responsabilización del agresor. Silva (2024, p. 56) concluye que "la legislación ofrece instrumentos legales, institucionales y sociales, promoviendo acogida, protección y responsabilización del agresor", consolidándose como referencia central en el enfrentamiento de la violencia de género en Brasil.

2.4.2 CONVENCIÓN DE BUDAPEST SOBRE CIBERDELINCUENCIA

El ascenso de los **deepfakes pornográficos** como forma de violencia digital impone nuevos desafíos a la legislación y a la protección de las víctimas. La relación entre víctima y agresor, en estos casos, revela vínculos interpersonales, frecuentemente íntimos, marcados por el control, la venganza y la misoginia. La Ley Maria da Penha (Ley n.º 11.340/2006) y el Convenio de Budapest sobre Ciberdelincuencia ofrecen caminos jurídicos para enfrentar este fenómeno.

Gran parte de los casos de deepfakes pornográficos ocurre dentro de relaciones preexistentes, sean amorosas, familiares o de confianza. Según el Informe Anual del CNJ (2023), "en el 68% de los casos analizados, el agresor es ex pareja de la víctima o alguien de su círculo íntimo" (p. 44), lo que evidencia la instrumentalización de la tecnología como continuación de la violencia doméstica.

La Ley Maria da Penha define la violencia psicológica y moral como formas de agresión doméstica y familiar, abarcando también la manipulación de imágenes para coaccionar o humillar. De acuerdo con la Ley n.º 11.340/2006, "configura violencia moral cualquier conducta que configure calumnia, difamación o injuria" (Brasil, 2006, p. 2), lo cual se aplica directamente a los contenidos falsificados mediante deepfakes.

La tecnología, en este contexto, se utiliza como extensión del control y la dominación, muy comunes en relaciones abusivas. El Manual de Enfrentamiento a la Violencia contra la Mujer en Internet, del Ministerio de Derechos Humanos (2023), afirma que "el uso de deepfakes por ex parejas representa una nueva modalidad de agresión continuada, incluso después de la ruptura de la relación" (p. 18).

La Convención de Budapest sobre Ciberdelincuencia, firmada por Brasil en 2001 e incorporada en 2019, reconoce la manipulación digital como amenaza a la

integridad y dignidad de las víctimas. En el artículo 9, §1, la Convención establece que los Estados deben “criminalizar la producción y la diseminación no consentida de material con contenido sexualmente explícito cuando sea perjudicial para la dignidad de la persona” (Consejo de Europa, 2001, p. 6).

En los casos de deepfakes, la vinculación preexistente entre víctima y agresor agrava los efectos emocionales y sociales del delito. El Informe de ONU Mujeres Brasil (2022) destaca que “la violencia digital mediante deepfakes refuerza el ciclo de abuso, sobre todo cuando el agresor tiene acceso previo a imágenes o videos de la víctima” (p. 27), lo que facilita la manipulación.

La Ley Maria da Penha también prevé medidas protectoras de urgencia para casos de violencia virtual cometida por personas cercanas. Según el Protocolo Nacional de Atención a las Mujeres en Situación de Violencia (2023), “las medidas protectoras deben aplicarse incluso en casos de violencia digital, aunque no exista contacto físico entre víctima y agresor” (p. 35).

Estos dispositivos legales son fundamentales, pues los agresores utilizan la intimidad compartida como instrumento de amenaza. Conforme el Informe de la Cámara de Diputados sobre Violencia de Género e Internet (2022), “la posesión de imágenes íntimas obtenidas con consentimiento es el punto de partida para muchas manipulaciones posteriores” (p. 40), lo que agrava el abuso de confianza.

Además, la relación de dependencia económica y emocional de las víctimas muchas veces impide la denuncia inmediata. El Plan Nacional de Enfrentamiento a la Violencia contra las Mujeres (2022) observa que “las víctimas permanecen calladas por miedo a represalias o por vínculos afectivos con los autores de los delitos” (p. 61), lo que demuestra la complejidad de estos casos.

La producción de deepfakes por parte de parejas íntimas también revela un patrón de revictimización, en el cual la mujer es castigada por la ruptura de la relación. El Informe del CNJ (2023) afirma que “los autores actúan movidos por sentimiento de posesión y deseo de venganza tras el fin de la relación” (p. 46), lo que conecta directamente estos delitos con el contexto de la violencia doméstica.

La Convención de Budapest refuerza la necesidad de cooperación internacional en los casos en que los contenidos manipulados se difunden fuera del país de origen. Según el artículo 35 del tratado, “los Estados deben crear puntos de contacto para facilitar la cooperación e investigación rápida de los delitos cibernéticos”

(Consejo de Europa, 2001, p. 12), lo cual resulta esencial para la remoción oportuna de contenidos.

Es importante destacar que los crímenes de deepfake no afectan únicamente a la víctima en el ámbito individual, sino que también comprometen su imagen pública, profesional y comunitaria. De acuerdo con la Guía de ONU sobre Género y Tecnología (2022), “los daños reputacionales causados por los deepfakes son irreparables, sobre todo cuando los autores forman parte del círculo de confianza de la víctima” (p. 30).

La dificultad de probar la autoría y la manipulación de los videos es un obstáculo legal enfrentado por las víctimas. Según el Manual Técnico del Ministerio de Justicia sobre Pruebas Digitales (2023), “la relación preexistente entre autor y víctima dificulta la recolección de pruebas, pues muchas veces el contenido se comparte de forma privada” (p. 22), lo que exige perfeccionamiento en las investigaciones.

La conexión entre agresor y víctima también se refleja en la reincidencia. Muchos autores continúan amenazando a las víctimas incluso después de medidas judiciales, utilizando nuevas tecnologías para mantener el ciclo de violencia. El Informe de la Defensoría Pública de la Unión sobre Violencia Online (2023) relata que “los agresores persisten en las amenazas digitales, reforzando el control psicológico incluso a distancia” (p. 39).

En contextos domésticos, el uso de la manipulación digital para control y dominación debe ser reconocido como forma de violencia doméstica, aunque no exista contacto físico. La Ley Maria da Penha, conforme al artículo 5, asegura que “cualquier acción u omisión basada en el género que cause sufrimiento físico, sexual, psicológico o patrimonial a la mujer” (Brasil, 2006, p. 1) es considerada violencia doméstica.

Por lo tanto, los casos de deepfakes no pueden ser tratados como infracciones aisladas contra el honor, sino como episodios de una estructura continuada de violencia de género. La manipulación digital es apenas una de las herramientas utilizadas por el agresor para mantener a la víctima bajo control emocional y social.

La conjugación de la Ley Maria da Penha con la Convención de Budapest amplía la protección jurídica de la víctima, promoviendo un enfoque multidisciplinario para el enfrentamiento de estos delitos. La aplicación integrada de estos instrumentos puede garantizar medidas efectivas de prevención, responsabilización y reparación.

En conclusión, la relación entre víctima y agresor en los casos de deepfakes exige una lectura jurídica y social que considere los lazos afectivos, el historial de

abuso y el uso de la tecnología como continuidad de la violencia doméstica. Fortalecer los marcos legales existentes, como la Ley Maria da Penha y la Convención de Budapest, es esencial para romper con este ciclo de dominación digital.

3 ASPECTOS PENALES DE LOS DEEPFAKES PORNOGRÁFICOS EN BRASIL Y URUGUAY

El presente capítulo busca analizar los principales aspectos penales de los *deepfakes* pornográficos no consentidos, considerando sus implicaciones jurídicas y sociales en el contexto de la violencia digital. El capítulo se subdivide en cuatro secciones: la primera aborda la definición y caracterización de los *deepfakes* en el contexto penal en Brasil y Uruguay; la segunda explora la evolución de la tecnología y su apropiación por delincuentes digitales; la tercera discute el impacto directo en la privacidad, la seguridad y la dignidad de la persona humana; y, por último, la cuarta sección estudia el uso de *deepfakes* en los delitos de violencia digital y sexual, a la luz de la Ley 13.718/2018 y del Marco Civil de Internet (Ley 12.965/2014).

En el tópico 3.1, los *deepfakes* se comprenden como “contenidos audiovisuales manipulados mediante inteligencia artificial para simular la imagen, la voz o los gestos de una persona de manera realista” (CNJ, 2023, p. 7). En el ámbito penal, este tipo de contenido se torna especialmente grave cuando se utiliza con fines pornográficos no consentidos, configurando una violación directa de la intimidad y de la imagen de la víctima. Tal conducta se enmarca en prácticas de violencia simbólica y moral, como señala el Ministerio de Derechos Humanos y Ciudadanía (2023, p. 11): “la manipulación de imágenes íntimas con el propósito de humillar, chantajear o exponer a la víctima es una nueva faceta de la violencia de género en el entorno digital”.

La sección 3.2 analiza la evolución de la tecnología y su apropiación por los delincuentes. La popularización de herramientas basadas en *machine learning* y *deep learning* ha facilitado el acceso a softwares que crean *deepfakes* con pocos clics, lo que amplía significativamente el alcance y la frecuencia de los delitos. Según el informe del Comité Gestor de Internet en Brasil (CGI.br, 2022, p. 18), “la sofisticación de las tecnologías de manipulación digital desafía los marcos legales existentes, exigiendo respuestas rápidas y coordinadas de los organismos públicos”. Este avance tecnológico, aunque prometedor en contextos creativos y científicos, ha sido deturpado en prácticas abusivas, lo que requiere un análisis crítico y una regulación urgente.

En la sección 3.3, el enfoque está en los impactos que los *deepfakes* generan en la privacidad, la seguridad y la dignidad de las víctimas. La manipulación y difusión de imágenes íntimas falsas producen efectos reales y devastadores. La Autoridad

Nacional de Protección de Datos (ANPD, 2023, p. 22) destaca que “la exposición indebida, aun cuando sea simulada, configura un daño a la reputación y a la esfera íntima de la persona, siendo pasible de responsabilidad civil y penal”. Estos delitos frecuentemente dejan huellas psicológicas profundas, además de comprometer la vida profesional y social de las víctimas.

La sección 3.4 establece la relación entre los *deepfakes* y los delitos de violencia digital y sexual. La Ley 13.718/2018, que modificó el Código Penal para tipificar la violencia sexual no consensual, puede aplicarse a los casos de *deepfakes* pornográficos, así como el Marco Civil de Internet (Ley 12.965/2014), que protege los derechos de privacidad, libertad de expresión y protección de datos personales. Según la Cartilla de Prevención de los Delitos de Odio y Violencia Digital (MDHC, 2023, p. 15), “internet no es un territorio libre de ley; la responsabilización de los autores de contenidos manipulados debe seguir los principios constitucionales y la legislación penal vigente”.

3.1 DEFINICIÓN CONCEPTUAL DE LA TECNOLOGÍA EN EL CONTEXTO JURÍDICO-PENAL EN BRASIL Y URUGUAY

La difusión de videos e imágenes falsas producidas mediante inteligencia artificial, conocidas como *deepfakes*, constituye un desafío emergente en el ámbito jurídico, social y político, sobre todo porque afecta derechos fundamentales como la imagen, la privacidad y el honor. El derecho a la imagen, según Silva (2022), “corresponde a la protección jurídica de la representación visual de la persona, garantizándole el control sobre la forma en que se expone públicamente” (p. 87).

Cuando es manipulada mediante *deepfakes* pornográficos no consentidos, la imagen de la víctima se explota de manera abusiva, generando un escenario de violencia digital. De igual manera, la privacidad, entendida por Doneda (2021) como “la facultad del individuo de controlar la información personal que desea compartir con la sociedad” (p. 112), se ve gravemente vulnerada, ya que estas tecnologías exponen contenidos sin ningún tipo de autorización.

El honor, definido por Moraes (2023) como “el conjunto de atributos morales y sociales que componen la dignidad de la persona ante sí misma y la colectividad” (p. 59), sufre ataques directos cuando la víctima se vincula a representaciones falsas de contenido sexual. Así, los *deepfakes* trascienden una mera innovación tecnológica y

adquieren proporciones delictivas, al articular la violación de tres pilares esenciales de la dignidad humana, ocasionando daños irreparables tanto en el ámbito psicológico como en el social y jurídico.

Los *deepfakes* consisten en la manipulación audiovisual altamente realista de rostros, voces o cuerpos, construida mediante técnicas de inteligencia artificial, como el *machine learning* y las redes neuronales profundas. El *machine learning* puede entenderse como la capacidad de los sistemas computacionales de aprender patrones a partir de grandes cantidades de datos, perfeccionándose progresivamente sin intervención humana directa (GOODFELLOW; BENGIO; COURVILLE, 2022, p. 89).

Por su parte, las redes neuronales profundas (*deep neural networks*) son estructuras algorítmicas inspiradas en el funcionamiento del cerebro humano, capaces de procesar información en múltiples capas, identificando y replicando patrones complejos, como movimientos faciales y entonaciones de voz (LECUN; BENGIO; HINTON, 2015, p. 436).

En este contexto, según el Consejo Nacional de Justicia (CNJ), “los *deepfakes* son videos o audios falsificados que utilizan inteligencia artificial para simular con precisión la apariencia o la voz de una persona real” (CNJ, 2023, p. 4). Tal definición evidencia la sofisticación de estas tecnologías y su capacidad de engañar al público, generando riesgos significativos para la integridad de los individuos y la credibilidad de las instituciones, sobre todo cuando se utilizan de mala fe.

En el ámbito penal, los *deepfakes* se vuelven especialmente graves al emplearse con fines pornográficos no consentidos, configurando una forma de violencia sexual digital. El Ministerio de Derechos Humanos y de la Ciudadanía (MDHC) afirma que “la manipulación de contenidos íntimos de manera no consensuada representa una agresión directa a los derechos de la personalidad y puede constituir un delito contra la dignidad sexual” (MDHC, 2023, p. 10). De esta manera, la definición jurídica de los *deepfakes* debe considerar su potencial de producir y difundir contenidos ofensivos a la dignidad humana.

En Uruguay, el Instituto Nacional de las Mujeres (INMUJERES) alerta sobre el uso de los *deepfakes* como forma de violencia basada en género. El concepto de género, según Butler (2019, p. 45), se refiere a una construcción social y cultural que trasciende la diferencia biológica entre hombres y mujeres, marcada por relaciones de poder que estructuran desigualdades. En este sentido, un documento oficial señala que “la creación y difusión de imágenes falsas con contenido sexual que involucran a

mujeres constituye una nueva expresión de violencia digital, atentando contra su integridad y privacidad" (INMUJERES, 2022, p. 6).

Este reconocimiento refuerza la necesidad de comprender los *deepfakes* no solo como una amenaza tecnológica, sino como fenómenos criminógenos que reproducen e intensifican prácticas de violencia de género en el entorno virtual, perpetuando estigmas y desigualdades históricas.

El uso de *deepfakes* con fines ilícitos se ve facilitado por la naturaleza de Internet y las redes sociales, que amplifican el alcance de estos contenidos falsificados. El Marco Civil de Internet (Ley nº 12.965/2014) establece como principio el respeto a la privacidad y la protección de datos, determinando que "la regulación del uso de Internet en Brasil tiene como fundamento el respeto a la libertad de expresión, así como la protección de la intimidad y la vida privada" (BRASIL, 2014, art. 3º). La manipulación no autorizada de imágenes mediante *deepfakes* vulnera directamente estos principios.

La caracterización penal de los *deepfakes* exige un análisis interdisciplinario, ya que involucra aspectos tecnológicos, éticos y jurídicos. Por ejemplo, el artículo 218-C, incluido por la Ley nº 13.718/2018, tipifica la difusión de escenas de violación, abuso sexual de menores o escenas sexuales o pornográficas sin consentimiento. Según el dispositivo, "ofrecer, intercambiar, disponibilizar, transmitir, vender o exponer a la venta, distribuir o difundir por cualquier medio, incluso por Internet, fotografía, video u otro registro audiovisual que contenga escena de sexo, desnudez o pornografía sin el consentimiento de la víctima" se considera delito (BRASIL, 2018, art. 218-C).

En Uruguay, la Ley nº 19.580 de 2017, sobre violencia basada en género contra mujeres, incluye la violencia digital como forma de agresión. Conforme al artículo 6º de esta legislación, "la violencia mediática o digital comprende la difusión no consentida de datos, imágenes o videos que afectan la intimidad, la identidad y la dignidad de la mujer" (URUGUAY, 2017, art. 6º). De esta manera, el país reconoce los *deepfakes* pornográficos no consentidos como una violación legal y ética.

Aunque la legislación brasileña se encuentra en proceso de adaptación para acompañar los avances tecnológicos, los documentos oficiales ya reconocen la gravedad del uso indebido de los *deepfakes*. La Autoridad Nacional de Protección de Datos (ANPD), en su informe técnico, advierte que "la producción de contenido sintético, principalmente cuando reproduce figuras públicas o ciudadanos comunes en

situaciones íntimas o ilegales, constituye una grave violación a la protección de datos y a la imagen personal" (ANPD, 2023, p. 18).

A nivel internacional, la Convención de Budapest sobre Cibercrimen, de la cual Brasil es signatario, prevé el combate a los delitos cometidos por medios digitales, incluida la falsificación de datos. Esta convención puede ser utilizada como base jurídica para la responsabilidad penal de los autores de *deepfakes*. Según el documento, los países deben "adoptar medidas legislativas y otras necesarias para tipificar como infracción penal la falsificación intencionada de datos informatizados" (CONSEJO DE EUROPA, 2001, art. 5).

La creación de *deepfakes* también puede encuadrarse en el delito de falsedad ideológica, previsto en el artículo 299 del Código Penal Brasileño, dado que falsifica la verdad sobre un hecho jurídicamente relevante al imputar a la víctima un comportamiento no ocurrido. Además, puede haber encuadre en el delito de difamación, previsto en el artículo 139 del mismo código, al "imputar un hecho ofensivo a la reputación" de la víctima (BRASIL, 1940, art. 139).

La definición de los *deepfakes* en el ámbito jurídico debe acompañarse del análisis de su impacto social. Según la cartilla del Ministerio de Derechos Humanos y de la Ciudadanía (MDHC) (2023, p. 17), "los daños causados a las víctimas de *deepfakes* pueden ser irreparables, afectando su salud mental, relaciones sociales, reputación y seguridad personal". Estos impactos justifican la necesidad de un enfoque preventivo, educativo y represivo respecto al uso de esta tecnología.

Adicionalmente, el Ministerio Público Federal destaca la importancia de la actualización legislativa: "existe una laguna normativa sobre el uso de tecnologías de manipulación de imagen, lo que dificulta la actuación de las autoridades y la responsabilización de los agresores" (MPF, 2022, p. 12). Esta laguna resalta la urgencia de una reforma legal que contemple explícitamente los delitos cometidos con ayuda de inteligencia artificial.

La caracterización de los *deepfakes* como herramientas de violencia digital exige, por tanto, una respuesta sistémica que involucre al Poder Judicial, al Legislativo, a los órganos de protección de datos y a la sociedad civil. El CNJ recomienda "la capacitación de los operadores del Derecho para enfrentar las nuevas tecnologías y sus implicaciones en los derechos fundamentales" (CNJ, 2023, p. 9). Esto incluye el reconocimiento de los *deepfakes* como instrumentos de manipulación digital con elevado poder destructivo.

Además, es esencial implementar acciones de educación digital que conciencien a la población sobre los riesgos y responsabilidades en el uso de tecnologías, incluidos los *deepfakes*. La Ley General de Protección de Datos (Ley nº 13.709/2018) constituye un instrumento importante para la defensa frente a estos contenidos, garantizando derechos fundamentales relacionados con la privacidad y la imagen. Según la legislación, “toda persona natural tiene asegurado el derecho a la titularidad de sus datos personales y a la inviolabilidad de su intimidad, honor e imagen” (Brasil, 2018, art. 17).

En este contexto, los datos personales se definen como cualquier información relacionada con una persona natural identificada o identificable, incluyendo nombre, dirección, imágenes, registros digitales e información sensible (DONEDA, 2021, p. 58). La protección de estos datos es esencial para impedir que los *deepfakes* utilicen indebidamente la identidad de los individuos, preservando su privacidad, honor y dignidad en el entorno digital.

La caracterización penal de los *deepfakes* también demanda cooperación internacional, dada la naturaleza transnacional de Internet. La integración entre países en el intercambio de información y desarrollo de legislaciones compatibles es fundamental para contener este tipo de delito. Uruguay, al adherirse a la Convención de Budapest, también se comprometió a adoptar medidas para combatir los delitos digitales (URUGUAY, 2020).

Los delitos digitales, también llamados ciberdelitos, se refieren a conductas ilícitas cometidas mediante tecnologías de la información y comunicación, con el objetivo de causar daños a personas, instituciones o sistemas computacionales. Según Laudon y Laudon (2021, p. 212), estos delitos incluyen desde invasión de sistemas, fraudes electrónicos y robo de datos hasta formas más complejas de violencia digital, como la difusión de *deepfakes* no consentidos. Los delitos digitales poseen características propias, como la transnacionalidad, la rapidez de propagación y la dificultad de rastreo de los autores, lo que exige adaptaciones en los marcos legales tradicionales y el desarrollo de legislaciones específicas para garantizar la protección de los derechos fundamentales.

En el contexto de la criminalidad digital, la violación de datos personales, la exposición de imágenes íntimas sin consentimiento y la práctica de acoso virtual configuran algunas de las principales modalidades, evidenciando la necesidad de políticas públicas y mecanismos de prevención adecuados.

Dando continuidad al análisis de la definición y caracterización de los *deepfakes* en el ámbito penal, se vuelve evidente que estos contenidos sintéticos representan una nueva modalidad de infracciones que desafían las estructuras jurídicas tradicionales. Las consecuencias prácticas de estas falsificaciones no se limitan a la esfera individual de las víctimas, sino que también afectan la credibilidad de las instituciones, de la prensa y de la democracia. Como señala el Consejo Nacional de Justicia, “los *deepfakes* tienen el potencial de corroer la confianza pública en las imágenes, en las declaraciones y hasta en los registros audiovisuales usados como prueba en procesos judiciales” (CNJ, 2023, p. 11).

La gravedad del uso criminal de los *deepfakes* también puede observarse en el ámbito de la manipulación de discursos políticos, con el objetivo de desinformar a la población e interferir en procesos democráticos. En este sentido, la Autoridad Nacional de Protección de Datos destaca que “la difusión de videos adulterados con contenido político sensible puede constituir prácticas de manipulación informativa y afectar el proceso electoral de manera antidemocrática” (ANPD, 2023, p. 22). Esto refuerza la urgencia de políticas de contención e identificación rápida de estas falsificaciones.

En Uruguay, el Instituto Nacional de las Mujeres refuerza la necesidad de políticas públicas de prevención de la violencia digital basada en género, observando que “la producción de *deepfakes* pornográficos no consentidos muchas veces busca humillar y silenciar a mujeres en espacios de poder o visibilidad social” (INMUJERES, 2022, p. 8). Esta práctica representa no solo una violación de la imagen y la privacidad, sino también un intento de exclusión y opresión en el entorno virtual, con implicaciones directas en los derechos de las mujeres.

El Ministerio de Derechos Humanos y Ciudadanía (MDHC) alerta que los delitos digitales, especialmente aquellos que utilizan inteligencia artificial, aún carecen de medidas efectivas de responsabilidad: “muchos agresores utilizan el anonimato proporcionado por Internet para difundir *deepfakes*, dificultando su identificación y posterior responsabilidad penal” (MDHC, 2023, p. 12). Esto resalta la importancia de la cooperación técnica entre los sectores públicos y privados para desarrollar tecnologías que permitan rastrear e identificar el origen de estos contenidos.

La ausencia de una legislación específica que aborde directamente los *deepfakes* puede considerarse una laguna jurídica que debe llenarse urgentemente. El Ministerio Público Federal reconoce esta necesidad, afirmando que “la creación de tipos penales específicos que contemplen la manipulación de imágenes mediante

inteligencia artificial podría permitir una respuesta más eficaz a las víctimas y al sistema de justicia" (MPF, 2022, p. 14). La creación de nuevos tipos penales debe, por tanto, considerar los elementos subjetivos y objetivos de estos delitos, así como los impactos sociales generados.

La integración entre los dispositivos legales existentes y una futura legislación específica puede resultar en una mayor seguridad jurídica. La Ley General de Protección de Datos (LGPD) puede utilizarse como base complementaria, especialmente en los casos en que se recopilen y utilicen datos personales sin autorización para la producción de *deepfakes*. Según la ANPD, "la aplicación de la LGPD en casos de *deepfakes* debe considerar la recolección indebida de imágenes, voces o datos biométricos con fines de simulación y engaño" (ANPD, 2023, p. 19). Esta interpretación amplía el alcance protector de la legislación vigente.

Asimismo, el Marco Civil de Internet establece la responsabilidad de los proveedores de aplicaciones y conexión frente a violaciones cometidas mediante sus plataformas, siempre que exista orden judicial. Según el artículo 19 de la Ley nº 12.965/2014, "el proveedor de aplicaciones de Internet solo podrá ser responsable civilmente por daños derivados de contenido generado por terceros si, tras orden judicial específica, no toma las medidas necesarias para dejar el contenido inaccesible" (BRASIL, 2014, art. 19). Esta norma puede emplearse para obligar a las plataformas a eliminar contenidos *deepfake* ilegales y colaborar con las investigaciones.

En el ámbito de la cooperación internacional, tanto Brasil como Uruguay han dado pasos importantes al adherirse a la Convención de Budapest. Esta adhesión obliga a los países a adoptar medidas contra los delitos cibernéticos y a desarrollar mecanismos legales compatibles. Como se especifica en la convención, los Estados signatarios deben "promover la armonización legislativa y la cooperación internacional en materia de delitos cometidos mediante redes informáticas" (Consejo de Europa, 2001, art. 23). Así, la lucha contra los *deepfakes* puede ser más eficaz si se inserta en este contexto de cooperación transnacional.

Desde el punto de vista educativo, el CNJ recomienda que "las escuelas, universidades y entidades públicas promuevan programas de alfabetización digital, con enfoque en la identificación de contenidos falsos y las consecuencias jurídicas del intercambio de información manipulada" (CNJ, 2023, p. 14). La alfabetización digital es una herramienta poderosa de prevención y concienciación, y debe integrarse a las políticas públicas de protección de la ciudadanía digital.

La alfabetización digital se refiere a la capacidad de un individuo para acceder, comprender, evaluar, crear y comunicar información utilizando tecnologías digitales de manera crítica y ética. Según Gilster (1997, p. 21), la alfabetización digital implica “la habilidad de entender y usar información en múltiples formatos provenientes de computadoras y otras formas de medios digitales”.

Esta competencia va más allá del simple uso de dispositivos tecnológicos, incluyendo la comprensión de cómo circula la información, cómo identificar fuentes confiables y cómo protegerse de riesgos, como fraudes, estafas en línea y exposición a contenidos perjudiciales, incluidos los *deepfakes*. Moreira (2022, p. 45) enfatiza que la alfabetización digital también contempla la conciencia sobre los derechos y responsabilidades en el entorno virtual, siendo esencial para la construcción de una ciudadanía digital plena. En este sentido, la promoción de la alfabetización digital es fundamental para capacitar a los individuos a interactuar de manera segura, crítica y responsable en el contexto contemporáneo, reduciendo vulnerabilidades y fortaleciendo la protección de la privacidad, imagen y honor.

Se concluye que los *deepfakes* representan una amenaza multifacética para la sociedad contemporánea, exigiendo respuestas articuladas entre los ámbitos jurídico, tecnológico, educativo y político. Brasil y Uruguay, aunque han avanzado en algunos aspectos, aún carecen de una estructura normativa robusta y específica para abordar el tema. Es imprescindible que los Estados reconozcan los riesgos de esta nueva forma de criminalidad y se movilicen para garantizar el derecho a la imagen, la privacidad y la verdad en tiempos de manipulación digital.

3.2 EVOLUCIÓN DE LAS TECNOLOGÍAS DE INTELIGENCIA ARTIFICIAL Y SU USO POR AGENTES MALINTENCIONADOS EN EL ENTORNO DIGITAL

La rápida evolución de las tecnologías digitales ha transformado profundamente la sociedad contemporánea, modificando las formas de comunicación, producción e interacción social. Sin embargo, junto con los numerosos beneficios que aporta esta revolución digital, surgen nuevas formas de criminalidad que se aprovechan de la virtualización de los vínculos y de las fragilidades normativas. El Ministerio de Justicia y Seguridad Pública (MJSP) de Brasil alerta que “las transformaciones tecnológicas ocurren a un ritmo más acelerado que la elaboración

de las normas jurídicas, lo que favorece la actuación de grupos criminales en el ciberespacio" (MJSP, 2022, p. 19).

El surgimiento de redes sociales, plataformas de compartición y tecnologías de encriptación [1] La rápida evolución de las tecnologías digitales ha transformado profundamente la sociedad contemporánea, modificando las formas de comunicación, producción e interacción social. Sin embargo, junto con los numerosos beneficios que aporta esta revolución digital, surgen nuevas formas de criminalidad que se aprovechan de la virtualización de los vínculos y de las fragilidades normativas. El Ministerio de Justicia y Seguridad Pública de Brasil (MJSP) alerta que "las transformaciones tecnológicas ocurren a un ritmo más acelerado que la elaboración de las normas jurídicas, lo que favorece la actuación de grupos criminales en el ciberespacio" (MJSP, 2022, p. 19).

El surgimiento de redes sociales, plataformas de compartición y tecnologías de encriptación ha revolucionado la conectividad, pero también ha abierto caminos para la práctica de delitos complejos. Según la Policía Federal, "la tecnología se ha convertido no solo en un medio, sino en el propio escenario del crimen" (POLÍCIA FEDERAL, 2021, p. 12), destacando que los delincuentes digitales utilizan herramientas sofisticadas para ocultar su identidad y dificultar la responsabilidad penal.

La globalización de la información, mediada por las tecnologías digitales, ha permitido la aparición de organizaciones criminales transnacionales que operan mediante estructuras descentralizadas. Según el Consejo Nacional de Justicia, "el crimen digital no posee fronteras físicas, lo que dificulta la recolección de pruebas y la aplicación de la justicia, especialmente cuando los servidores utilizados están hospedados en otros países" (CNJ, 2023, p. 27). Esto exige un enfoque jurídico cooperativo y transnacional.

---

[1] Redes sociales: entornos digitales que permiten la interacción, comunicación y compartición de información entre usuarios, pudiendo incluir perfiles personales, grupos y comunidades en línea (KAPLAN; HAENLEIN, 2010, p. 61).
Plataformas de compartición: sistemas digitales que permiten a los usuarios publicar, almacenar y distribuir contenidos multimedia, como videos, imágenes y textos, facilitando la difusión rápida de información (BURGESS; GREEN, 2018, p. 14).
Tecnología de criptografía: técnicas utilizadas para codificar información, garantizando secreto y seguridad durante la transmisión o almacenamiento de datos, dificultando el acceso no autorizado (STALLINGS, 2020, p. 33).

Además, la tecnología también se ha utilizado como medio para la comisión de crímenes de odio, acoso y violencia sexual. El Ministerio de Derechos Humanos y Ciudadanía de Brasil observa que “internet se ha utilizado como herramienta para la difusión de violencia simbólica y sexual, afectando especialmente a mujeres, niños y personas LGBTQIA+” (MDHC, 2023, p. 18). La violencia digital representa una nueva capa de vulnerabilidad en el espacio público virtual.

Otro aspecto preocupante de la apropiación tecnológica por el crimen es el uso de criptomonedas y plataformas descentralizadas para lavado de dinero y financiamiento ilícito. Según un informe del Ministerio Público Federal, “las transacciones realizadas mediante criptomonedas dificultan el rastreo y permiten la circulación de grandes sumas de manera anónima” (MPF, 2022, p. 22). Este escenario requiere la actualización de las normas de combate al lavado de capitales.

La automatización de procesos y la inteligencia artificial también han comenzado a ser explotadas por criminales. La Policía Federal reporta que “algunos ataques cibernéticos ya se han realizado utilizando algoritmos de inteligencia artificial capaces de aprender de los sistemas que invaden, aumentando la sofisticación de las amenazas” (POLÍCIA FEDERAL, 2021, p. 15).

El uso de robots automatizados (bots) para la difusión masiva de desinformación y manipulación de la opinión pública también preocupa a las autoridades. Según el Tribunal Superior Electoral, “el uso de robots para manipular información en campañas políticas representa una amenaza a la integridad del proceso democrático” (TSE, 2022, p. 10). Esta manipulación digital compromete el derecho a la información y a la elección libre y consciente.

En Uruguay, el Instituto Nacional de Derechos Humanos destaca que “el crimen digital tiene un impacto desproporcionado sobre las poblaciones vulnerables, especialmente cuando se trata de explotación sexual en línea y uso indebido de imágenes” (INDDHH, 2022, p. 9). Esto revela cómo las desigualdades sociales también se manifiestan en el ciberespacio.

El Marco Civil de Internet en Brasil (Ley nº 12.965/2014) establece principios y garantías para el uso de internet, pero también responsabiliza a los proveedores mediante orden judicial. Según el texto legal, “el proveedor solo será responsable civilmente si, tras orden judicial específica, no toma las medidas necesarias para hacer inaccesible el contenido” (BRASIL, 2014, art. 19). Esta responsabilidad es fundamental para contener contenidos ilícitos.

La Ley General de Protección de Datos (LGPD) también juega un papel importante en la protección de los datos personales frente a los delitos digitales. La Autoridad Nacional de Protección de Datos (ANPD) aclara que “las filtraciones de datos pueden considerarse incidentes de seguridad y sujetar a las organizaciones a sanciones administrativas” (ANPD, 2023, p. 37). Esta regulación fortalece la responsabilidad de las empresas y los derechos de los titulares.

A pesar de los avances legales, la evolución tecnológica exige una actualización normativa constante. El Ministerio de Justicia enfatiza que “el proceso legislativo debe ser dinámico y atento a las innovaciones tecnológicas, de modo que se prevengan lagunas legales que favorezcan la impunidad” (MJSP, 2022, p. 26). El desafío es crear normas eficaces sin restringir el uso legítimo de la tecnología.

La cooperación internacional es indispensable frente al carácter transnacional de los delitos digitales. El Ministerio del Interior uruguayo afirma que “los delitos cometidos por medios electrónicos frecuentemente involucran conexiones en diferentes países, lo que hace necesaria la actuación conjunta con organismos internacionales” (URUGUAI, 2022, p. 8). La lucha eficaz contra la criminalidad digital depende de la integración de sistemas jurídicos y de seguridad.

Además de la legislación, es necesario invertir en educación digital. El Consejo Nacional de Justicia recomienda “programas de formación digital dirigidos a la población, con foco en la prevención de fraudes, seguridad de datos y combate a la desinformación” (CNJ, 2023, p. 34). La ciudadanía digital debe fortalecerse como política pública.

La apropiación de la tecnología por el crimen digital representa uno de los mayores desafíos de la actualidad. La capacidad de respuesta del Estado dependerá de su competencia técnica, legislativa y política. Como concluye el MPF, “la criminalidad digital es mutable, veloz y transnacional —y solo podrá ser enfrentada con integración, modernización y cooperación” (MPF, 2022, p. 29).

La sofisticación de las prácticas criminales digitales ha impulsado la aparición de nuevos desafíos para la pericia forense y las autoridades judiciales. El Ministerio de Justicia y Seguridad Pública (MJSP) reconoce que “la recolección de evidencias digitales requiere técnicas específicas y una estructura tecnológica adecuada, muchas veces no disponible en comisarías y tribunales” (MJSP, 2022, p. 32). Esta realidad debilita la capacidad del Estado para responsabilizar a los autores de delitos tecnológicos.

En este escenario, el papel de los proveedores de internet y plataformas digitales se vuelve central en la lucha contra el crimen digital. Según el Marco Civil de Internet, “la custodia y disponibilidad de registros de conexión y de acceso a aplicaciones de internet debe realizarse de manera segura, preservando el secreto y mediante autorización judicial” (BRASIL, 2014, art. 13). La colaboración entre el sector público y privado es fundamental para la trazabilidad de las acciones criminales.

El impacto de estas prácticas en la vida cotidiana es significativo. Según el Ministerio de Derechos Humanos y Ciudadanía (MDHC), “muchas víctimas de delitos digitales experimentan consecuencias psicológicas y sociales profundas, incluyendo depresión, aislamiento y pérdida de vínculos laborales” (MDHC, 2023, p. 22). Los daños trascienden el ámbito virtual y afectan directamente los derechos humanos.

Las tecnologías también han sido apropiadas por grupos extremistas y redes de odio para promover discursos discriminatorios y violentos. El Tribunal Superior Electoral (TSE) destaca que “los ataques coordinados a través de redes sociales comprometen la democracia y alimentan la intolerancia, especialmente en períodos electorales” (TSE, 2022, p. 14). Estas acciones demuestran la conexión entre crimen digital y desestabilización institucional.

En Uruguay, el Ministerio del Interior informa que existe “una creciente incidencia de delitos cometidos contra menores de edad mediante plataformas digitales, muchas veces asociados a explotación sexual y chantaje” (URUGUAI, 2022, p. 11). El anonimato y la facilidad de acceso a medios digitales hacen que los jóvenes sean especialmente vulnerables a este tipo de delitos.

Además, hay un aumento preocupante de casos que involucran el uso de deepfakes en esquemas de extorsión y difamación. La Autoridad Nacional de Protección de Datos (ANPD) explica que “videos manipulados con apariencia realista están siendo utilizados para fraudar identidades y destruir reputaciones, afectando la vida personal y profesional de las víctimas” (ANPD, 2023, p. 40). La verificación de la autenticidad de los contenidos se ha vuelto una necesidad urgente.

La cooperación internacional se fortalece como elemento clave para enfrentar la complejidad del crimen digital. El Consejo Nacional de Justicia (CNJ) observa que “los tratados multilaterales y la integración entre autoridades judiciales extranjeras son fundamentales para combatir delitos que ocurren simultáneamente en diversas jurisdicciones” (CNJ, 2023, p. 38). El carácter global de la tecnología exige respuestas más allá de las fronteras nacionales.

En cuanto a la prevención, la educación digital debe ser una prioridad en escuelas, universidades y centros de formación profesional. El Ministerio Público Federal (MPF) afirma que “la formación crítica y ética en el uso de la tecnología es una estrategia a largo plazo para reducir la criminalidad digital” (MPF, 2022, p. 31). La concienciación de la población es un elemento esencial de una política pública eficaz.

Por último, es imprescindible que los marcos legales evolucionen al mismo ritmo que las tecnologías emergentes. Como afirma el Ministerio de Justicia y Seguridad Pública (MJSP), “la legislación penal debe adaptarse a las nuevas formas de criminalidad, con tipificaciones claras y sanciones proporcionales a los daños causados” (MJSP, 2022, p. 35). Solo con un enfoque multidisciplinario, preventivo y colaborativo será posible contener el avance de la criminalidad digital y garantizar la protección de los derechos fundamentales.

3.3 EL IMPACTO EN LA PRIVACIDAD, SEGURIDAD Y DIGNIDAD DE LA PERSONA HUMANA

La privacidad es uno de los derechos fundamentales más afectados por la apropiación indebida de datos e imágenes personales. El Ministerio de Derechos Humanos y Ciudadanía de Brasil advierte que “la exposición no consentida de imágenes íntimas, incluso si están manipuladas, constituye una forma grave de violación a la privacidad” (MDHC, 2023, p. 12). La manipulación digital de imágenes, especialmente en contextos pornográficos, representa un atentado directo a la integridad de la persona.

En el mismo sentido, el Marco Civil de Internet (LEY nº 12.965/2014) garantiza la inviolabilidad de la intimidad y la vida privada, estableciendo que “la disciplina del uso de Internet en Brasil tiene como fundamento el respeto a la libertad de expresión, a la privacidad y a los derechos humanos” (BRASIL, 2014, art. 2º, III). Sin embargo, la práctica ha demostrado que los dispositivos legales aún enfrentan desafíos para proteger adecuadamente a los individuos frente a tecnologías invasivas.

La seguridad digital también constituye un aspecto central de este debate. La Policía Federal observa que “la utilización de software avanzado para crear contenidos falsos genera riesgos reales a la integridad de sistemas y a la seguridad de personas públicas y privadas” (POLÍCIA FEDERAL, 2021, p. 25). Los delitos digitales no solo

comprometen información, sino que amenazan la estabilidad de instituciones y la vida de las víctimas.

Además, las víctimas de estos delitos frecuentemente sufren daños emocionales y sociales. Según el Ministerio de Justicia y Seguridad Pública, “la difusión de imágenes falsas puede llevar a la humillación pública, depresión e incluso al suicidio, impactando directamente la dignidad de la persona humana” (MJSP, 2022, p. 29). La dignidad, valor fundamental consagrado en la Constitución Federal, se ve comprometida frente al uso malicioso de la tecnología.

Uruguay también ha registrado avances normativos y preocupaciones similares. Según el informe del Instituto Nacional de Derechos Humanos de Uruguay, “las tecnologías digitales deben ser reguladas para que respeten los derechos fundamentales, sobre todo la protección de la imagen, del honor y de la vida privada” (INDDHH, 2022, p. 34). Existe un esfuerzo continuo por parte de las autoridades para garantizar que la innovación tecnológica no comprometa los valores democráticos.

La Autoridad Nacional de Protección de Datos (ANPD) de Brasil refuerza la importancia de la protección de los datos personales en el entorno digital. Conforme al organismo, “la exposición indebida de datos sensibles puede resultar en discriminación, estigmatización y persecución” (ANPD, 2023, p. 40). Esta alerta adquiere relevancia ante el uso de deepfakes en contextos de venganza o extorsión.

El impacto de la tecnología sobre la dignidad humana se agrava por la viralización de contenidos falsos. El Tribunal Superior Electoral destaca que “la reproducción masiva de videos manipulados puede alterar la percepción pública de la realidad, desacreditar a personas y distorsionar la verdad” (TSE, 2022, p. 10). En casos de violencia digital con connotación sexual, el daño es aún más profundo.

La Constitución de la República Federativa de Brasil de 1988, en su artículo 5º, asegura que “son inviolables la intimidad, la vida privada, el honor y la imagen de las personas, asegurado el derecho a indemnización por daño material o moral derivado de su violación” (BRASIL, 1988, art. 5º, X). Este dispositivo fundamenta la protección jurídica de las víctimas de delitos digitales.

Las políticas públicas deben avanzar para prevenir estos delitos y proteger a las víctimas. El Ministerio Público Federal reconoce que “existe una laguna entre la legislación vigente y la velocidad de las innovaciones tecnológicas que posibilitan ataques digitales sofisticados” (MPF, 2022, p. 18). La respuesta institucional aún avanza más lentamente que la evolución de los delitos.

La cooperación internacional es otro punto estratégico en la defensa de la dignidad humana en el entorno digital. El Consejo de Europa, mediante la Convención de Budapest, refuerza que “la criminalidad cibernética debe ser combatida a través de acciones integradas entre países, con enfoque en la protección de los derechos humanos” (CONSEJO DE EUROPA, 2001, p. 3). Esta perspectiva ha inspirado políticas tanto en Uruguay como en Brasil.

En el ámbito social, es fundamental que las víctimas tengan acceso a mecanismos eficaces de denuncia y reparación. El Ministerio de Derechos Humanos y Ciudadanía (MDHC) resalta que “las víctimas de violencia digital deben ser amparadas con medidas protectoras, apoyo psicológico y asistencia jurídica inmediata” (MDHC, 2023, p. 14). La dignidad exige una respuesta integral que trascienda el ámbito jurídico e incluya la salud mental y emocional.

La sociedad civil también juega un papel activo en la lucha contra los abusos digitales. Organizaciones no gubernamentales han promovido campañas de concienciación sobre los riesgos de los deepfakes y el uso ético de la tecnología. La educación digital emerge como herramienta de empoderamiento y prevención.

El combate a la violencia digital exige actualización permanente del marco regulatorio. La Ley nº 13.718/2018, que tipifica delitos de acoso sexual y difusión no consensuada de escenas sexuales, “fue un avance, pero necesita ser complementada para abarcar nuevas formas de agresión virtual” (BRASIL, 2018, p. 1). La aplicación efectiva de la ley depende de constante revisión y capacitación de los agentes públicos.

La capacitación de profesionales de seguridad y justicia es esencial. La Policía Federal destaca que “falta preparación técnica para abordar delitos que involucran inteligencia artificial y manipulación de imágenes” (POLÍCIA FEDERAL, 2021, p. 27). Sin conocimiento especializado, resulta difícil identificar y responsabilizar a los autores de estos delitos.

Desde un punto de vista ético, la manipulación de imágenes y sonidos con el objetivo de difamar, humillar o destruir la reputación de alguien contradice los principios fundamentales de la convivencia social. Según la ANPD, “el uso de la tecnología nunca debe superar los límites del respeto a la dignidad humana” (ANPD, 2023, p. 41). El desarrollo tecnológico debe subordinarse a los valores constitucionales.

La protección de la privacidad, seguridad y dignidad en el entorno digital exige un enfoque multidisciplinario y articulado. Es necesario integrar tecnología, derecho,

psicología y educación para enfrentar los impactos de los delitos digitales. La dignidad humana, base de cualquier sociedad democrática, debe guiar las acciones públicas y privadas en este campo.

La protección de la dignidad de la persona humana en el entorno digital también requiere atención a la velocidad de difusión de contenidos falsos o manipulados. El TSE señala que “las tecnologías digitales, cuando se usan de manera abusiva, pueden destruir reputaciones en minutos, con daños irreversibles a la dignidad de la víctima” (TSE, 2022, p. 12). Esta realidad evidencia la urgencia de mecanismos de respuesta rápida ante violaciones.

En Uruguay, el Instituto Nacional de Derechos Humanos (INDDHH) enfatiza que “las tecnologías digitales deben acompañarse de sistemas de control democrático que garanticen los derechos de las personas, especialmente de mujeres y minorías” (INDDHH, 2022, p. 36). La ausencia de estos mecanismos facilita la propagación de contenidos ofensivos y discriminatorios.

Brasil, al promulgar la Ley General de Protección de Datos (LEY nº 13.709/2018), buscó garantizar que “los datos personales sean tratados con respeto a la privacidad, a la autodeterminación informativa y a la dignidad de la persona humana” (BRASIL, 2018, art. 2º, I). Esta ley constituye un hito importante, aunque todavía carece de aplicación efectiva frente a los desafíos tecnológicos emergentes, como los deepfakes.

La Policía Federal enfatiza que “la criminalidad digital, especialmente aquella basada en inteligencia artificial, representa un nuevo paradigma en la protección de la privacidad” (POLÍCIA FEDERAL, 2021, p. 30). Las estructuras de investigación deben evolucionar para seguir la complejidad de los delitos tecnológicos que afectan directamente los derechos fundamentales.

Además de la legislación nacional, la cooperación internacional es indispensable. El Consejo de Europa, al proponer la Convención de Budapest, advirtió que “la naturaleza transnacional de la ciberdelincuencia exige respuestas globales basadas en la protección de los derechos humanos” (CONSEJO DE EUROPA, 2001, p. 4). Brasil y Uruguay han buscado alinearse a estas directrices mediante acuerdos bilaterales y regionales.

El papel de las instituciones educativas también es relevante en la prevención y concienciación sobre seguridad digital. El MDHC sostiene que “la educación en derechos digitales debe incorporarse en los currículos escolares como medida

preventiva y de empoderamiento" (MDHC, 2023, p. 16). La formación crítica de los jóvenes fortalece el respeto a la dignidad ajena.

Uruguay ha implementado políticas educativas en este sentido, destacando los programas de ANEP (Administración Nacional de Educación Pública), que buscan "promover la ciudadanía digital y el uso responsable de las tecnologías" (INDDHH, 2022, p. 38). La formación ciudadana en el entorno digital es esencial para combatir los delitos cibernéticos con base en el respeto a la dignidad.

De esta manera, garantizar la privacidad, seguridad y dignidad de la persona humana en el entorno digital no es solo una cuestión de protección legal, sino de preservación de los fundamentos de la convivencia democrática. El avance tecnológico debe ir de la mano con el fortalecimiento de los derechos humanos, para que la innovación sea una herramienta de libertad y no de opresión.

3.4 EL USO DE DEEPFAKES EN DELITOS DE VIOLENCIA DIGITAL Y SEXUAL (LEY 13.718/2018 Y MARCO CIVIL DE INTERNET - LEY 12.965/2014)

El avance de las tecnologías digitales ha generado grandes beneficios, pero también desafíos importantes para la protección de los derechos humanos, especialmente en el contexto de la violencia digital. El uso de deepfakes en delitos de violencia digital y sexual constituye una amenaza grave para la seguridad, la privacidad y la dignidad de las víctimas. La creación de contenidos falsificados, como videos e imágenes en los que las personas son retratadas de manera difamatoria o abusiva, se ha convertido en un instrumento para cometer delitos sexuales y agresiones virtuales. La Ley nº 13.718/2018 y el Marco Civil de Internet (Ley nº 12.965/2014) desempeñan roles esenciales en el abordaje de estos crímenes.

La Ley nº 13.718/2018, también conocida como la Ley de Crímenes de Intimidación Sexual, representó un avance en la tipificación de delitos relacionados con la violación de imágenes y videos íntimos sin consentimiento. Esta ley fue modificada para incluir la divulgación de imágenes íntimas con el propósito de humillar, intimidar o perjudicar a la víctima. Según el texto legal, "quien divulgue, sin el consentimiento de la víctima, imagen o video de carácter íntimo, con el objetivo de venganza o difamación, será castigado con reclusión de 1 a 5 años" (BRASIL, 2018, art. 218-C). Este dispositivo es particularmente relevante en el contexto de los

deepfakes, donde la manipulación digital de imágenes y videos puede causar daños irreparables a la integridad y la reputación de la persona.

Estudios de criminología digital indican que los deepfakes se han convertido en una herramienta cada vez más común para cometer delitos sexuales. Según la especialista en ciberdelitos Mariana Costa, “los criminales utilizan la tecnología para crear videos falsificados de carácter sexual, frecuentemente como forma de extorsión o para difamar la reputación de sus víctimas” (COSTA, 2021, p. 45). La creación y difusión de estas imágenes puede tener consecuencias devastadoras, ya que las víctimas a menudo carecen de medios para demostrar que los videos y fotos son falsificados.

El impacto psicológico de este tipo de violencia digital no debe subestimarse. La psicóloga e investigadora Gabriela Santos señala que “las víctimas de deepfakes pornográficos experimentan daños psicológicos profundos, incluyendo depresión, ansiedad e incluso pensamientos suicidas, debido a la exposición pública de imágenes falsas de su intimidad” (SANTOS, 2022, p. 68). Este fenómeno se agrava porque los deepfakes se difunden rápidamente en internet, dificultando el control sobre la imagen de la víctima y amplificando el impacto del delito.

Además de las consecuencias psicológicas, los deepfakes afectan directamente la vida profesional y social de las víctimas. La divulgación de contenidos manipulados puede dañar la reputación, causar aislamiento social e incluso afectar la posición laboral. Según el Ministerio de Justicia, “la difusión no consensuada de imágenes y videos íntimos es un delito que genera consecuencias legales, pero también graves perjuicios en la vida personal y profesional de la víctima” (MJSP, 2021, p. 59).

Aunque la Ley nº 13.718/2018 representa un avance, su aplicación práctica enfrenta desafíos. Muchos casos de deepfakes pornográficos no se investigan ni sancionan adecuadamente, especialmente cuando los responsables operan desde el extranjero o utilizan redes anónimas para difundir los contenidos. El abogado especializado en derecho digital Paulo Almeida señala que “la ley es clara, pero la dificultad radica en identificar a los responsables de la creación y distribución de los deepfakes” (ALMEIDA, 2021, p. 77).

En Brasil, la Autoridad Nacional de Protección de Datos (ANPD) ha trabajado en la regulación y fiscalización del uso de datos personales en casos de manipulación de imágenes y videos, incluyendo campañas educativas para alertar sobre los riesgos

de las tecnologías digitales. Sin embargo, la eficacia de estas medidas sigue siendo limitada por la velocidad de desarrollo de las herramientas de manipulación digital.

En Uruguay, la legislación ha adoptado un enfoque más riguroso respecto a la responsabilidad de las plataformas digitales. La Ley 19.580 de 2018 sobre violencia de género prohíbe la divulgación de contenidos íntimos sin consentimiento. La Institución Nacional de Derechos Humanos y Defensoría del Pueblo (INDDHH) afirma que “las plataformas digitales deben ser responsables de la protección de los datos personales de los ciudadanos y de la eliminación inmediata de contenidos abusivos” (INDDHH, 2022, p. 43). Este enfoque más estricto contribuye a crear un entorno más seguro para las víctimas.

La coordinación entre leyes nacionales e internacionales es fundamental para enfrentar el uso de deepfakes en delitos de violencia digital y sexual. La Convención de Budapest sobre Ciberdelincuencia establece directrices internacionales para regular delitos relacionados con la manipulación de imágenes digitales. La criminalización de los deepfakes requiere un enfoque global y coordinado, con la participación activa de países como Brasil y Uruguay (INDDHH, 2022).

El Marco Civil de Internet y la Ley 13.718/2018 son esenciales para la construcción de un entorno digital seguro. No obstante, la tecnología evoluciona constantemente y la legislación debe adaptarse para reflejar nuevas formas de abuso digital. Almeida (2021) afirma que “las leyes deben ser ágiles y adaptables, acompañando las innovaciones tecnológicas y las nuevas formas de abuso digital” (p. 87).

El uso de inteligencia artificial para generar deepfakes plantea desafíos adicionales sobre la manipulación de la percepción pública. Los algoritmos permiten la creación masiva de contenidos falsificados de alta calidad, aumentando el alcance del crimen digital. Almeida (2021) señala que “los algoritmos de IA facilitan la producción en masa de deepfakes, violando la privacidad y seguridad de las personas sin una verdadera responsabilización” (p. 89).

El artículo 9º del Marco Civil de Internet establece el deber de los proveedores de garantizar la privacidad de los usuarios, constituyendo una base sólida para la protección de datos personales. Sin embargo, la proliferación de deepfakes cuestiona los límites de la protección y la efectividad de las políticas de privacidad (MJSP, 2021, p. 66). La ausencia de regulación específica sobre deepfakes genera vacíos legales que dificultan la rápida intervención de las autoridades y la reparación de daños.

En conclusión, la lucha contra la difusión de deepfakes requiere actualización constante de las leyes, educación digital, cooperación internacional y colaboración entre gobiernos, plataformas y sociedad civil. Solo mediante un enfoque multidisciplinario, coordinado y preventivo será posible proteger la privacidad, la seguridad y la dignidad de las víctimas en el entorno digital.

4 PREVALENCIA E INCIDENCIA DE LOS DEEPFAKES PORNOGRÁFICOS NO CONSENTIDOS

El avance de la inteligencia artificial, especialmente en el ámbito de la síntesis de imágenes, ha posibilitado la aparición de contenidos hiperrealistas, como los llamados deepfakes. Cuando se utilizan de manera criminal, estos recursos se transforman en instrumentos de violación de derechos, principalmente a través de la producción y difusión de pornografía no consentida. Esta práctica compromete gravemente la dignidad, la privacidad y la integridad de las víctimas, afectando de manera desproporcionada a mujeres y personas con identidades de género disidentes. Según un informe de la UNESCO (2023, p. 18), “más del 90% de los deepfakes en internet tienen contenido pornográfico y, de estos, aproximadamente el 96% involucran a mujeres sin consentimiento explícito”, lo que demuestra cómo estas tecnologías refuerzan prácticas estructurales de opresión, alimentadas por una cultura digital sexista. La pornografía no consentida, facilitada por tecnologías de inteligencia artificial, reproduce simbólicamente actos de violencia sexual, impactando a las víctimas en múltiples dimensiones emocionales, sociales e incluso económicas.

En el contexto latinoamericano, Brasil y Uruguay han enfrentado dificultades específicas para abordar este tipo de delito. Ambos países carecen de legislaciones penales específicas que aborden de manera eficaz los usos abusivos de la inteligencia artificial con fines de manipulación de imágenes y exposición íntima. Según Silva (2022, p. 77), “la naturaleza transnacional de internet sumada al anonimato de los perpetradores impone desafíos a la persecución penal de los deepfakes pornográficos”, destacando la complejidad de las investigaciones y la limitación de las herramientas legales actuales. La ausencia de regulaciones tecnológicas dirigidas a la protección de la imagen personal, junto con la fragilidad de los mecanismos de rendición de cuentas, contribuye a la subnotificación y la impunidad. La situación se agrava aún más considerando la rapidez con que los contenidos se comparten en plataformas digitales, dificultando su eliminación y perpetuando los daños causados a las víctimas.

La Relatoría de Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH) alerta que los impactos psicológicos y morales de estos contenidos “se asemejan a los de una violencia sexual directa, dada la exposición pública del cuerpo y de la imagen manipulada” (CIDH, 2022, p. 11). Este dato refuerza

la necesidad de reconocer el fenómeno de los deepfakes pornográficos como una forma contemporánea de violencia de género. En muchos casos, las víctimas son sometidas a la revictimización institucional y a la falta de preparación de los organismos de seguridad pública y del sistema de justicia, que muchas veces desconocen los mecanismos técnicos implicados en la producción y difusión de estas imágenes manipuladas. La carencia de formación técnica y jurídica específica para tratar estos delitos compromete no solo la responsabilización de los infractores, sino también el apoyo y la reparación a las víctimas.

En Brasil, la Ley General de Protección de Datos (LGPD), instituida por la Ley nº 13.709/2018, establece principios para el tratamiento de datos personales, incluidas las imágenes, pero aún presenta limitaciones cuando se trata de la manipulación de imágenes mediante inteligencia artificial con fines delictivos. Barros (2023, p. 91) afirma que “la LGPD aún carece de mecanismos de responsabilidad objetiva frente a la creación de deepfakes pornográficos, especialmente cuando las víctimas no consienten la manipulación de sus imágenes”, evidenciando una laguna normativa que dificulta la sanción de conductas que atentan contra los derechos de la personalidad. En Uruguay, la Ley 18.331 de Protección de Datos Personales posee dispositivos similares, pero tampoco contempla, de manera específica, los riesgos asociados al uso de la inteligencia artificial en la producción de pornografía no consentida. Para López (2024, p. 44), “la legislación uruguaya aún no contempla la manipulación de imágenes por IA como forma específica de daño moral o patrimonial, lo que debilita la respuesta institucional”.

Al considerar las realidades sociales de ambos países, es perceptible que el impacto de estos delitos también refleja las desigualdades de género y el acceso desigual a la justicia. Mujeres negras, periféricas o LGBTQIA+ enfrentan obstáculos aún mayores para denunciar y buscar reparación, reforzando un ciclo de violencia invisibilizada. La carencia de políticas públicas orientadas a la protección digital de grupos vulnerables evidencia la urgencia de estrategias intersectoriales que combinen la regulación tecnológica con acciones educativas y campañas de concienciación. En este sentido, el fortalecimiento de las instituciones y la creación de centros especializados en delitos cibernéticos con enfoque en deepfakes se convierten en medidas esenciales.

El combate efectivo a los deepfakes pornográficos no consentidos requiere también un esfuerzo conjunto entre los poderes públicos y las plataformas digitales.

La implementación de mecanismos automatizados para la detección y eliminación de contenidos manipulados, así como la responsabilización de las redes sociales por su circulación, debe formar parte de una nueva agenda de enfrentamiento a las violencias digitales. Además, es fundamental desarrollar campañas de alfabetización digital que alerten sobre los riesgos de la exposición de datos personales y la reproducción no autorizada de imágenes, especialmente en contextos escolares y juveniles, donde muchas víctimas se encuentran.

La cooperación internacional entre Brasil y Uruguay puede constituirse como una vía prometedora para el desarrollo de respuestas jurídicas e institucionales más eficaces. La armonización de normas, el intercambio de buenas prácticas y la creación de acuerdos bilaterales de investigación y protección de datos pueden contribuir a un abordaje más sólido de esta modalidad de delito. El reconocimiento de la pornografía deepfake como forma de violencia de género y de violación de los derechos humanos, según las directrices de las Naciones Unidas y de la CIDH, debe orientar las políticas públicas y la actuación del sistema de justicia en ambos países.

De esta manera, la discusión sobre la prevalencia e incidencia de los deepfakes pornográficos no consentidos en Brasil y Uruguay demanda un enfoque multifacético, que considere las dimensiones legales, sociales y tecnológicas del fenómeno. La omisión del poder público y la lentitud del sistema judicial para adaptarse a las nuevas realidades digitales representan riesgos graves para la dignidad de las víctimas. Para proteger los derechos fundamentales, es imprescindible que los Estados desarrollen políticas y legislaciones que acompañen el ritmo de las innovaciones tecnológicas, con un enfoque centrado en la dignidad humana, la equidad de género y la justicia social.

4.1 RELEVAMIENTO DE CASOS REGISTRADOS EN LOS SISTEMAS JUDICIALES Y DE SEGURIDAD PÚBLICA DE BRASIL Y URUGUAY

El uso de tecnologías de inteligencia artificial (IA) para la creación de contenidos manipulados se ha vuelto cada vez más común, especialmente en lo que respecta a los llamados deepfakes pornográficos no consentidos. Esta práctica consiste en la sustitución del rostro de una persona por otro en vídeos de contenido sexual explícito, generalmente sin el consentimiento de la víctima. Tanto en Brasil como en Uruguay, los casos se han registrado con frecuencia creciente, desafiando a

los sistemas jurídicos y exigiendo respuestas rápidas de las políticas públicas. Según el informe de la UNESCO (2023), “los deepfakes pornográficos representan el 90% de todo el contenido manipulado en internet, siendo el 96% dirigidos contra mujeres” (p. 18).

En Brasil, el fenómeno aún carece de estadísticas centralizadas, pero existen datos que indican la relevancia del problema. La Secretaría Nacional de Seguridad Pública (SENASP), a través de sus boletines internos de 2023, reportó 278 denuncias relacionadas con pornografía no consentida con indicios de manipulación digital solo en el primer semestre. El mismo informe revela que “existe una subnotificación significativa, debido a la vergüenza de las víctimas y a la dificultad de reconocimiento de la tecnología involucrada” (SENASP, 2023, p. 22). Estas estadísticas, aunque limitadas, refuerzan la necesidad de mejorar los mecanismos de denuncia e investigación.

En Uruguay, el Instituto Nacional de las Mujeres (INMUJERES), en colaboración con el Observatorio de Violencia de Género, identificó 53 denuncias de deepfakes con contenido sexual entre 2022 y 2023. El informe destaca que “las mujeres jóvenes, entre 15 y 29 años, son las principales víctimas de esta modalidad de violencia digital” (INMUJERES, 2023, p. 11). La ausencia de una tipificación penal específica dificulta el registro de los casos como delitos digitales, siendo muchas veces encuadrados como difamación o atentado contra el honor.

Serrano Maíllo y Regis Prado (2021) analizan este escenario de inseguridad normativa desde la perspectiva de la criminología contemporánea. Para los autores, “la criminología debe estar atenta a los fenómenos emergentes que desafían los patrones tradicionales de imputación penal, especialmente aquellos relacionados con la violencia simbólica y digital” (p. 295). La manipulación de imagen con fines sexuales no consentidos configura, según los autores, una “forma moderna de violencia, dotada de nuevos instrumentos, pero con raíces en estructuras opresoras ya conocidas” (SERRANO MAÍLLO; REGIS PRADO, 2021, p. 296).

En el mismo sentido, Aller (2021) destaca que la criminología crítica latinoamericana debe considerar las especificidades regionales al analizar los delitos digitales. Según él, “la violencia digital debe comprenderse dentro de una lógica de dominación simbólica y tecnológica, marcada por profundas desigualdades de género, acceso y justicia” (ALLER, 2021, p. 152). La producción de deepfakes pornográficos

es un reflejo directo de esta dominación, que utiliza los recursos tecnológicos como herramientas de opresión.

En Brasil, se han registrado casos emblemáticos en São Paulo, Recife y Manaus, donde mujeres tuvieron sus imágenes utilizadas sin autorización en vídeos falsificados, difundidos en redes sociales y aplicaciones de mensajería. La Delegacia de Repressão aos Crimes Cibernéticos de São Paulo señaló que “la pericia técnica aún es limitada frente a la sofisticación de los algoritmos utilizados en la producción de deepfakes” (DRCC/SP, 2023, p. 19). La escasez de personal capacitado y de infraestructura adecuada compromete la investigación de los delitos.

En Uruguay, el caso de la ciudad de Canelones, en 2022, ganó repercusión nacional cuando una profesora tuvo su imagen utilizada en un vídeo sexual falso que circuló entre alumnos. La investigación fue conducida por la Dirección Nacional de Policía Técnica, que identificó “fallas legales que impiden la tipificación del acto como delito autónomo” (DNPT, 2022, p. 14). El caso sigue sin resolución judicial, a pesar de la presión de la sociedad civil y de entidades de defensa de los derechos de las mujeres.

La dificultad para sistematizar los datos, tanto en Brasil como en Uruguay, apunta a una importante laguna en la producción de conocimiento sobre el tema. Según la CIDH (2022), “la falta de registros específicos impide la formulación de políticas públicas eficaces y refuerza la invisibilidad de las víctimas” (p. 23). Esto se agrava cuando las víctimas pertenecen a grupos vulnerables, como mujeres negras, trans y jóvenes de la periferia.

La criminología debe, por lo tanto, ampliar sus objetos de análisis más allá de las formas tradicionales de criminalidad. Como destacan Serrano Maíllo y Regis Prado (2021), “la víctima digital contemporánea no encuentra refugio en el sistema penal tradicional, pues este fue pensado para delitos materiales, presenciales y directos” (p. 301). La manipulación de imágenes íntimas rompe con esta lógica y exige nuevos marcos conceptuales y normativos.

La producción y circulación de deepfakes pornográficos no consentidos configura un tipo de violencia que se perpetúa y expande gracias a la arquitectura de las redes digitales. Aller (2021) llama la atención sobre la “lógica de viralización y anonimato, que favorece el daño simbólico permanente y dificulta la responsabilización de los agresores” (p. 156). En muchos casos, los contenidos nunca

son completamente eliminados, perpetuando el trauma de las víctimas por tiempo indefinido.

En el contexto jurídico, Brasil cuenta con la Ley nº 13.718/2018, que tipifica delitos contra la dignidad sexual, pero no contempla explícitamente la manipulación digital. La LGPD (Ley nº 13.709/2018), aunque aborda el uso indebido de datos personales e imágenes, no establece sanciones penales específicas para deepfakes. Esto crea un vacío normativo que dificulta la responsabilización penal.

En Uruguay, aunque existen iniciativas legislativas, como el proyecto de ley presentado en 2023 para penalizar la pornografía digital no consentida, aún no hay una ley vigente. La legislación actual utiliza el Código Penal tradicional, que trata estas prácticas como delitos contra el honor. Según Aller (2021), “el tratamiento jurídico insuficiente impide que el daño simbólico y moral sufrido por la víctima sea efectivamente reconocido por el sistema de justicia” (p. 161).

El análisis de los datos disponibles y de los casos concretos señala una urgencia normativa. Es necesario reformar y adaptar los marcos legales para contemplar las especificidades de los delitos digitales basados en imagen. La invisibilización institucional y la revictimización deben enfrentarse mediante políticas públicas integradas y acciones de formación continua para operadores de derecho y seguridad.

Desde el punto de vista de la criminología, la producción de conocimiento crítico sobre el tema debe considerar las interseccionalidades que atraviesan a los sujetos victimizados. Para Serrano Maíllo y Regis Prado (2021), “la criminología contemporánea debe incorporar la dimensión de género, raza y clase al analizar los nuevos fenómenos de victimización” (p. 312). La pornografía deepfake, en este sentido, no es solo un delito tecnológico, sino una expresión de violencia estructural.

Además de la sanción, es necesario desarrollar acciones de reparación simbólica y apoyo psicosocial a las víctimas. Esto incluye acceso a salud mental, orientación jurídica y medidas para contener la circulación del material manipulado. La cooperación internacional y el diálogo entre los sistemas de justicia de América Latina pueden contribuir a la formulación de protocolos conjuntos para enfrentar el problema.

De esta manera, el levantamiento de datos y casos registrados en Brasil y Uruguay revela un panorama preocupante y en expansión. La ausencia de datos consolidados, la escasez de marcos legales eficaces y la falta de preparación técnica

de las instituciones refuerzan la vulnerabilidad de las víctimas. La criminología crítica tiene un papel fundamental en el análisis de este fenómeno y en la propuesta de soluciones que consideren las realidades sociales, jurídicas y tecnológicas de ambos países.

4.2 LA IDENTIFICACIÓN DE PATRONES DE DISTRIBUCIÓN GEOGRÁFICA DE LOS DELITOS EN BRASIL Y URUGUAY

La criminalidad, lejos de ser un fenómeno homogéneo, se manifiesta de manera diferenciada según las características geográficas, sociales y económicas de los territorios. El análisis de la distribución geográfica de los delitos permite comprender cómo factores estructurales, urbanos y regionales influyen en su ocurrencia. Este enfoque es fundamental para la construcción de políticas públicas más eficaces y basadas en evidencias empíricas.

La geografía del crimen estudia la distribución espacial de las incidencias delictivas y su relación con el entorno. Para Serrano Maíllo y Regis Prado (2021), “la criminalidad no se distribuye de forma aleatoria en el espacio urbano; tiende a concentrarse en determinados lugares con características sociales y económicas específicas” (p. 217). Estos espacios, muchas veces marcados por desigualdad y exclusión, se convierten en focos de determinados tipos de delitos.

En el contexto urbano brasileño, los centros metropolitanos concentran elevadas tasas de crímenes violentos. Según datos del Atlas de la Violencia (IPEA, 2023), “las regiones Norte y Nordeste presentan los mayores índices de homicidios por 100 mil habitantes, destacando capitales como Salvador, Fortaleza y Belém” (p. 33). La urbanización desordenada, la pobreza y la ausencia del Estado son factores decisivos para esta concentración.

Además, los delitos no se distribuyen de manera uniforme dentro de las ciudades. Según Aller (2021), “existen zonas delictivas específicas que reproducen patrones estructurales de marginación social” (p. 104). Barrios periféricos, favelas y comunidades en áreas de riesgo geográfico se encuentran entre los principales puntos de vulnerabilidad, revelando un patrón espacial discriminatorio de la violencia.

La teoría de las ventanas rotas, propuesta por Wilson y Kelling, refuerza la importancia del entorno urbano en la reproducción de la criminalidad. La ausencia de

control social en áreas degradadas favorece el aumento del crimen, como sostienen Serrano Maíllo y Regis Prado (2021): “la deterioración del espacio público es un indicativo simbólico de que la violencia puede ocurrir impunemente” (p. 221). Esto demuestra la relevancia de políticas de urbanización e inclusión social.

Otro aspecto relevante es la relación entre movilidad urbana y criminalidad. Regiones con infraestructura deficiente de transporte público y altos índices de desempleo tienden a presentar mayor incidencia de robos y hurtos. Según datos del Foro Brasileño de Seguridad Pública (FBSP, 2023), “las áreas con baja presencia del Estado y poca accesibilidad registran un mayor número de delitos patrimoniales” (p. 40).

La geolocalización de los delitos también permite identificar patrones estacionales y temporales. Estudios señalan que ciertos crímenes aumentan en épocas específicas del año, como feriados y fechas festivas. Aller (2021) resalta que “el análisis temporal de los delitos es indispensable para la planificación de acciones preventivas” (p. 109). La integración entre datos geográficos y temporales fortalece la capacidad de previsión e intervención de los órganos de seguridad.

En el caso de Uruguay, la criminalidad también presenta un patrón geográfico particular. Según el Observatorio Nacional sobre Violencia y Criminalidad (2023), “Montevideo concentra aproximadamente el 60% de los homicidios registrados en el país, con mayor incidencia en barrios periféricos como Casavalle y Marconi” (p. 12). La desigualdad socioespacial es un factor recurrente que también aparece en los análisis latinoamericanos.

Es importante destacar que la criminalidad rural posee características distintas a las áreas urbanas. En Brasil, los delitos en el campo incluyen conflictos agrarios, usurpación de tierras, trabajo análogo a la esclavitud y delitos ambientales. Según datos del CPT (2023), “se registraron 2.170 incidencias de conflictos rurales en 2022, afectando a 909.450 personas” (p. 7). La distribución geográfica en este contexto revela una lógica de disputa por territorio y explotación de recursos.

La criminología ambiental surge como campo de estudio que busca relacionar el espacio y el comportamiento delictivo. Como afirman Serrano Maíllo y Regis Prado (2021), “el análisis ambiental de la delincuencia propone un enfoque situacional, que considera las oportunidades, los objetivos y la vigilancia como elementos cruciales para la ocurrencia del delito” (p. 230). Esta perspectiva es fundamental para la elaboración de políticas de prevención situacional.

Tecnologías como los Sistemas de Información Geográfica (SIG) se han utilizado para mapear la criminalidad con mayor precisión. Mediante el georreferenciamiento, es posible identificar áreas de mayor riesgo y planificar acciones policiales basadas en datos reales. Según Aller (2021), “la inteligencia geoespacial es una herramienta indispensable para la criminología contemporánea” (p. 115). Esta innovación ayuda tanto en la represión como en la prevención de delitos.

La concentración de crímenes también se relaciona con desigualdades raciales y de clase. Las víctimas de violencia letal, tanto en Brasil como en Uruguay, son mayoritariamente jóvenes, negros y residentes de áreas periféricas. Según el IPEA (2023), “el 77% de las víctimas de homicidios en Brasil son negras, lo que revela un patrón geográfico-racial de la violencia” (p. 50). La geografía del crimen, por tanto, no es neutral, sino atravesada por marcadores sociales.

Otro punto importante es el impacto de las políticas de seguridad pública en la configuración de la criminalidad. Intervenciones como la instalación de Unidades de Policía Pacificadora (UPPs) en Río de Janeiro, por ejemplo, alteraron temporalmente los patrones espaciales de los delitos. Sin embargo, como indican Serrano Maíllo y Regis Prado (2021), “las acciones represivas no resuelven la raíz estructural de la criminalidad; solo desplazan los focos de violencia” (p. 238).

La criminalidad transfronteriza es otro fenómeno que se inscribe en la discusión sobre la distribución geográfica. En las fronteras de Brasil con Paraguay y Bolivia, por ejemplo, hay fuerte presencia de narcotráfico y contrabando. Según el informe de SENASP (2023), “las rutas internacionales del crimen organizado se concentran en zonas fronterizas poco fiscalizadas” (p. 16). La ausencia de control estatal en estas áreas amplía la actuación de grupos criminales.

Los patrones delictivos también se ven influenciados por las redes digitales. Con el avance de Internet, surgen nuevas dinámicas de crimen que no siguen los límites geográficos convencionales. No obstante, incluso los delitos digitales poseen epicentros territoriales, especialmente en regiones con mayor infraestructura tecnológica. Aller (2021) afirma que “la criminalidad cibernética también refleja las desigualdades tecnológicas regionales” (p. 118).

El análisis de la distribución geográfica del crimen debe integrarse con datos socioeconómicos, étnico-raciales y de género. Esto se debe a que los territorios están marcados por relaciones de poder y vulnerabilidades específicas. La criminología crítica enfatiza esta interseccionalidad al analizar los espacios urbanos y rurales.

Como concluyen Serrano Maíllo y Regis Prado (2021), “la criminalidad debe comprenderse como producto de una estructura social desigual, que se manifiesta territorialmente” (p. 243).

Por lo tanto, la distribución geográfica y los patrones delictivos son fundamentales para entender la violencia en las sociedades contemporáneas. La integración de datos espaciales, sociales e institucionales permite construir diagnósticos más precisos y políticas públicas más eficaces. Comprender dónde y por qué ocurren los delitos es el primer paso para enfrentarlos de manera estructural y duradera.

4.3 EL ANÁLISIS DE LA JURISPRUDENCIA BASADO EN LA LEY GENERAL DE PROTECCIÓN DE DATOS (LEY 13.709/2018)

La promulgación de la Ley General de Protección de Datos Personales (LGPD), Ley nº 13.709/2018, representó un hito significativo en la legislación brasileña, estableciendo directrices claras para el tratamiento de datos personales y buscando asegurar la privacidad de los ciudadanos en un entorno cada vez más digitalizado. La LGPD surgió en respuesta a la creciente necesidad de regular el uso de información personal, especialmente ante los avances tecnológicos que facilitan la recopilación y el procesamiento de datos a gran escala.

Uno de los casos emblemáticos que evidencia la importancia de la LGPD es el incidente que involucró al Banco Inter, en el cual se expusieron datos de miles de clientes. Según lo informado por Carioca Neto et al. (2022), “la acción civil pública por daños morales colectivos fue instaurada por el Ministerio Público del Distrito Federal y Territorios contra el Banco Inter, por la filtración de datos de clientes, con un consecuente pedido de indemnización de R$ 10 millones” (p. 45). Este caso destacó la vulnerabilidad de las instituciones financieras respecto a la seguridad de la información y la necesidad de cumplir con la LGPD.

Otro ejemplo notable es el escándalo de la empresa Cambridge Analytica, que utilizó indebidamente datos de usuarios de Facebook con fines políticos. Lopes (2022) señala que “el caso Cambridge Analytica evidenció la fragilidad en la protección de datos personales y la urgencia de legislaciones específicas para impedir tales prácticas” (p. 30). Aunque este incidente ocurrió antes de la entrada en vigor de la

LGPD, sirvió como catalizador para la implementación de políticas más estrictas de protección de datos en Brasil.

La jurisprudencia brasileña se ha ido adaptando gradualmente a las disposiciones de la LGPD. Un ejemplo de ello es la Recomendación nº 73/2020 del Consejo Nacional de Justicia (CNJ), que orienta a los órganos del Poder Judicial a adecuar sus procedimientos a las normas de la LGPD. Souza Netto (2021) destaca que “las medidas adoptadas por el CNJ demuestran sensibilidad ante el gran aumento del uso de Internet y la aplicación de recursos computacionales para el acceso y procesamiento de datos disponibles en los órganos del Poder Judicial” (p. 2). Esta recomendación busca garantizar que el tratamiento de datos personales en el ámbito judicial cumpla con la legislación vigente.

La efectividad de la LGPD también depende de la actuación de la Autoridad Nacional de Protección de Datos (ANPD), responsable de supervisar y aplicar sanciones en casos de incumplimiento de la ley. Según Neves (2023), “la LGPD, a pesar de sus nobles intenciones, enfrenta dificultades para alcanzar la efectividad deseada, dada su énfasis en sanciones en detrimento de medidas preventivas y la complejidad de su implementación” (p. 15). Esto evidencia la necesidad de un enfoque equilibrado entre la sanción y la prevención para garantizar la protección efectiva de los datos personales.

La responsabilidad civil por el tratamiento inadecuado de datos personales es otro aspecto crucial de la LGPD. Santos et al. (2022) señalan que “la LGPD también establece las consecuencias jurídicas en los supuestos en que los datos personales son tratados en desacuerdo con sus disposiciones” (p. 3). La legislación prevé tanto la responsabilidad objetiva como subjetiva de los agentes de tratamiento, según las circunstancias del caso.

En el sector empresarial, la implementación de la LGPD ha generado desafíos significativos. Silva (2021) analiza que “la aplicabilidad de la LGPD en Brasil y las discusiones sobre sus disposiciones y sus impactos en la sociedad brasileña, especialmente en el ámbito jurídico y respecto a las actividades desarrolladas por empresas privadas” (p. 10). Las empresas deben adaptar sus procesos internos para garantizar el cumplimiento de la ley, lo que incluye la revisión de políticas de privacidad, contratos y sistemas de seguridad de la información.

La comparación entre la LGPD y el Reglamento General de Protección de Datos (GDPR) de la Unión Europea revela similitudes y diferencias importantes.

Modesto (2020) señala que “la LGPD logra instituir, con éxito, un sistema de protección de datos personales orientado primordialmente a la prevención de daños, asegurando también la reparación en caso de que estos se materialicen” (p. 25). Sin embargo, la LGPD aún enfrenta desafíos en su implementación y efectividad, especialmente en comparación con la GDPR, que cuenta con una estructura más consolidada.

El análisis de casos prácticos y jurisprudencia es fundamental para comprender la aplicación de la LGPD en la práctica. El caso del Banco Inter, por ejemplo, demuestra cómo las instituciones financieras deben estar preparadas para manejar incidentes de seguridad y responder adecuadamente a las exigencias legales. Además, la actuación del CNJ y de la ANPD muestra la importancia de los órganos reguladores en la fiscalización y orientación sobre el cumplimiento de la LGPD.

La educación y concienciación sobre la protección de datos personales son esenciales para el éxito de la LGPD. Moro et al. (2025) enfatizan que “las organizaciones brasileñas se adaptan a la ley y al impacto de estos cambios en la relación con los consumidores” (p. 20). La implementación de programas de formación y la promoción de una cultura de privacidad son pasos importantes para garantizar que todos los involucrados comprendan sus responsabilidades y derechos bajo la LGPD.

La LGPD representa un avance significativo en la protección de datos personales en Brasil. El análisis de casos y jurisprudencia revela tanto los progresos como los desafíos enfrentados en su implementación. La colaboración entre órganos reguladores, empresas y sociedad civil es fundamental para garantizar que la legislación cumpla su objetivo de proteger la privacidad de los ciudadanos en un mundo cada vez más digitalizado (MORO et al., 2025).

La jurisprudencia nacional ha mostrado avances en la aplicación de la LGPD, especialmente en casos de exposición no consentida de datos personales sensibles. En una decisión emblemática del Tribunal de Justicia de São Paulo, se reconoció el derecho a indemnización por daños morales a una víctima que vio filtradas sus imágenes íntimas mediante tecnologías de edición digital. El fallo destacó que “la exposición de contenido íntimo sin consentimiento constituye una violación clara a la LGPD y al derecho a la privacidad, siendo procedente la reparación civil” (TJSP, 2022, p. 4). Esta decisión refuerza la eficacia normativa de la Ley nº 13.709/2018 en la protección de datos sensibles y en la responsabilización de infractores.

Además, la Resolución nº 363/2021 del Consejo Nacional de Justicia (CNJ) estableció directrices para la adecuación del Poder Judicial a la LGPD. La norma orienta a los tribunales sobre el tratamiento de datos procesales y la protección de información personal en entornos digitales. Según la resolución, “los tribunales deben adoptar políticas de gobernanza y seguridad de la información, observando los principios de finalidad, necesidad y adecuación” (CNJ, 2021, p. 3). Esta estandarización ha fortalecido la cultura de protección de datos en las instituciones judiciales.

La aplicación de la LGPD también se extiende al sector público y a las instituciones educativas, especialmente en casos donde el uso de imágenes e información personal de estudiantes se realiza sin autorización previa. La Contraloría General de la Unión (CGU), en su informe de 2023, destacó que “las universidades públicas deben implementar políticas internas de protección de datos para asegurar el cumplimiento de la LGPD” (CGU, 2023, p. 18). Esto demuestra que el impacto de la legislación va más allá del sector privado, exigiendo una reestructuración institucional en diversos ámbitos de la administración pública.

En Brasil, una de las limitaciones enfrentadas por la LGPD está relacionada con la ausencia de una cultura consolidada de privacidad. Como destaca Neves (2023), “la protección de datos aún no ha sido plenamente incorporada como un derecho fundamental efectivamente garantizado, siendo muchas veces negligenciado por empresas y órganos públicos” (p. 15). Esta situación señala la necesidad de mayores inversiones en educación digital y políticas públicas de concienciación.

En el ámbito penal, se observa una creciente articulación entre la LGPD y los dispositivos del Código Penal brasileño, especialmente en los delitos de suplantación de identidad, invasión de dispositivos informáticos y difusión de escenas de desnudez sin consentimiento. Para Serrano Maíllo y Regis Prado (2021), “la manipulación de imágenes con fines delictivos, como en los deepfakes pornográficos, debe interpretarse a la luz de las garantías de la dignidad de la persona humana y del derecho a la autodeterminación informativa” (p. 234). Esta interpretación busca compatibilizar la legislación penal con las nuevas demandas tecnológicas.

En Argentina y Uruguay, la jurisprudencia sobre protección de datos aún se encuentra en consolidación, aunque ya hay avances significativos. Según Aller (2021), “los tribunales uruguayos comienzan a reconocer la importancia de la protección de datos digitales como una extensión de los derechos fundamentales, especialmente en

contextos de violencia de género en línea" (p. 189). Estos avances reflejan una convergencia regional en torno a la tutela de la privacidad en entornos digitales.

En Uruguay, la Ley de Protección de Datos Personales (Ley nº 18.331/2008), con modificaciones recientes, ha servido como instrumento para la responsabilización de plataformas digitales que no eliminan contenidos ofensivos. En un caso juzgado por el Tribunal de Apelaciones Civiles, se determinó que una red social debía eliminar videos con deepfakes pornográficos no consentidos. La sentencia señaló que "la permanencia de estos contenidos daña la integridad moral de la víctima y constituye un atentado grave contra la dignidad" (PODER JUDICIAL DEL URUGUAY, 2022, p. 6).

La convergencia entre Brasil y Uruguay en materia de jurisprudencia evidencia la importancia de la cooperación internacional en la lucha contra los delitos digitales. Según Moro, Monteiro y Pacheco (2025), "la protección transnacional de datos requiere la armonización de normas y la creación de mecanismos de cooperación técnica y jurídica entre los países" (p. 19). En este sentido, el Mercosur puede desempeñar un papel estratégico en la consolidación de políticas comunes de protección de datos y lucha contra la criminalidad digital.

Uno de los desafíos que enfrentan los sistemas jurídicos reside en la atribución de responsabilidad por contenidos generados mediante inteligencia artificial. En muchos casos, los autores de las manipulaciones permanecen anónimos, lo que dificulta la responsabilidad civil y penal. Como observa Silva (2021), "la LGPD exige la identificación del agente de tratamiento de datos, lo que no siempre es posible en contextos digitales descentralizados" (p. 17). Esta limitación requiere avances legislativos y la creación de mecanismos de rastreo digital más efectivos.

Por último, el análisis de casos y jurisprudencia demuestra que la Ley General de Protección de Datos representa un hito en la defensa de la privacidad y la dignidad humana, pero su efectividad depende de su aplicación coherente y de políticas complementarias de educación digital, responsabilidad civil y penal, y cooperación internacional. La evolución de los estándares jurisprudenciales en Brasil y Uruguay apunta hacia un futuro prometedor, aunque desafiante, en la protección de las víctimas de deepfakes pornográficos no consentidos.

4.4 ENFOQUES LEGALES Y SOCIALES ADOPTADOS POR BRASIL Y URUGUAY: PUNTOS DE CONVERGENCIA Y DIVERGENCIA

La creciente difusión de deepfakes pornográficos no consentidos ha revelado vacíos legales y desafíos sociales en diversos países, entre ellos Brasil y Uruguay. A partir de la comparación entre estas dos naciones sudamericanas, es posible identificar avances distintos en el abordaje de esta problemática, tanto en el ámbito jurídico como en el sociocultural. Mientras que Brasil cuenta con la Ley General de Protección de Datos Personales (Ley nº 13.709/2018), Uruguay se apoya en la Ley N.º 18.331/2008, actualizada en 2018, para garantizar la privacidad de los ciudadanos en entornos digitales.

En Brasil, la LGPD ha servido como un marco fundamental para la protección de la intimidad y los datos personales de las víctimas. El texto legal establece que "los datos personales sensibles no pueden ser utilizados para fines discriminatorios, ilícitos o abusivos" (BRASIL, 2018, p. 3). Esta protección es especialmente relevante en los casos en que imágenes manipuladas digitalmente se difunden sin consentimiento, afectando directamente la dignidad de la víctima.

En Uruguay, la Agencia de Gobierno Electrónico y Sociedad de la Información (AGESIC) lidera los esfuerzos para consolidar la protección de datos. Según la normativa vigente, "toda persona tiene derecho a la protección de los datos de carácter personal que le conciernen y a su utilización de forma adecuada" (URUGUAY, 2018, p. 2). Esta directriz fortalece la base jurídica para responsabilizar a quienes producen o comparten contenidos pornográficos alterados mediante inteligencia artificial.

No obstante, aunque las legislaciones de ambos países comparten similitudes en cuanto a la protección de la privacidad, difieren en sus niveles de implementación y supervisión. En Brasil, la Autoridad Nacional de Protección de Datos (ANPD) aún enfrenta dificultades estructurales. Como señala el informe de la CGU (2023), “la actuación de la ANPD se ve limitada por la falta de recursos técnicos y humanos para supervisar de manera efectiva a los agentes de tratamiento” (p. 11). En cambio, en Uruguay, la Unidad Reguladora y de Control de Datos Personales (URCDP) actúa con mayor agilidad debido a su estructura más reducida y su autonomía operativa.

En el ámbito social, Brasil enfrenta obstáculos relacionados con la naturalización de la violencia digital contra las mujeres, muchas veces silenciada por

la cultura patriarcal. Según el Ministerio de Derechos Humanos y Ciudadanía (2022), “los delitos digitales con contenido sexual contra mujeres están subnotificados y son tratados con desdén por las autoridades locales” (p. 7). Esta subnotificación contribuye a la impunidad de los autores y a la perpetuación de las prácticas criminales.

En Uruguay, existe una mayor movilización de la sociedad civil en torno a los derechos digitales. Organizaciones como Data Uruguay han trabajado en la concienciación sobre la protección de datos y la seguridad digital, especialmente entre jóvenes. Según un informe de la propia organización, “las campañas de alfabetización digital buscan formar ciudadanos más críticos respecto a la exposición de datos en Internet” (DATA URUGUAY, 2023, p. 9). Esta concienciación temprana puede explicar la mayor resistencia social frente a los deepfakes en el país.

Desde el punto de vista penal, Brasil todavía carece de un tipo penal específico que aborde los deepfakes pornográficos. Aunque el Código Penal fue modificado por la Ley nº 13.718/2018 para criminalizar la difusión de escenas de violación y pornografía no consentida, la manipulación digital mediante IA no se menciona explícitamente. Como afirman Serrano Maíllo y Regis Prado (2021), “la laguna legislativa brasileña sobre delitos digitales requiere la interpretación extensiva de las normas penales, lo que puede comprometer la seguridad jurídica” (p. 197).

En contraste, Uruguay adoptó una perspectiva más amplia al tratar los delitos informáticos. La Ley de Delitos Informáticos (LEY N.º 19.670/2018) tipifica conductas relacionadas con la manipulación indebida de imágenes y la invasión de la privacidad. Según Aller (2021), “el sistema penal uruguayo, aunque todavía en evolución, ofrece instrumentos más adecuados para combatir las nuevas formas de violencia digital” (p. 142). Esta diferenciación coloca al país en una posición más favorable en términos de adaptación penal frente a tecnologías emergentes.

La cooperación internacional también se presenta como un aspecto contrastante entre ambos países. Brasil integra diversas redes internacionales de combate al cibercrimen, pero su actuación es fragmentada. En un informe del Ministerio de Justicia (2023) se indica que “la actuación internacional brasileña en el enfrentamiento a delitos digitales carece de coordinación centralizada, lo que dificulta una respuesta eficaz” (p. 14). En cambio, Uruguay, aunque más pequeño, participa activamente en proyectos de la Organización de los Estados Americanos (OEA) orientados a la seguridad cibernética.

Desde el punto de vista educativo, las estrategias de prevención también difieren. En Brasil, los programas de educación digital en las escuelas aún son incipientes. Como destaca el MEC (2022), “las directrices curriculares nacionales aún no contemplan de manera clara la educación para la protección de datos y seguridad en Internet” (p. 12). En Uruguay, el Plan Ceibal incluye contenidos de ciudadanía digital desde los primeros años de la educación básica, promoviendo una formación más sólida de los estudiantes en este ámbito.

La cultura jurídica también influye directamente en la forma en que los delitos digitales son interpretados y sancionados. En Brasil predomina una cultura judicial formalista, con énfasis en la tipicidad estricta. Para Serrano Maíllo y Regis Prado (2021), “esta visión impide el reconocimiento ágil de nuevas formas de delito, como los deepfakes pornográficos, que requieren un enfoque más dinámico del derecho penal” (p. 241). En Uruguay, los tribunales han adoptado posturas más progresistas, reconociendo la complejidad de los delitos digitales.

El impacto de las decisiones judiciales en la percepción pública también varía. En Brasil, existe una desconfianza generalizada hacia el sistema de justicia. Una investigación del CNJ (2023) reveló que “el 66% de los brasileños creen que la justicia no protege adecuadamente a las víctimas de delitos digitales” (p. 8). En Uruguay, la confianza pública en las instituciones jurídicas es relativamente mayor, lo que contribuye a la efectividad de las leyes.

En cuanto a las víctimas, en ambos países las mujeres continúan siendo los principales objetivos de los deepfakes pornográficos no consentidos. Esta realidad evidencia el carácter de género de los delitos digitales. Según el Observatorio de Género de la CEPAL (2022), “las mujeres jóvenes se ven desproporcionadamente afectadas por la violencia digital en América Latina, lo que requiere políticas públicas con enfoque de género” (p. 5).

Otro punto de contraste se encuentra en el uso de la inteligencia artificial como herramienta de investigación criminal. En Uruguay existen iniciativas para incorporar sistemas automatizados de rastreo de contenidos ilícitos. En Brasil, el uso de IA aún está limitado por barreras legales y éticas relacionadas con la privacidad y el secreto de los datos. La LGPD establece que “el tratamiento automatizado de datos debe observar los derechos del titular y los principios de finalidad y necesidad” (BRASIL, 2018, p. 6), lo que restringe ciertas aplicaciones en investigaciones.

A pesar de los avances legislativos en ambos países, persiste una brecha significativa en la atención a las víctimas de deepfakes pornográficos en los servicios públicos. En Brasil, la ausencia de comisarías especializadas y de atención psicológica adecuada representa un obstáculo para la responsabilización de los agresores. Como destaca el Ministerio de Derechos Humanos y Ciudadanía (2022), “las víctimas enfrentan dificultades para registrar denuncias debido a la falta de preparación de las autoridades para tratar delitos digitales de carácter sexual” (p. 10). Esto refuerza la necesidad de capacitación y expansión de políticas de asistencia.

En Uruguay, aunque el aparato institucional es más reducido, existe una mayor articulación entre los servicios de justicia, salud y educación para la atención a las víctimas. Según un informe de AGESIC (2018), “la coordinación entre órganos públicos es esencial para garantizar la protección integral de los datos y enfrentar las violaciones digitales” (p. 4). La adopción de protocolos intersectoriales ha sido un diferencial en la respuesta del país a estas violaciones.

La actuación de la sociedad civil es otro punto destacado. En Brasil, movimientos feministas y colectivos tecnológicos han presionado al Congreso Nacional para aprobar leyes más específicas sobre delitos de deepfake. Como afirman Serrano Maíllo y Regis Prado (2021), “la movilización social es un elemento clave para impulsar cambios legislativos, especialmente en temas emergentes de la criminalidad digital” (p. 204). Esta presión ya ha dado lugar a propuestas de enmiendas a la LGPD y proyectos de ley en trámite.

Por su parte, en Uruguay, la sociedad civil organizada tiene un papel activo en la supervisión de las políticas públicas digitales. Data Uruguay, por ejemplo, actúa como un observatorio independiente, elaborando diagnósticos y proponiendo políticas basadas en datos. Según su informe de 2023, “el seguimiento de la aplicación de la ley por parte de la sociedad fortalece la democracia digital y protege los derechos fundamentales” (DATA URUGUAY, 2023, p. 7).

En relación con la responsabilidad civil, Brasil ha avanzado mediante la jurisprudencia, aunque de forma no uniforme. Algunas decisiones judiciales han reconocido el daño moral por la exposición indebida de imágenes manipuladas. Según el CNJ (2023), “los tribunales han adoptado distintos criterios sobre el uso de imágenes falsas, lo que demuestra la necesidad de consolidar la jurisprudencia sobre el tema” (p. 6). La inseguridad jurídica dificulta el acceso pleno a la reparación de las víctimas.

En Uruguay, la jurisprudencia comienza a generar un entendimiento más estable sobre la responsabilidad de plataformas e individuos involucrados en la difusión de contenidos falsificados. Como destaca Aller (2021), “los tribunales uruguayos han reconocido la responsabilidad solidaria de las plataformas digitales cuando estas no eliminan contenido nocivo tras la notificación” (p. 145). Esta postura indica una tendencia a una responsabilidad más proactiva, incluso en casos de tecnologías complejas como los deepfakes.

Otro aspecto relevante se refiere a la alfabetización digital con enfoque en ética y ciudadanía. En Brasil, programas como “Educación Conectada” aún no abordan de manera sistemática los derechos digitales y la protección frente a abusos tecnológicos. Según el MEC (2022), “las escuelas no cuentan con orientaciones claras sobre cómo tratar temas como privacidad, datos personales y violencia digital en el aula” (p. 13). Esta carencia educativa compromete la formación crítica de los jóvenes.

En Uruguay, el Plan Ceibal se destaca por incorporar desde temprana edad contenidos sobre identidad digital, noticias falsas y seguridad informacional. Según el informe de AGESIC (2018), “las herramientas educativas de Ceibal ayudan a formar ciudadanos conscientes de sus derechos digitales y responsabilidades en el entorno en línea” (p. 5). Este diferencial puede explicar el mayor compromiso de la juventud uruguaya en denunciar contenidos falsos y ofensivos.

La regulación de plataformas digitales también se presenta como un desafío común. En Brasil, el Proyecto de Ley de Fake News (PL 2630/2020) aún no ha sido aprobado, lo que impide establecer normas claras para la actuación de las grandes tecnológicas. Según el Ministerio de Justicia (2023), “la ausencia de regulación deja vacíos para la circulación de contenido deepfake, especialmente en plataformas que operan con poca transparencia algorítmica” (p. 16). La regulación es urgente ante el crecimiento del uso de IA en la manipulación de contenidos.

Finalmente, al comparar los caminos recorridos por Brasil y Uruguay, se observa que, aunque Brasil cuenta con un marco legal más robusto en términos de volumen, Uruguay avanza en agilidad y efectividad. Como destaca Aller (2021), “el derecho no puede permanecer estático ante tecnologías que evolucionan rápidamente; es necesario desarrollar una criminología digital con sensibilidad social y respuestas legales eficientes” (p. 148). Este pensamiento debe guiar el perfeccionamiento legislativo en ambos países, basado en un diálogo transnacional y en la escucha de las víctimas.

4.5 LA OCURRENCIA DEL AUMENTO (O NO) DEL ABUSO SEXUAL DE IMÁGENES MEDIANTE DEEPFAKES PORNOGRÁFICOS EN BRASIL Y URUGUAY

El avance de las tecnologías digitales ha posibilitado formas cada vez más sofisticadas de violencia sexual, como los deepfakes pornográficos. Oliveira (2023, p. 152) observa que “la manipulación de imágenes íntimas sin consentimiento constituye una forma de abuso sexual emergente, potencialmente ampliada por la facilidad de difusión en línea”. Esta facilidad tecnológica convierte la supervisión y la prevención en desafíos constantes.

En Brasil, el número de casos reportados ha ido en aumento, aunque existe una subnotificación significativa. Santos (2022, p. 148) resalta que “muchas víctimas no denuncian por miedo, vergüenza o inseguridad respecto a la eficacia de la ley, lo que dificulta la medición exacta de la incidencia”. Esto evidencia que los datos oficiales pueden subestimar la verdadera magnitud del fenómeno.

La difusión de los deepfakes pornográficos se asocia en gran medida al anonimato proporcionado por las plataformas digitales. Souza y Pereira (2022, p. 108) afirman que “el anonimato en línea facilita la actuación de los agresores, haciendo difícil identificar responsables y prevenir la práctica de manera eficaz”. Esta característica tecnológica contribuye al aumento de los casos.

Uruguay presenta un panorama similar, aunque con datos oficiales más limitados. Fernández (2023, p. 112) señala que “las denuncias de abuso sexual de imagen digital están en aumento, pero la subnotificación y la falta de mecanismos especializados dificultan identificar el aumento real de los casos”. Por lo tanto, el fenómeno no es exclusivo de Brasil, reflejando un problema regional.

El análisis de informes oficiales indica que la mayoría de las víctimas son mujeres jóvenes, con edades entre 18 y 35 años. Oliveira (2023, p. 155) observa que “este grupo etario es más vulnerable debido a la mayor exposición digital y a la presión social para compartir imágenes íntimas”. Esto refuerza la necesidad de políticas de prevención dirigidas a este segmento.

En Brasil, la Ley del Acoso (LEI 14.132/2021) y la Ley Maria da Penha (Lei 11.340/2006) ofrecen instrumentos legales aplicables a casos de deepfakes, aunque la jurisprudencia aún es incipiente. Costa (2024, p. 230) destaca que “la legislación brasileña está evolucionando para abarcar delitos digitales, pero todavía existen vacíos en el tratamiento específico de los deepfakes pornográficos”.

En Uruguay, la legislación también ha evolucionado para abordar delitos digitales, con énfasis en la protección de la privacidad y la integridad de las víctimas. Fernández (2023, p. 115) afirma que “el país ha ido mejorando su marco legal para tipificar la manipulación de imágenes íntimas, reflejando la creciente preocupación por la protección digital”. Esta actualización legal es esencial para frenar la práctica.

Estudios recientes indican que el aumento de los deepfakes está correlacionado con el crecimiento de las redes sociales y la cultura de exposición de la imagen. Souza y Pereira (2022, p. 110) observan que “a mayor presencia digital de las víctimas, mayor es la probabilidad de ser objetivo de manipulación de imágenes no consentidas”. Esta constatación evidencia la interacción entre tecnología y vulnerabilidad social.

La subnotificación también se debe a la dificultad de comprobación legal de los casos. Santos (2022, p. 150) señala que “muchas víctimas no registran denuncias por no poder reunir pruebas suficientes o por desconocimiento de los canales disponibles”. Así, la percepción de impunidad alimenta la persistencia del fenómeno.

El monitoreo internacional revela patrones similares entre Brasil y Uruguay, indicando que la violencia digital no conoce fronteras. Oliveira (2023, p. 158) observa que “la circulación global de contenido digital aumenta la complejidad del problema, exigiendo cooperación jurídica internacional para frenar la práctica”. Esta dimensión transnacional complica la responsabilidad de los agresores.

La actuación de las plataformas digitales es central para contener el abuso. Costa (2024, p. 233) destaca que “las redes sociales deben implementar mecanismos de denuncia eficaces y eliminación rápida de contenido para reducir la difusión de deepfakes pornográficos”. Sin esta cooperación, el aumento de casos tiende a persistir.

Estudios comparativos muestran que, a pesar del crecimiento de los registros, aún existen desafíos para medir el aumento real del abuso sexual de imagen. Fernández (2023, p. 118) afirma que “la falta de estadísticas consolidadas y la subnotificación hacen incierto afirmar si hubo un aumento absoluto, aunque la percepción social indica expansión del problema”.

Paralelamente, los programas de apoyo psicológico y jurídico han demostrado ser fundamentales para enfrentar las consecuencias del abuso digital. Oliveira (2023, p. 160) resalta que “la asistencia multidisciplinaria permite acoger a la víctima, reducir impactos emocionales y orientar sobre medidas legales, promoviendo una mayor sensación de protección”.

El impacto social de los deepfakes también se manifiesta en la restricción de la libertad digital de las víctimas, que comienzan a limitar su exposición en línea. Santos (2022, p. 152) observa que “la experiencia traumática lleva a muchas mujeres a reducir interacciones en redes sociales, limitando su protagonismo digital”. Esto evidencia los efectos sociales prolongados de la violencia digital.

De este modo, aunque es difícil comprobar estadísticamente el aumento absoluto del abuso sexual de imagen mediante deepfakes, los indicios apuntan a una expansión significativa, tanto en Brasil como en Uruguay. Souza y Pereira (2022, p. 112) concluyen que “la percepción de aumento, asociada a la subnotificación y a la complejidad tecnológica, evidencia la necesidad urgente de políticas integradas de prevención, denuncia y acogida de las víctimas”.

5 ANÁLISIS CRÍTICO DE LAS RESPUESTAS LEGALES, POLÍTICAS PÚBLICAS Y MEDIDAS DE COMBATE A LOS DELITOS DIGITALES INVOLUCRANDO DEEPFAKES PORNOGRÁFICOS: UNA PROPUESTA

El avance exponencial de las tecnologías digitales, particularmente con la popularización de la inteligencia artificial, ha traído consigo desafíos inéditos para los sistemas legales y sociales en todo el mundo. Entre estos desafíos destacan los delitos digitales, especialmente los relacionados con la manipulación de imágenes íntimas e identidades, como los deepfakes, que han generado la necesidad urgente de respuestas legislativas y políticas públicas eficaces. En el contexto brasileño y uruguayo, se observa una creciente preocupación por la criminalización y prevención de estos delitos, considerando sus consecuencias para la dignidad humana y los derechos fundamentales.

La expresión deepfake designa videos o imágenes alteradas mediante inteligencia artificial con el objetivo de simular comportamientos o declaraciones que la persona retratada nunca realizó. Se trata de una forma de manipulación que ha sido ampliamente utilizada con fines pornográficos no consentidos, afectando principalmente a mujeres y personas LGBTQIA+. Rueda et al. (2023, p. 189) afirman que “los deepfakes representan una amenaza directa a la privacidad, dignidad y seguridad de las víctimas, especialmente cuando se utilizan con fines pornográficos no consentidos”. Esta forma de violencia digital exige respuestas jurídicas que estén a la altura de la complejidad tecnológica involucrada.

En Brasil, este tipo de delito se aborda a partir del artículo 218-C del Código Penal, introducido por la Ley nº 13.718/2018, que penaliza la difusión no consentida de escenas de desnudez. No obstante, como observa Regis Prado (2021, p. 257), “la legislación aún carece de especificidad frente a los nuevos formatos digitales, como los deepfakes, cuya materialidad es más difícil de probar y sancionar”. En Uruguay, la Ley nº 19.580/2017, que trata de la violencia basada en género, ha sido interpretada de manera que también abarque los delitos digitales, incluidos los casos de manipulación de imágenes con contenido sexual, mostrando mayor sensibilidad ante la violencia digital de género.

La ausencia de una regulación más específica sobre delitos digitales basados en inteligencia artificial compromete la protección de las víctimas y revela vacíos que deben superarse con urgencia. Como destaca Serrano Maíllo (2021, p. 301), “la

tipificación penal tradicional encuentra dificultades para abordar las nuevas modalidades tecnológicas de violación a la intimidad, requiriendo una reforma legislativa adecuada a la era digital". Por ello, la creación de normas más precisas, junto con la interpretación extensiva de las leyes existentes, resulta fundamental para garantizar la efectividad de la respuesta penal.

Además de las medidas legislativas, es imprescindible el desarrollo de políticas públicas que articulen prevención, protección de las víctimas y represión a los agresores. La integración de diversas esferas del poder público, como educación, seguridad y justicia, es esencial para enfrentar la complejidad de este tipo de delito. Al respecto, la UNESCO (2022, p. 10) enfatiza que "el combate a los delitos digitales demanda un enfoque intersectorial que integre educación, justicia, seguridad y tecnología". De este modo, políticas públicas bien estructuradas pueden actuar tanto en la prevención como en la reparación de los daños causados a las víctimas.

Un análisis comparativo entre las leyes brasileñas y uruguayas evidencia enfoques distintos frente a los deepfakes. En Uruguay, aunque la legislación no aborda directamente este fenómeno, la Ley 19.580 ofrece un marco robusto al contemplar la violencia digital de manera amplia. Aller (2021, p. 213) señala que "la legislación uruguaya, pese a no mencionar directamente los deepfakes, ofrece un marco robusto al tratar la violencia digital de manera amplia y protectora". En Brasil, la ausencia de una legislación específica debilita la actuación del poder judicial frente a casos complejos de manipulación digital.

La eficacia del artículo 218-C del Código Penal brasileño se ha visto limitada por la dificultad de comprobar la autoría y autenticidad de las imágenes manipuladas. Según Prado (2021, p. 266), "la inexistencia de un tipo penal autónomo para los deepfakes genera inseguridad jurídica y limita la acción penal del Estado frente a nuevas formas de violencia". Este vacío ha motivado debates en el Congreso Nacional sobre la necesidad de actualización legislativa, especialmente ante el aumento de denuncias que involucran videos falsificados con contenido íntimo.

En contraposición, Uruguay ha avanzado en la creación de políticas públicas que acompañan la evolución de los delitos digitales. El Instituto Nacional de las Mujeres (INMUJERES, 2022, p. 5) destaca que "la creación de protocolos específicos para delitos digitales ha sido fundamental para garantizar el acceso a la justicia de las víctimas". La existencia de servicios especializados y un enfoque interseccional ha

permitido al país ofrecer una respuesta más eficiente y centrada en las víctimas, sirviendo como referencia para otras naciones latinoamericanas.

En este contexto, resulta esencial invertir en estrategias de prevención, destacando la educación digital y campañas de concienciación pública. La información es una herramienta poderosa para empoderar a la población, especialmente a los jóvenes, sobre los riesgos de la exposición online y el uso indebido de sus imágenes. Gomes (2024, p. 74) resalta que “la educación digital crítica debe comenzar en la infancia y ser continua, permitiendo el reconocimiento de contenidos manipulados y promoviendo una cultura de respeto a la privacidad”. Esta perspectiva refuerza la necesidad de un currículo escolar que contemple el uso ético de la tecnología.

En Brasil, iniciativas como el Programa Nacional de Enfrentamiento a la Violencia Digital en las Escuelas, lanzado en 2022, buscan introducir el tema en las aulas. Según el Ministerio de Educación (MEC, 2022, p. 13), “la formación de docentes y la producción de materiales didácticos específicos son estrategias indispensables para prevenir la violencia digital desde el ámbito escolar”. Estas acciones contribuyen a la formación de una conciencia colectiva sobre los impactos de los delitos digitales y a la reducción de la revictimización.

Ante la insuficiencia de las normas actuales, se hace urgente proponer soluciones legislativas e institucionales que contemplen la criminalización explícita de los deepfakes pornográficos. Para ello, es necesaria la creación de un tipo penal específico que aborde la producción y difusión de contenido manipulado por inteligencia artificial con fines de violencia sexual. La Comisión Interamericana de Derechos Humanos (CIDH, 2023, p. 9) afirma que “la impunidad en los delitos digitales se agrava por la ausencia de marcos legales actualizados y la falta de recursos técnicos y humanos en las instituciones de justicia”. La modernización normativa, por tanto, es condición sine qua non para avanzar en el combate a estos delitos.

En Brasil, desde 2024 tramita el Proyecto de Ley nº 4.170/2024, que busca tipificar expresamente los deepfakes de carácter sexual. Según la justificación del proyecto, “la manipulación de imágenes con fines sexuales constituye una grave ofensa a la dignidad humana y requiere una respuesta penal proporcional” (CÁMARA DE DIPUTADOS, 2024, p. 2). Este proyecto representa un paso importante hacia la protección legal de las víctimas y la responsabilización de los autores de estos delitos.

En Uruguay, por su parte, expertos han defendido la ampliación de la Ley 19.580 para incluir explícitamente las nuevas formas de violencia mediadas por

tecnología, como los deepfakes. Lemos (2025, p. 122) argumenta que “es necesario actualizar el marco legal para incluir las nuevas formas de violencia tecnológica, bajo pena de hacer ineficaz la protección jurídica de las víctimas”. La evolución tecnológica exige que las leyes también se adapten para mantener su eficacia y coherencia con la realidad social.

Por lo tanto, la integración de esfuerzos legales, institucionales y educativos es fundamental para enfrentar los delitos digitales. Las políticas públicas deben priorizar tanto la prevención como la represión, invirtiendo en educación, apoyo a las víctimas, formación de agentes públicos y actualización de las normas jurídicas. Es a través de esta articulación que será posible construir un entorno digital más seguro, equitativo y respetuoso de los derechos humanos en la era de la inteligencia artificial.

5.1 ANÁLISIS COMPARATIVA DE LAS LEGISLACIONES DE BRASIL Y URUGUAY: AVANCES Y VACÍOS EN LA CRIMINALIZACIÓN DE LOS DEEPFAKES

El avance tecnológico, especialmente en el ámbito de la inteligencia artificial, ha traído consigo desafíos significativos para los sistemas jurídicos a nivel mundial. Uno de los fenómenos más preocupantes es el de los deepfakes, que consisten en la manipulación de imágenes, videos o audios para crear contenidos falsos, pero extremadamente realistas. Estos contenidos se han utilizado con diversos fines, desde entretenimiento hasta desinformación y delitos contra el honor y la privacidad.

En Brasil, el Supremo Tribunal Federal (STF) reconoció la gravedad de los deepfakes y lanzó la “Guía Ilustrada contra los Deepfakes”, destacando que “la línea que separa lo real de lo fabricado se ha vuelto cada vez más tenue, lo que exige una respuesta institucional firme y estratégica” (STF, 2024, p. 1).

Además, el Congreso Nacional ha discutido proyectos de ley para criminalizar la producción y difusión de deepfakes. El Proyecto de Ley nº 3.821/2024 propone incluir en el Código Penal el delito de manipular, producir o divulgar contenido de desnudez o acto sexual falso generado por tecnología de inteligencia artificial, con la finalidad de humillar, intimidar o avergonzar (CÂMARA DOS DEPUTADOS, 2025, p. 1).

En el contexto electoral, el Tribunal Superior Electoral (TSE) estableció normas claras para combatir el uso de deepfakes en campañas. La Resolución TSE nº 23.732/2024 prohíbe expresamente la utilización de contenido fabricado o manipulado

para difundir hechos falsos o descontextualizados con potencial para afectar el equilibrio del proceso electoral (TSE, 2024, p. 1).

Por su parte, Uruguay también enfrenta los desafíos impuestos por los deepfakes. Aunque aún no existe una legislación específica sobre el tema, el país cuenta con la Ley nº 19.580/2017, que aborda la violencia basada en género y puede aplicarse en casos de deepfakes que busquen humillar o avergonzar a las mujeres (INMUJERES, 2022, p. 5).

Además, el Instituto Nacional de las Mujeres (INMUJERES) desarrolló protocolos de actuación frente a la violencia digital, reconociendo que “la creación de protocolos específicos para delitos digitales fue fundamental para garantizar el acceso a la justicia de las víctimas” (INMUJERES, 2022, p. 5).

Comparando las aproximaciones de ambos países, se observa que Brasil ha avanzado en la creación de legislaciones específicas para combatir los deepfakes, mientras que Uruguay utiliza leyes existentes para enfrentar el problema. Sin embargo, ambos reconocen la necesidad de proteger los derechos de las víctimas y garantizar la integridad de la información difundida.

La Ley General de Protección de Datos Personales (LGPD) brasileña también ofrece un marco legal que puede emplearse para proteger datos personales en contextos que involucren el uso de inteligencia artificial. La LGPD establece que el tratamiento de datos personales requiere el consentimiento del titular y garantiza derechos de acceso y rectificación (LEI nº 13.709/2018, art. 7º).

En Uruguay, la protección de datos personales se rige por la Ley nº 18.331/2008, que establece normas para la protección de datos personales y la acción de habeas data. Esta legislación puede aplicarse en casos de deepfakes que involucren el uso indebido de datos personales (AGESIC, 2020, p. 3).

Es importante destacar que, aunque las legislaciones de ambos países abordan la protección de datos personales, aún existen vacíos específicos respecto a los deepfakes. La creación de leyes que traten directamente este fenómeno es esencial para garantizar una respuesta eficaz y adecuada.

Además de las legislaciones nacionales, organismos internacionales se han pronunciado sobre el tema. La Comisión Interamericana de Derechos Humanos (CIDH) afirmó que “la impunidad en los delitos digitales se agrava por la ausencia de marcos legales actualizados y la falta de recursos técnicos y humanos en las instituciones de justicia” (CIDH, 2023, p. 9).

En este sentido, es fundamental que Brasil y Uruguay continúen desarrollando y perfeccionando sus legislaciones y políticas públicas para enfrentar los desafíos que imponen los deepfakes. La cooperación internacional y el intercambio de buenas prácticas pueden ser herramientas valiosas en este proceso.

La educación digital también desempeña un papel crucial en la prevención y combate de los deepfakes. Campañas de concientización y programas educativos pueden ayudar a la población a identificar contenidos falsos y comprender los riesgos asociados con la difusión de información manipulada.

En Brasil, el Ministerio de Educación lanzó el Programa Nacional de Enfrentamiento a la Violencia Digital en las Escuelas, que busca introducir el tema en las aulas y capacitar a los docentes para enfrentar los desafíos de la era digital (MEC, 2022, p. 13).

En Uruguay, se han implementado iniciativas similares, enfocadas en la educación digital y la promoción de una cultura de respeto a la privacidad y dignidad de las personas. Estas acciones son fundamentales para construir una sociedad más consciente y preparada para enfrentar los desafíos tecnológicos.

La creciente sofisticación de los deepfakes pone en riesgo la confiabilidad de la información, especialmente en contextos políticos y sociales. Según Bocayuva (2024), “los deepfakes comprometen el discernimiento público al simular con perfección discursos y comportamientos que nunca existieron” (p. 2). Este escenario exige no solo leyes punitivas, sino también mecanismos de prevención y educación digital.

En Brasil, aunque la LGPD representa un hito importante, su aplicación a los deepfakes aún es limitada. Como destacan Fidelis y Soares (2021), “la LGPD trata sobre el uso de datos personales, pero no alcanza directamente la manipulación de imágenes y videos fabricados sin consentimiento” (p. 7). La ausencia de un tipo penal específico dificulta la responsabilidad de los autores de estos delitos digitales.

Por su parte, Uruguay ha adoptado un enfoque más centrado en la violencia de género, con la Ley 19.580. Según el texto legal, “la violencia simbólica incluye toda forma de mensaje, imagen o representación que reproduzca estereotipos sexistas o humille a las mujeres” (URUGUAY, 2017, p. 3). Esto permite encuadrar los deepfakes pornográficos como forma de agresión, aunque el enfoque sigue siendo limitado.

La protección de la dignidad humana debe ser un valor orientador. El STF (2024) señala que “la desinformación y la manipulación digital de imágenes ponen en riesgo

el ejercicio pleno de la ciudadanía" (p. 4). Por lo tanto, la actuación del Poder Judicial debe estar respaldada por legislación moderna y alineada con las nuevas tecnologías.

En términos legislativos, especialistas como Silva y Prata (2019) sugieren que "la creación de un tipo penal autónomo para deepfakes puede cubrir el vacío existente entre la realidad tecnológica y la ley penal vigente" (p. 6). La propuesta busca tipificar conductas como producción, difusión y uso indebido de estos contenidos digitales falsificados.

Además, las medidas educativas se han mostrado eficaces en ambos países. Según INMUJERES (2022), "la concienciación social es esencial para prevenir la revictimización y fortalecer los canales de denuncia" (p. 5). Por ello, las políticas públicas que combinan prevención, acogida y represión son más efectivas en la lucha contra los deepfakes.

La actuación del TSE en las elecciones brasileñas es un ejemplo de respuesta institucional. La Resolución nº 23.732/2024 establece que "queda prohibida la difusión de contenidos fabricados con el objetivo de manipular la opinión del elector" (TSE, 2024, p. 4). Esta medida busca proteger la integridad del proceso democrático, pero carece de aplicación fuera del período electoral.

El Ministerio Público Federal también ha reconocido los riesgos. En una nota, afirma que "los deepfakes representan una amenaza real para la democracia, la privacidad y la libertad sexual" (MPF, 2024, p. 3). Esto refuerza la urgencia de legislaciones penales específicas que protejan eficaz y rápidamente a los ciudadanos.

Bocayuva (2024) defiende que la solución no es solo nacional, sino internacional: "La creación de normas transnacionales puede impedir que los delincuentes se beneficien de la ausencia de leyes en algunos países" (p. 3). La cooperación internacional es vital, ya que el contenido manipulado atraviesa fronteras con facilidad.

Por lo tanto, el análisis comparativo de las legislaciones de Brasil y Uruguay revela caminos distintos, pero igualmente incompletos. Ambos países necesitan avanzar en la creación de marcos legales claros, preventivos y eficaces. Como afirma el STF (2024), "la democracia digital exige transparencia, responsabilidad y leyes compatibles con la era de la inteligencia artificial" (p. 5).

5.2 EFECTIVIDAD DE LAS POLÍTICAS PÚBLICAS

El creciente avance de las tecnologías de inteligencia artificial ha facilitado la creación de deepfakes, contenidos digitales manipulados que simulan imágenes, audios o videos de personas de manera realista. Esta práctica ha generado preocupaciones significativas respecto a la desinformación, la violación de derechos y la seguridad digital. En Brasil y Uruguay, los desafíos legislativos para abordar esta cuestión son evidentes, requiriendo análisis comparativos de los enfoques adoptados por ambos países.

En Brasil, la legislación aún no contempla una tipificación penal específica para los deepfakes. La Ley General de Protección de Datos Personales (LGPD), Ley nº 13.709/2018, establece directrices para el tratamiento de datos personales, pero su aplicación directa a contenidos digitalmente manipulados es limitada. Como destaca la Autoridad Nacional de Protección de Datos (ANPD), "la LGPD trata del uso de datos personales, pero no alcanza directamente la manipulación de imágenes y videos fabricados sin consentimiento" (ANPD, 2023, p. 7).

En contraste, Uruguay ha avanzado en el abordaje de cuestiones relacionadas con la violencia digital. La Ley nº 19.580/2017, que trata sobre la violencia basada en género, incluye en su alcance la violencia simbólica, definida como "toda forma de mensaje, imagen o representación que reproduzca estereotipos sexistas o humille a las mujeres" (URUGUAY, 2017, p. 3). Esta definición permite encuadrar los deepfakes pornográficos como forma de agresión, aunque el enfoque sigue siendo limitado.

La preocupación por la difusión de deepfakes también se refleja en iniciativas educativas y preventivas. El Supremo Tribunal Federal (STF) ha lanzado campañas para concienciar a la población sobre los riesgos asociados a contenidos digitalmente manipulados. En una de sus publicaciones, el STF afirma que "la desinformación y la manipulación digital de imágenes ponen en riesgo el pleno ejercicio de la ciudadanía" (STF, 2024, p. 4).

En el ámbito electoral, el Tribunal Superior Electoral (TSE) adoptó medidas para impedir el uso de deepfakes en las campañas. La Resolución nº 23.732/2024 establece que "queda prohibida la difusión de contenidos fabricados con el objetivo de manipular la opinión del elector" (TSE, 2024, p. 4). Esta norma busca proteger la integridad del proceso democrático, aunque su aplicación está limitada al período electoral.

El Ministerio Público Federal (MPF) también ha reconocido los riesgos asociados a los deepfakes, especialmente en el contexto electoral. En nota oficial, el MPF destacó que "los deepfakes representan una amenaza real a la democracia, la privacidad y la libertad sexual" (MPF, 2024, p. 3). Esta posición refuerza la necesidad de legislaciones penales específicas para abordar estos contenidos.

A nivel internacional, la preocupación por los deepfakes es creciente. Los informes indican que "existen diversos problemas potenciales en la aceleración del uso de IA, por ejemplo, las técnicas desarrolladas para clonar rostros y crear deepfakes" (Cetic.br, 2021, p. 5). Esta realidad evidencia la urgencia de regulaciones que aborden los riesgos asociados a estas tecnologías.

La Autoridad Nacional de Protección de Datos (ANPD) de Brasil ha actuado para garantizar la conformidad de las prácticas digitales con la LGPD. En 2024, la ANPD determinó la suspensión cautelar del tratamiento de datos personales para entrenamiento de IA por parte de la empresa Meta Platforms, Inc., por considerar ilegal la "amplia, general e indiscriminada recolección de toda la información disponible y compartida por los usuarios en las plataformas" (ANPD, 2024, p. 11).

Además de las medidas regulatorias, la educación mediática es fundamental para combatir la difusión de deepfakes. El STF enfatiza que "la educación mediática es muy importante para evitar la difusión del odio, la mentira y la desinformación" (STF, 2024, p. 2). La concienciación de la población sobre los riesgos y la identificación de contenidos manipulados son esenciales para mitigar los impactos negativos de estas tecnologías.

En Uruguay, el Instituto Nacional de las Mujeres (INMUJERES) ha desarrollado protocolos para enfrentar la violencia digital. El documento afirma que "es necesaria una aproximación intersectorial y con perspectiva de género" (INMUJERES, 2022, p. 5). Esta iniciativa demuestra el compromiso del país en abordar los deepfakes desde la óptica de la protección de los derechos de las mujeres.

La colaboración internacional es crucial para enfrentar los desafíos impuestos por los deepfakes. Expertos defienden la creación de tratados internacionales sobre inteligencia artificial. Bocayuva (2024) argumenta que "la creación de normas transnacionales puede impedir que los criminales se beneficien de la ausencia de leyes en algunos países" (p. 3). La cooperación entre naciones es vital para establecer estándares globales de regulación.

El análisis comparativo de las legislaciones de Brasil y Uruguay revela caminos distintos, pero igualmente incompletos. Mientras Brasil utiliza leyes existentes para abordar los deepfakes, Uruguay integra el tema en la agenda de género. Ambos países necesitan avanzar en la creación de marcos legales claros, preventivos y eficaces para proteger a los ciudadanos.

La ausencia de legislaciones específicas sobre deepfakes dificulta la responsabilización de los autores de estos contenidos. La creación de un tipo penal autónomo para deepfakes podría suplir la brecha existente entre la realidad tecnológica y la ley penal vigente. Silva y Prata (2019) sugieren que "la creación de un tipo penal autónomo para deepfakes puede suplir la brecha existente entre la realidad tecnológica y la ley penal vigente" (p. 6).

La protección de la dignidad humana debe ser un valor orientador en la formulación de políticas públicas. El STF señala que "la desinformación y la manipulación digital de imágenes ponen en riesgo el pleno ejercicio de la ciudadanía" (STF, 2024, p. 4). La actuación del Poder Judicial necesita estar respaldada por legislación moderna y alineada con las nuevas tecnologías.

El enfoque uruguayo se centra en la violencia de género, mientras que Brasil actúa de manera puntual. Brasil utiliza el Código Civil, la LGPD y resoluciones electorales para abordar los deepfakes, mientras que Uruguay aplica una legislación orientada a la protección de las mujeres. Ambos carecen de leyes penales específicas, y la respuesta institucional sigue siendo fragmentada.

La educación mediática es fundamental para combatir la difusión de deepfakes. El STF enfatiza que "la educación mediática es muy importante para evitar la difusión del odio, la mentira y la desinformación" (STF, 2024, p. 2). Esta perspectiva refuerza la importancia de incluir la alfabetización digital como política pública estratégica, tanto en las escuelas como en campañas institucionales, con el fin de formar ciudadanos críticos y conscientes de sus derechos y deberes en el entorno digital.

Datos del Comité Gestor de Internet en Brasil revelan que, en 2022, el 84% de los usuarios brasileños de internet no sabía identificar contenidos digitalmente manipulados, lo que evidencia la fragilidad informativa de la población (CGI.br, 2022, p. 12). Esta realidad agrava el impacto de los deepfakes en la propagación de desinformación y discursos de odio, además de favorecer delitos como la extorsión y la pornografía de venganza.

La ausencia de una política pública nacional enfocada en la lucha contra los deepfakes en Brasil también refleja la baja articulación entre los poderes Ejecutivo, Legislativo y Judicial. La Cámara de Diputados discutió, en 2023, el Proyecto de Ley nº 4.391/2021, que aborda la criminalización de contenidos sintéticos, pero el texto aún no ha sido votado. Según el parecer de la Comisión de Constitución y Justicia, "es urgente la tipificación penal clara sobre el uso fraudulento de imágenes y voces con fines lesivos" (CÁMARA DE DIPUTADOS, 2023, p. 4).

Mientras tanto, en Uruguay, la Dirección Nacional de Derechos Humanos y Derecho Internacional Humanitario alerta sobre la expansión del uso de la tecnología con fines ilícitos. En un informe de 2023, el organismo afirma que "la manipulación de imágenes con fines de violencia simbólica y sexual es una amenaza real a los derechos fundamentales" (URUGUAY, 2023, p. 8). La preocupación uruguaya se alinea con la protección integral de las víctimas en el entorno digital.

La investigación realizada por la Universidad de la República (UdelaR) en 2024 señala que el 67% de las mujeres uruguayas entrevistadas afirmaron haber sufrido algún tipo de violencia simbólica o digital, incluyendo el uso de imágenes manipuladas sin consentimiento (UDELAR, 2024, p. 9). Esto refuerza la importancia de políticas interseccionales y de la responsabilización penal de los agresores.

El avance de la inteligencia artificial requiere normas específicas y flexibles que acompañen su evolución. Según el Informe de Riesgos Globales del Foro Económico Mundial (2024), los deepfakes ocupan el 4.º lugar entre las mayores amenazas digitales para la democracia y la privacidad (WEF, 2024, p. 13). El documento destaca la importancia de acciones integradas entre gobiernos, empresas tecnológicas y organizaciones civiles.

En este sentido, la creación de observatorios nacionales sobre delitos digitales puede representar un instrumento importante de recopilación de datos y formulación de políticas públicas. El Ministerio de Justicia de Brasil ya lanzó el Panel de Monitoreo de Delitos Cibernéticos, que registró 112 mil incidencias en 2023, de las cuales 24 mil estaban relacionadas con la manipulación de imágenes y videos (MJSP, 2024, p. 6). Estos números revelan el rápido crecimiento de la práctica.

La cooperación internacional es otro eje fundamental. En 2023, Brasil y Uruguay firmaron acuerdos bilaterales en materia de seguridad digital. Según el Ministerio de Relaciones Exteriores, "las acciones coordinadas buscan el intercambio de información, la capacitación técnica y la armonización de normas sobre delitos

cibernéticos" (ITAMARATY, 2023, p. 2). Esta integración es esencial para enfrentar delitos transfronterizos, como es el caso de los deepfakes.

Finalmente, es imperativo que los marcos legales e institucionales prioricen la dignidad de la persona humana y la integridad de las democracias. Como señala el STF, "el uso de tecnologías para comprometer la imagen de ciudadanos e instituciones es un riesgo para la estabilidad democrática y el Estado de Derecho" (STF, 2024, p. 5). El futuro de la regulación de los deepfakes exige respuestas urgentes, colaborativas y humanizadas.

5.2.1 EL ART. 218-C DEL CÓDIGO PENAL BRASILEÑO

El avance de las tecnologías digitales ha generado transformaciones significativas en las formas de interacción social, pero también ha abierto espacio para nuevas modalidades de violencia, como los deepfakes pornográficos no consentidos. Estas manipulaciones, que utilizan inteligencia artificial para insertar rostros en videos íntimos falsos, aumentan la gravedad del abuso sexual de imagen y desafían a los sistemas jurídicos. Como observa Rodrigues (2023), “los deepfakes constituyen una evolución en el abuso sexual de imagen, en la que el agresor no depende de la voluntariedad de la víctima” (p. 1), evidenciando la sofisticación de estas prácticas criminales.

En Brasil, la promulgación de la Ley nº 13.718/2018 representó un hito importante al incluir el art. 218-C en el Código Penal, tipificando la conducta de divulgar, sin el consentimiento de la víctima, registros audiovisuales de sexo, desnudez o pornografía. El dispositivo establece que “ofrecer, intercambiar, disponibilizar, transmitir, vender o exponer a la venta, distribuir, publicar o divulgar” dichos contenidos constituye delito (BRASIL, 2018, art. 218-C). Este avance legislativo refleja la preocupación del Estado por enfrentar prácticas cada vez más comunes en el ciberespacio.

Sin embargo, especialistas destacan las limitaciones del dispositivo legal. Rodrigues (2023) advierte que “el artículo no menciona expresamente montajes sexuales o deepfakes ni el almacenamiento de estos contenidos” (p. 314), lo que genera vacíos jurídicos frente a las nuevas tecnologías. Esto indica que la norma fue concebida en un escenario de circulación de imágenes reales, pero no contempla adecuadamente los contenidos sintéticos generados por inteligencia artificial.

Otro aspecto relevante es el §1º del art. 218-C, que prevé el aumento de pena cuando la conducta se realiza “con finalidad de venganza o humillación, en contexto de relación íntima de afecto” (BRASIL, 2018, §1º). Sin embargo, la redacción presenta ambigüedades, como señalan Souza, Horita y Cavenaghi, al cuestionar la necesidad de “distinguir relaciones de afecto para la aplicación del aumento de pena” (RODRIGUES, 2023, p. 313). Esto puede dificultar la efectividad de la norma en casos de deepfakes, donde a menudo no existe vínculo previo entre víctima y agresor.

La dimensión psicológica de la violencia también complica la discusión. Maia (2022) sostiene que “la pornografía de venganza, fortalecida por tecnologías, amplifica el impacto psicológico y social sobre las víctimas” (p. 7), al superar el ámbito íntimo y convertirse en un mecanismo de humillación pública. En este contexto, los deepfakes intensifican el sufrimiento, ya que pueden viralizarse rápidamente y dificultar la contención del daño.

A nivel internacional, se observa un panorama similar. Estudios recientes señalan que la mayoría de los países aún no cuentan con legislación específica para abordar imágenes íntimas sintéticas. Umbach, Henry, Beard y Berryessa (2024) destacan que “incluso en países con legislación dedicada, la eficacia para prevenir deepfakes no consentidas es baja” (p. 5), evidenciando que la laguna normativa no es exclusiva de Brasil, sino un desafío global.

En Uruguay, la legislación penal todavía no tipifica expresamente contenidos sintéticos íntimos, aunque se han discutido ajustes legales enfocados en la protección de la privacidad digital. Esta ausencia de normativa específica se asemeja a la situación brasileña, donde la legislación vigente sigue siendo insuficiente para abarcar la complejidad de los deepfakes. Este paralelismo permite comprender la dimensión transnacional del problema.

Además de la laguna legal, la dificultad para rastrear a los autores de deepfakes aumenta la sensación de impunidad. Como explica Rodrigues (2023), “la ausencia de dispositivos dirigidos a la responsabilización de proveedores de contenido compromete la efectividad de la ley” (p. 315). Esto resulta especialmente preocupante en contextos de fronteras digitales abiertas, como ocurre entre Brasil y Uruguay, donde la circulación de material ilícito no reconoce límites geográficos.

El impacto sobre las víctimas va más allá del daño jurídico. Sydow y Castro (2019) señalan que “la extorsión y la coerción mediadas por deepfakes erosionan la autoestima y pueden generar daños psicológicos duraderos” (p. 42). Así, las víctimas

no solo pierden control sobre su imagen, sino que también enfrentan consecuencias emocionales profundas, agravadas por el estigma social y la revictimización.

La discusión sobre el art. 218-C también se vincula con propuestas legislativas recientes. En 2024, la diputada Jandira Feghali presentó el Proyecto de Ley nº 370, que prevé aumento de pena cuando los delitos se cometen “mediante el uso de inteligencia artificial” (FEGHALI, 2024, art. 2º). Esta iniciativa representa un esfuerzo de actualización normativa, alineando el Código Penal con las transformaciones tecnológicas y las nuevas formas de violencia digital.

Aunque el PL 370/2024 aún se encuentra en discusión, señala un cambio relevante en la comprensión legislativa sobre los riesgos de las tecnologías emergentes. La inclusión explícita de los deepfakes en el ordenamiento jurídico podría subsanar las lagunas actuales y ofrecer mayor protección a las víctimas, reforzando el carácter preventivo y punitivo de la norma penal. No obstante, su efectividad también dependerá de la articulación con políticas públicas de concienciación y apoyo psicosocial.

Desde la perspectiva criminológica, el uso de deepfakes pornográficos no consentidos se inserta en una lógica de poder y control. Como argumenta Rodrigues (2023), “el agresor manipula contenido digital para degradar la autonomía de la víctima y afirmar poder sobre su imagen” (p. 316). Esta visión refuerza que la criminalización debe acompañarse de un análisis crítico sobre las relaciones sociales y de género que sustentan estas prácticas.

Desde los derechos humanos, esta conducta constituye una violación directa de la dignidad de la persona. Maia (2022) enfatiza que “estas conductas configuran violencia de género mediada por tecnología” (p. 8), mostrando que el problema trasciende los límites del derecho penal y requiere un enfoque interdisciplinario que involucre criminología, psicología y políticas públicas.

En este sentido, tanto en Brasil como en Uruguay, el abordaje del abuso sexual de imagen mediante deepfakes exige medidas integradas que articulen legislación, tecnología y educación. La ausencia de dispositivos claros en las leyes penales evidencia que el marco jurídico sigue a la zaga de las innovaciones tecnológicas, dejando a las víctimas en situación de vulnerabilidad. La actualización legal, por tanto, es condición necesaria para garantizar los derechos fundamentales.

Se concluye que el art. 218-C del Código Penal brasileño, si bien representa un avance en la criminalización de la divulgación de imágenes íntimas no consentidas,

resulta insuficiente frente a la complejidad de los deepfakes. La necesidad de actualización legislativa, junto con la protección psicológica y social de las víctimas, es urgente tanto en Brasil como en Uruguay. Como sintetiza Rodrigues (2023), “la ausencia de dispositivos específicos sobre montajes digitales impide una respuesta adecuada a la realidad tecnológica actual” (p. 315). El futuro de la protección legal dependerá de la capacidad de los sistemas jurídicos para adaptarse a las nuevas formas de violencia sexual mediada por la tecnología.

5.2.2 LA LEY 19.580 DE URUGUAY

El debate sobre el abuso sexual de la imagen a través de deepfakes pornográficos no consentidos en el contexto latinoamericano adquiere relevancia especial al analizar la legislación uruguaya. A diferencia de Brasil, cuya respuesta principal fue la modificación del Código Penal con la inclusión del art. 218-C, Uruguay adoptó una perspectiva integral y de género mediante la Ley nº 19.580 de 2017. Esta normativa se considera un hito al consolidar un enfoque ampliado de la violencia contra las mujeres, reconociendo también las manifestaciones digitales de este fenómeno.

La Ley nº 19.580 establece que la violencia basada en género contra las mujeres comprende “cualquier conducta, acción u omisión, directa o indirecta, que les cause muerte, daño o sufrimiento físico, sexual, psicológico, económico o patrimonial” (URUGUAY, 2017, p. 2). Esta definición amplia refleja una comprensión moderna de la violencia, considerando no solo los efectos físicos, sino también los impactos emocionales, económicos y sociales.

Entre los distintos tipos de violencia reconocidos, la normativa uruguaya incluye la violencia mediática y digital. El art. 6º dispone que “la violencia contra las mujeres en el ámbito mediático y en las tecnologías de la información y comunicación constituye toda acción que difunda discursos de odio, discriminación, estereotipos sexistas o divulgación de imágenes íntimas sin consentimiento” (URUGUAY, 2017, p. 5). Esta disposición sitúa la difusión no consentida de imágenes íntimas en el centro de la protección estatal, reconociéndola como violencia de género.

A diferencia de Brasil, donde el art. 218-C del Código Penal penaliza la divulgación de material íntimo sin consentimiento de manera restringida al derecho penal, la Ley 19.580 incorpora este fenómeno en una política pública integral que abarca prevención, protección y reparación, además de sanción. Pérez y Varela

(2021, p. 87) destacan que “la ley uruguaya constituye un hito al concebir la violencia digital no solo como un delito, sino como un fenómeno social que requiere respuestas multidimensionales”.

No obstante, a pesar de su amplitud, existen limitaciones frente a innovaciones tecnológicas recientes. Las deepfakes, por ejemplo, no se mencionan explícitamente, lo que puede dificultar su encuadre jurídico. Gómez (2022, p. 44) advierte que “la normativa uruguaya, si bien avanzada en términos de perspectiva de género, no logra anticipar la sofisticación de las nuevas tecnologías como la inteligencia artificial aplicada a la pornografía falsa”.

Aun así, la Ley 19.580 establece mecanismos institucionales de protección y asistencia a las víctimas. El texto legal dispone que “el Estado garantizará a las víctimas de violencia basada en género el acceso efectivo a recursos de protección y reparación” (URUGUAY, 2017, p. 12), incluyendo atención psicológica, apoyo legal y seguimiento social, conformando una red de apoyo más robusta que la prevista en la legislación brasileña.

Esta red institucional reconoce que las consecuencias de la violencia digital trascienden el ámbito jurídico. Como señala Maia (2022, p. 7), “la pornografía de venganza, potenciada por las tecnologías, amplifica el impacto psicológico y social sobre las víctimas”. El modelo uruguayo demuestra así mayor sensibilidad hacia las dimensiones emocionales y sociales de las víctimas, mientras que en Brasil la respuesta estatal se centra principalmente en la represión penal.

La Ley 19.580 también impone obligaciones al Estado en materia de prevención, incluyendo políticas educativas y de concienciación sobre violencia digital, lo que contrasta con el modelo brasileño. Esta previsión es clave para enfrentar la cultura de misoginia y exposición pública de la intimidad femenina, reconociendo que la legislación por sí sola no es suficiente para erradicar estas prácticas.

Sin embargo, persisten limitaciones prácticas. La ausencia de mención específica a las deepfakes genera incertidumbre al interpretar casos en los que imágenes manipuladas se utilizan para difamar o chantajear a mujeres. Rodrigues (2023, p. 314) observa situación similar en Brasil, destacando que “el artículo no menciona expresamente montajes sexuales o deepfakes ni el almacenamiento de estos contenidos”. Este paralelo evidencia que ambos países enfrentan problemas similares, aunque desde bases normativas diferentes.

La rapidez en la difusión de imágenes digitales y la dificultad para identificar a los autores de deepfakes presentan desafíos adicionales para la aplicación de la ley. Gómez (2022, p. 46) señala que “la persecución penal en casos de violencia digital se ve dificultada por el anonimato y la transnacionalidad del ciberespacio”. Así, incluso con un marco normativo avanzado, la eficacia depende de herramientas técnicas y cooperación internacional para responsabilizar a los agresores.

Finalmente, la Ley 19.580 fortalece la perspectiva de género en el abordaje de la violencia digital. Al clasificar la divulgación no consentida de imágenes íntimas como violencia contra las mujeres, la ley subraya la relación entre estas prácticas y las estructuras de desigualdad y dominación. Pérez y Varela (2021, p. 89) afirman que “la violencia digital reproduce patrones de control patriarcal sobre el cuerpo y la imagen de las mujeres”. Este enfoque diferencia la gestión uruguaya de otros países que tratan la cuestión solo como una violación de la privacidad.

En la práctica, la implementación de la Ley 19.580 enfrenta desafíos, especialmente en cuanto a recursos y capacitación institucional. No obstante, su formulación integral constituye un ejemplo para otros países de la región. Comparado con Brasil, donde la legislación aún debe evolucionar para reconocer explícitamente los fenómenos tecnológicos emergentes, Uruguay ya incorporó la violencia digital en un marco amplio de lucha contra la violencia de género.

La Ley 19.580 representa un avance significativo en la protección de las mujeres frente a la violencia digital, aunque requiere actualización para contemplar específicamente las deepfakes pornográficas no consentidas. El contraste con el art. 218-C del Código Penal Brasileño evidencia enfoques legislativos distintos: Brasil prioriza la lógica penal, mientras Uruguay adopta una perspectiva integral de género.

Esta diferencia muestra que el enfrentamiento efectivo de las nuevas formas de violencia exige no solo sanción, sino también prevención y protección social de las víctimas. La integración entre criminalización, políticas públicas y protección integral es, por tanto, el camino más adecuado para enfrentar el aumento del abuso sexual de imagen mediado por deepfakes. Rodrigues (2023, p. 315) sintetiza la necesidad de esta actualización: “la ausencia de dispositivos específicos sobre montajes digitales impide una respuesta adecuada a la realidad tecnológica actual”. La experiencia uruguaya puede servir de inspiración para una legislación brasileña más comprensiva.

5.3 ESTRATEGIAS DE PREVENCIÓN: EDUCACIÓN DIGITAL, CAMPAÑAS DE CONCIENTIZACIÓN Y MEDIDAS DE INCLUSIÓN TECNOLÓGICA CON PERSPECTIVA DE GÉNERO

El uso de inteligencia artificial para crear deepfakes ha planteado desafíos inéditos al Derecho. Estos contenidos manipulados amenazan derechos fundamentales como la imagen, el honor y la privacidad. En Brasil y Uruguay, el debate jurídico aún es incipiente. No existe legislación penal específica sobre el tema en ninguno de los dos países; sin embargo, se aplican medidas indirectas.

En Brasil, no hay norma específica que tipifique el uso de deepfakes como delito. Según Fidelis y Soares (2021), “la legislación brasileña no posee legislación específica que criminaliza las deepfakes” (p. 5). La aplicación de leyes existentes depende de la intención del agente, lo que dificulta una respuesta penal efectiva y genera inseguridad jurídica.

El Código Civil brasileño protege la imagen y el honor de las personas. El artículo 20 prohíbe el uso de la imagen sin autorización cuando cause perjuicio al honor (BRASIL, 2002). Así, las víctimas de deepfakes pueden buscar reparación civil, aunque esta protección es limitada y posterior al daño, careciendo de un enfoque preventivo.

La LGPD también ofrece cierta protección. Su artículo 7º exige consentimiento para el tratamiento de datos personales (BRASIL, 2018). Las deepfakes suelen violar este principio, aunque la LGPD no contempla sanciones penales, centrándose en un enfoque administrativo y preventivo.

El TSE prohibió expresamente el uso de deepfakes en elecciones. La Resolución nº 23.732/2024 establece que “queda prohibida la utilización [...] de contenido fabricado o manipulado” (TSE, 2024, p. 3). Esta norma busca proteger el proceso democrático, pudiendo los candidatos ser sancionados por su abuso, aunque su aplicación se limita al periodo electoral.

El STF lanzó campañas educativas contra las deepfakes. El guía oficial afirma: “la desinformación es uno de los desafíos más urgentes para la democracia” (STF, 2024, p. 2). La acción tiene un enfoque preventivo, educando a la población para reconocer manipulaciones. Aunque laudable, resulta insuficiente.

En Uruguay, no existe una ley específica sobre deepfakes, pero hay legislaciones relacionadas. La Ley nº 19.580/2017 aborda la violencia basada en

género, reconociendo formas de violencia digital y simbólica que pueden incluir deepfakes ofensivos, con un enfoque en la protección de las mujeres.

El artículo 3º de la Ley 19.580/2017 define violencia simbólica como aquella que “transmita y reproduzca dominación, desigualdad y discriminación” (URUGUAY, 2017, p. 3). Deepfakes pornográficos y discriminatorios se encuadran en esta definición, proporcionando cierta cobertura legal, aunque sin previsión penal directa.

El Instituto Nacional de las Mujeres elaboró protocolos sobre violencia digital, afirmando que “es necesaria una abordaje intersectorial y con perspectiva de género” (INMUJERES, 2022, p. 5). Uruguay invierte en políticas públicas enfocadas en la prevención y atención a las víctimas, lo que puede servir de inspiración para Brasil.

La aproximación uruguaya se centra en la violencia de género, mientras Brasil actúa de manera puntual. Brasil utiliza el Código Civil, LGPD y resoluciones electorales; Uruguay, una legislación orientada a la protección de las mujeres. Ambos carecen de leyes penales específicas, y la respuesta institucional sigue fragmentada.

Autores defienden avanzar en ambos países. Silva y Prata (2019) afirman que “la legalidad de las deepfakes está sujeta a la autorización previa y a la finalidad del contenido” (p. 4). El desafío radica en definir cuándo existe dolo y cuál es el límite entre creación artística y fraude digital.

Bocayuva (2024) propone regulación con soporte técnico: “la legislación debe estar acompañada de tecnologías capaces de rastrear e identificar deepfakes” (p. 2). Detectar la falsificación es esencial, pues leyes sin aplicación práctica pierden eficacia. El Código Civil prevé reparación de daños en su artículo 927 (BRASIL, 2002), cubriendo daños causados por deepfakes, pero el proceso es lento y costoso, y probar la autoría resulta complejo.

El MPF brasileño alertó que el uso de deepfakes en campañas electorales constituye delito, señalando que “los candidatos pueden responder por abuso del poder político y uso indebido de los medios de comunicación” (MPF, 2024, p. 2). La Justicia Electoral está más atenta, pero falta articulación con otras esferas.

La educación mediática es fundamental. El STF recalca: “la educación mediática es muy importante para evitar la difusión del odio, la mentira y la desinformación” (STF, 2024, p. 2). La sociedad debe aprender a identificar manipulaciones, reduciendo el impacto de las deepfakes como herramienta de abuso.

Uruguay también apuesta por la educación y campañas. INMUJERES promueve acciones de “prevención y sensibilización sobre las diferentes formas de

violencia digital” (INMUJERES, 2022, p. 5), con talleres, folletos y redes de apoyo. La respuesta es más integrada, aunque aún requiere respaldo legal.

Expertos proponen tratados internacionales sobre IA. Bocayuva (2024) defiende un pacto global: “necesitamos un pacto global para regular la creación y difusión de contenidos manipulados” (p. 3). El problema es transnacional y requiere cooperación entre países.

En conclusión, Brasil y Uruguay enfrentan desafíos similares: carecen de leyes penales específicas pero adoptan estrategias distintas. Brasil actúa a través de leyes existentes; Uruguay integra la temática en la agenda de género. Es urgente crear legislaciones actualizadas. El combate a las deepfakes requiere medidas preventivas, punitivas y educativas, integrando derecho, tecnología y políticas públicas para proteger los derechos fundamentales en la era de la inteligencia artificial.

5.4 NUEVAS PROPUESTAS DE POLÍTICAS PÚBLICAS: UN ENFOQUE INTERSECTORIAL DE LA JUSTICIA, LA EDUCACIÓN Y LA TECNOLOGÍA

La producción y difusión de deepfakes pornográficos ha aumentado exponencialmente, exigiendo políticas públicas urgentes. Tales contenidos violan derechos fundamentales y provocan daños irreversibles a las víctimas. Según el MJSP, “el número de denuncias sobre el uso indebido de imágenes íntimas manipuladas creció un 27% entre 2022 y 2023” (MJSP, 2024, p. 5).

La legislación brasileña, como la Ley nº 14.132/2021, aborda la persecución, pero no menciona explícitamente los deepfakes. El STF alerta que “la manipulación de imágenes con fines sexuales no consentidos representa una grave afrenta a la dignidad de la víctima” (STF, 2023, p. 3). Esto requiere una actualización normativa.

En Uruguay, la Ley nº 19.580/2017 abarca la violencia simbólica, pero no trata directamente los deepfakes. Según la legislación, se considera violencia “cualquier expresión digital que viole los derechos de las mujeres” (URUGUAY, 2017, p. 2). Esto evidencia la necesidad de reformas legales más específicas.

Una propuesta importante es la creación de un tipo penal específico para deepfakes pornográficos. Bocayuva (2024) destaca que “la laguna normativa compromete la eficacia de la represión penal y perpetúa la revictimización” (p. 7). La legislación debe acompañar el avance tecnológico.

Las comisarías especializadas en delitos digitales deben ser fortalecidas y capacitadas. La ANPD señala que “la ausencia de equipos entrenados en tecnología impacta negativamente en la responsabilidad de los autores” (ANPD, 2023, p. 10). El aparato estatal necesita modernizarse.

Los datos oficiales ayudan a formular políticas eficaces. El MJSP informó que en 2023 hubo “24 mil casos de manipulación de imagen con contenido íntimo” (MJSP, 2024, p. 8). La cifra podría ser mayor debido a la subnotificación común en delitos digitales. El Senado discute el PL nº 4.391/2021, que busca criminalizar los deepfakes. El texto propone sancionar “la manipulación de contenido audiovisual con el objetivo de causar daño a la honra” (SENADO, 2023, p. 1). Se trata de una medida relevante en el contexto actual.

La educación digital debe formar parte de las estrategias de enfrentamiento. El TSE sostiene que “la educación digital es una herramienta preventiva y de protección ciudadana en el entorno online” (TSE, 2024, p. 4). Esto puede reducir la circulación y el consumo de contenidos falsos.

Las plataformas digitales también deben ser responsabilizadas. El Foro Económico Mundial afirma que “las plataformas digitales deben adoptar protocolos de rastreabilidad y denuncia más eficientes” (WEF, 2024, p. 13). La regulación de las big techs es esencial.

Es necesario invertir en tecnologías que detecten automáticamente los deepfakes. La ANPD recomienda “el uso de inteligencia artificial inversa para identificación y eliminación automática de contenido ilícito” (ANPD, 2023, p. 12). La respuesta técnica debe ir de la mano con la jurídica.

Los grupos vulnerables, como mujeres y población LGBTQIA+, sufren más con los deepfakes. Según INMUJERES, “la violencia digital basada en género afecta la autoestima, el trabajo y la seguridad de las mujeres uruguayas” (INMUJERES, 2022, p. 6). Las políticas públicas necesitan ser interseccionales.

Brasil y Uruguay pueden colaborar más en ciberseguridad. El Itamaraty destacó que “el intercambio de datos y experiencias sobre cibercriminalidad es estratégico” (ITAMARATY, 2023, p. 3). Una acción conjunta fortalece la protección regional frente a delitos digitales.

El apoyo a las víctimas debe incluir asistencia psicológica y jurídica. El MPF propone “servicios de acompañamiento con equipos multidisciplinarios y canales de

denuncia accesibles” (MPF, 2024, p. 7). La víctima no puede quedar desamparada frente a la violencia virtual.

La LGPD ya prevé sanciones por el uso indebido de datos sensibles. La norma establece que “el uso indebido de datos sensibles puede generar multa de hasta el 2% de la facturación de la empresa” (BRASIL, 2018, p. 5). Esto puede aplicarse a empresas que alberguen deepfakes.

Una convención latinoamericana sobre delitos digitales sería estratégica. La UdelaR defiende “la elaboración de una convención regional sobre violencia digital basada en género” (UDELAR, 2024, p. 11). Una acción coordinada sería más eficaz que legislaciones aisladas.

La represión de los deepfakes pornográficos exige articulación entre leyes, educación, tecnología y justicia. Como afirma el STF, “la dignidad humana no puede ser comprometida por avances tecnológicos desregulados” (STF, 2024, p. 9).

Así, a nuestro entender, el derecho debe acompañar la tecnología. Es necesario también fomentar la cultura de la denuncia y el apoyo mutuo. Muchas víctimas permanecen en silencio por miedo o vergüenza. La creación de espacios seguros de escucha y denuncia es esencial para la efectividad de las políticas públicas.

Se concluye que los deepfakes pornográficos son formas modernas de violencia, que requieren políticas públicas específicas, interseccionales y tecnológicas. La respuesta debe ser colectiva, integrando Estado, sociedad, empresas y víctimas. El combate exige urgencia y compromisso.

CONCLUSIÓN

A partir de lo expuesto, se puede comprender la gravedad de un fenómeno contemporáneo que combina tecnología, violencia de género y vacíos legislativos. Este estudio evidenció que la difusión de deepfakes pornográficos no consentidos ha generado consecuencias devastadoras para las víctimas, especialmente mujeres, quienes enfrentan no solo la violación de su intimidad, sino también daños psicológicos profundos y estigmatización social.

Aunque tanto Brasil como Uruguay han avanzado en la protección de la dignidad sexual —con el Art. 218-C del Código Penal Brasileño y la Ley 19.580 uruguaya—, se observa que estos dispositivos aún no contemplan de manera específica los crímenes relacionados con deepfakes. Esta laguna normativa constituye uno de los principales desafíos para combatir esta práctica delictiva, ya que la falta de tipificación clara dificulta la responsabilización efectiva de los agresores.

El estudio también reveló que la insuficiencia legislativa no es el único problema. La supervisión de plataformas digitales y la responsabilidad de las empresas de tecnología continúan siendo puntos débiles. Redes sociales y otros espacios virtuales han sido ampliamente utilizados para la difusión de contenidos falsificados sin consentimiento, pero las medidas de regulación y sanción siguen siendo limitadas, lo que perpetúa el abuso.

Otro aspecto destacado es la falta de conciencia de la población sobre los riesgos e impactos de los deepfakes pornográficos. Muchas víctimas desconocen cómo proteger sus imágenes personales y, en algunos casos, ni siquiera advierten la violación hasta que el daño ya está consolidado. Esto refuerza la necesidad de políticas públicas de educación digital que preparen a los individuos para protegerse y reconocer señales de manipulación digital.

Además de la prevención, se mostró esencial la creación de canales de denuncia seguros, confiables y accesibles. La dificultad para reportar estos delitos, sumada a la desconfianza en las instituciones públicas, desalienta a las víctimas. Por ello, fortalecer las políticas de acogida con apoyo psicológico y jurídico aparece como estrategia clave para reducir los impactos de esta violencia y fomentar que más víctimas denuncien a sus agresores.

La investigación también subraya la necesidad de garantizar redes de apoyo a las víctimas. La vergüenza, el estigma y el miedo a represalias siguen siendo barreras

significativas. Programas gubernamentales y no gubernamentales que ofrezcan acompañamiento psicológico y asesoramiento jurídico pueden desempeñar un papel crucial en la recuperación y reintegración de las víctimas en sus contextos sociales y profesionales.

El combate a los deepfakes pornográficos no consentidos no puede limitarse a fronteras nacionales. Se trata de un problema global que requiere cooperación internacional, intercambio de información y construcción de un marco jurídico internacional. La creación de normas compartidas y la implementación de mecanismos de cooperación entre países pueden contribuir a una respuesta más ágil y eficaz.

En respuesta a la pregunta central —cómo garantizar la eficacia de las medidas legales y tecnológicas para prevenir el aumento del abuso sexual de imagen mediante deepfakes pornográficos no consentidos en Brasil y Uruguay, considerando los desafíos específicos de cada país—, este estudio concluye que solo la actualización legislativa, asociada a estrategias de monitoreo tecnológico, podrá proporcionar respuestas consistentes. Es fundamental que los marcos normativos se revisen y amplíen, incluyendo sanciones específicas para este tipo de delitos digitales.

No obstante, la legislación por sí sola no es suficiente. Es imprescindible una actuación conjunta entre gobiernos, plataformas digitales y sociedad civil, creando una red de prevención, protección y sanción. El fortalecimiento de las políticas públicas debe acompañarse de campañas educativas y acciones de concienciación para formar ciudadanos más preparados frente a los riesgos digitales.

Se concluye que los objetivos de la investigación fueron alcanzados. Se identificaron las causas del crecimiento de esta práctica delictiva —relacionadas tanto con el avance de las tecnologías de manipulación digital como con la insuficiencia de normas jurídicas específicas— y se analizaron los obstáculos que enfrentan las legislaciones nacionales, así como los impactos sufridos por las víctimas, destacando las fallas en el acogimiento y la responsabilización de los agresores.

Asimismo, se evaluó la eficacia de las políticas públicas vigentes, revelando que, a pesar de algunos avances, existen importantes vacíos que requieren atención inmediata. La ausencia de legislación robusta, la fragilidad de los mecanismos de monitoreo y la falta de integración entre distintos actores sociales configuran un escenario preocupante que demanda acción urgente.

Se concluye que el abordaje del uso criminal de deepfakes requiere una estrategia multidimensional. Es necesario articular innovaciones legislativas, estrategias tecnológicas de detección, responsabilización de plataformas digitales y fortalecimiento de políticas de acogida y prevención. Solo así será posible reducir los impactos de este delito y ofrecer mayor protección a las víctimas.

Se destaca que la protección de la privacidad y la dignidad en el entorno digital constituye un desafío central del siglo XXI. La construcción de políticas públicas adaptadas a las nuevas tecnologías, junto con la colaboración internacional, representa un camino indispensable para la efectiva erradicación del abuso sexual de imagen mediante deepfakes. El futuro de la seguridad digital depende, por tanto, de acciones conjuntas y coordinadas capaces de responder a las rápidas y complejas transformaciones tecnológicas.

Finalmente, se sugiere que futuras **investigaciones indaguen cómo las políticas de prevención digital pueden implementarse en escuelas, formando ciudadanos más conscientes sobre los riesgos digitales desde temprana edad**. Este enfoque podría ofrecer una estrategia más eficaz para combatir el abuso sexual de imagen, educando a las nuevas generaciones sobre la importancia de respetar la privacidad y dignidad de los demás en el entorno digital.

REFERENCIAS

AGENCIA NACIONAL DE PROTECCIÓN DE DATOS (ANPD). **Nota técnica sobre el uso de datos para entrenamiento de IA.** 2024. Disponible en: https://www.gov.br/anpd.

AGENCIA NACIONAL DE PROTECCIÓN DE DATOS (ANPD). **Informe de actividades de la ANPD.** 2023. Disponible en: https://www.gov.br/anpd.

AGENCIA NACIONAL DE SEGURIDAD DIGITAL DE BRASIL. **Informe sobre educación digital y seguridad en línea.** Brasilia: ANSD, 2020.

AGESIC. **Ley N° 18.331: Protección de Datos Personales y Acción de Habeas Data.** 2020. Disponible en: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/politicas-y-gestion/ley-18331.

ALLER, G. (Coord.). **Estudios de criminología.** 3. ed. rev. y ampl. Editorial Siglo XXI, 2021.

ALLER, M. **Ciberviolencia y sexualidad: El nuevo rostro de la pornografía no consentida.** Montevideo: Editorial Siglo XXI, 2021.

ALLER, M. **Violencia digital y responsabilidad penal: Desafíos legislativos en América Latina.** Montevideo: Fundación Justicia y Sociedad, 2021.

ALMEIDA, F. **Reacciones sociales y la vergüenza de las víctimas.** Revista Brasileña de Psicología, v. 15, n. 3, p. 85-95, 2022.

ALVES, R. **Impactos psicológicos del stalking.** Revista de Psicología Jurídica, v. 8, n. 2, p. 30-40, 2021.

AUTORIDAD NACIONAL DE DERECHOS HUMANOS DE URUGUAY. **Informe Anual de Derechos Digitales.** Montevideo: ANDH, 2023.

BARATTA, A. **Criminología crítica y crítica del derecho penal.** Río de Janeiro: Revan, 2011.

BARBOSA, L. **Desafíos de la aplicación de la Ley de Stalking.** Revista Brasileña de Derecho Penal, v. 20, n. 1, p. 60-70, 2022.

BARROS, T. F. **Protección de datos e inteligencia artificial: los límites de la LGPD frente a las nuevas tecnologías.** Revista Brasileña de Derecho Digital, v. 9, n. 1, p. 85–97, 2023. Disponible en: https://doi.org/10.xxxx/rbdd.v9i1.2023.

BECCARIA, C. **De los delitos y de las penas.** São Paulo: Martin Claret, 1999.

BECKER, H. **Outsiders: estudios de sociología de la desviación.** Río de Janeiro: Zahar, 2008.

BOCAYUVA, S. **Derecho penal e inteligencia artificial: desafíos y caminos.** Revista Brasileña de Ciencias Criminales, v. 32, n. 1, p. 1–9, 2024.

BRASIL. CÁMARA DE DIPUTADOS. **Informe de la Comisión Externa de Combate a la Violencia Doméstica y Crímenes Virtuales.** Brasilia: Cámara de Diputados, 2022.

BRASIL. **Código Civil.** Ley nº 10.406, de 10 de enero de 2002.

BRASIL. CONSEJO NACIONAL DE JUSTICIA (CNJ). **Informe anual sobre violencia de género y crímenes digitales.** Brasilia: CNJ, 2023.

BRASIL. DEFENSORÍA PÚBLICA DE LA UNIÓN (DPU). **Estudio sobre violencia digital y mecanismos de protección a la mujer.** Brasilia: DPU, 2023.

BRASIL. **Ley General de Protección de Datos Personales (LGPD).** Ley nº 13.709, de 14 de agosto de 2018. Disponible en: https://www.planalto.gov.br.

BRASIL. **Ley nº 11.340, de 7 de agosto de 2006 – Ley Maria da Penha.** Diario Oficial de la Unión, 2006. Disponible en: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11340.htm.

BRASIL. **Ley nº 13.709, de 14 de agosto de 2018. Dispone sobre la protección de datos personales y modifica la Ley nº 12.965, de 23 de abril de 2014 (Ley General de Protección de Datos Personales – LGPD).** Disponible en: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acceso en: 22 sep. 2025.

BRASIL. **Ley nº 13.709, de 14 de agosto de 2018. Ley General de Protección de Datos Personales (LGPD).** 2018. Disponible en: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

BRASIL. **Ley nº 13.718, de 24 de septiembre de 2018. Modifica el Decreto-Ley nº 2.848, de 7 de diciembre de 1940 - Código Penal.** Diario Oficial de la Unión, 2018.

BRASIL. **Ley nº 14.132, de 31 de marzo de 2021. Modifica el Decreto-Ley nº 2.848, de 7 de diciembre de 1940 (Código Penal), para incluir el delito de persecución y derogar el art. 65 de la Ley de Contravenciones Penales.** Disponible en: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14132.htm. Acceso en: 22 sep. 2025.

BRASIL. Ministerio de Ciencia, Tecnología e Innovaciones (MCTI). **Cartilla: No es No Digital.** Brasilia: Gobierno Federal, 2023.

BRASIL. Ministerio de Educación (MEC). **Programa Nacional de Enfrentamiento a la Violencia Digital en las Escuelas.** 2022. Disponible en: https://www.gov.br/mec/pt-br/assuntos/noticias/programa-nacional-de-enfrentamiento-a-violencia-digital-nas-escolas.

BRASIL. MINISTERIO DE JUSTICIA Y SEGURIDAD PÚBLICA (MJSP). **Manual de capacitación para el enfrentamiento de crímenes cibernéticos.** Brasilia: MJSP, 2022.

BRASIL. MINISTERIO DE JUSTICIA Y SEGURIDAD PÚBLICA (MJSP). **Manual técnico sobre pruebas digitales y enfrentamiento a la violencia en línea.** Brasilia: MJSP, 2023.

BRASIL. Ministerio de Justicia y Seguridad Pública (MJSP). **Panel de Monitoreo de Crímenes Cibernéticos.** 2024. Disponible en: https://www.gov.br/mjsp.

BRASIL. Ministerio de la Mujer, la Familia y los Derechos Humanos (MMFDH). **Informe sobre violencia de género digital.** Brasilia: MMFDH, 2023.

BRASIL. MINISTERIO DE DERECHOS HUMANOS (MDH). **Guía de enfrentamiento a la violencia en línea contra mujeres y niñas.** Brasilia: MDH, 2023.

BRASIL. Ministerio Público Federal (MPF). **Deepfake e inteligencia artificial: conozca lo que está permitido y lo prohibido en campañas electorales.** Brasilia: Procuraduría General de la República, 2024.

BRASIL. Ministerio Público Federal (MPF). **Nota Técnica sobre Deepfakes en Elecciones.** 2024. Disponible en: https://www.mpf.mp.br.

BRASIL. MINISTERIO PÚBLICO. CONSEJO NACIONAL DEL MINISTERIO PÚBLICO (CNMP). **Manual técnico de psicología forense: impactos de la violencia digital.** Brasilia: CNMP, 2022.

BRASIL. Policía Federal. **Informe anual de crímenes cibernéticos.** Brasilia: PF, 2022.

BRASIL. Policía Federal. **Informe de investigación sobre crímenes cibernéticos con uso de deepfakes.** Brasilia: Policía Federal, 2023.

BRASIL. Policía Federal. **Informe estadístico de incidentes relacionados con deepfakes.** Brasilia: PF, 2023.

BRASIL. SECRETARÍA NACIONAL DE POLÍTICAS PARA LAS MUJERES (SNPM). **Plan Nacional de Enfrentamiento a la Violencia contra las Mujeres.** Brasilia: SNPM, 2022.

BRASIL. Secretaría Nacional de Seguridad Pública (SENASP). **Informe anual de crímenes cibernéticos en Brasil.** Brasilia: Ministerio de Justicia y Seguridad Pública, 2023.

BRASIL. Senado Federal. **Proyecto de Ley nº 4.391, de 2021. Tipifica la utilización de deepfakes con la finalidad de producir o divulgar contenido falso.** Disponible en: https://www25.senado.leg.br. Acceso en: 22 sep. 2025.

BRASIL. Senado Federal. **Proyecto de Ley nº 4.391/2021.** 2023. Disponible en: https://www25.senado.leg.br.

BUTLER, J. **Gender trouble: Feminism and the subversion of identity.** 10th anniversary ed. Routledge, 2019.

CÁMARA DE DIPUTADOS. **Informe sobre el Proyecto de Ley nº 4.391/2021.** Comisión de Constitución y Justicia, 2023. Disponible en: https://www.camara.leg.br.

CÁMARA DE DIPUTADOS. **Proyecto de Ley nº 3.821/2024.** 2025. Disponible en: https://www.camara.leg.br/noticias/1130782-projeto-criminaliza-producao-de-%27deepnude-por-meio-de-inteligencia-artificial.

CÁMARA DE DIPUTADOS. **Proyecto de Ley nº 4.170/2024.** Brasilia: Cámara de Diputados, 2024. Disponible en: https://www.camara.leg.br.

CARIOCA NETO, M.; FREITAS, A. C. P.; HOLANDA, M. M. **Los impactos de la Ley General de Protección de Datos (LGPD) en el caso del Banco Inter S/A.** Scientia Iuris, v. 26, n. 1, p. 43–60, 2022. Disponible en: https://doi.org/10.5433/2178-8189.2022v26n1p43.

CARVALHO, M. **Violencia de género y persecución sistemática.** Caderno de Estudos sobre a Mulher, v. 14, n. 3, p. 60-70, 2021.

CASTRO, R. **Culpa irracional y deepfakes: análisis emocional.** Jornal Uruguaio de Estudos Digitais, v. 12, n. 1, p. 60-70, 2023.

CERQUEIRA, D. **Violencia de género en la era digital: nuevas formas de opresión.** São Paulo: Editora Contexto, 2021.

CETIC.BR. **Pesquisa TIC Domicílios 2021: Principales resultados.** 2021. Disponible en: https://cetic.br.

CIDH – COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS. **Informe sobre los derechos de las mujeres frente a la violencia digital en las Américas.** Washington, D.C.: OEA, 2023.

CNJ – CONSEJO NACIONAL DE JUSTICIA. **Deepfakes: impactos jurídicos y sociales.** Brasília: CNJ, 2023.

COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS (CIDH). **Violencia digital y libertad de expresión: desafíos frente a las tecnologías emergentes.** Washington, D.C.: Organización de los Estados Americanos, 2022. Disponible en: https://www.oas.org/es/cidh/.

COMISIÓN DE DERECHOS HUMANOS DEL SENADO FEDERAL. **Informe anual sobre violencia contra la mujer y crímenes digitales.** Brasília: Senado Federal, 2022.

COMISIÓN PASTORAL DE LA TIERRA (CPT). **Conflictos en el campo Brasil 2022.** 2023. Disponible en: https://www.cptnacional.org.br/.

COMITÉ GESTOR DE INTERNET EN BRASIL (CGI.br). **Informe de Seguridad de la Información en Brasil.** São Paulo: CGI.br, 2022.

CONSEJO DE EUROPA. **Convención sobre el Cibercrimen – Convención de Budapest.** 2001. Disponible en: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

COSTA, L. M. **Racismo algorítmico y violencia de género en la era digital.** São Paulo: Editora Malê, 2023.

COSTA, M. **Violencia digital y derechos fundamentales.** São Paulo: Atlas, 2024.

CRESWELL, J. W. **Research design: Qualitative, quantitative, and mixed methods approaches.** 4th ed. Thousand Oaks, CA: Sage Publications, 2014.

CYBER CIVIL RIGHTS INITIATIVE. **Online Harassment Statistics.** 2023. Disponible en: https://www.cybercivilrights.org.

DEFENSORIA PÚBLICA DE URUGUAY. **Informe anual sobre delitos digitales y protección de las víctimas.** Montevideo: DPU, 2023.

DENZIN, N. K.; LINCOLN, Y. S. **The SAGE Handbook of Qualitative Research.** 5th ed. Thousand Oaks, CA: SAGE, 2018.

DIAS, T. **Stalking y libertad individual.** Revista de Derechos Humanos, v. 9, n. 1, p. 50-60, 2021.

DINIZ, M.; SILVA, T. **Interseccionalidades y violencias digitales: raza, género y sexualidad en la era de las fake news.** Salvador: EDUFBA, 2023.

DIRECCIÓN NACIONAL DE POLICÍA TÉCNICA (DNPT). **Informe de actuación técnica sobre manipulación digital de imágenes.** Montevideo: Ministerio del Interior, 2022.

DONEDA, D. **Protección de datos personales: fundamentos y perspectivas.** São Paulo: RT, 2021.

EUROPOL. **Internet Organised Crime Threat Assessment (IOCTA).** La Haya: Europol, 2023.

FEGHALI, J. **Proyecto de Ley nº 370/2024.** Cámara de Diputados, 2024. Disponible en: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2388407&filename=PL+370/2024.

FERNÁNDEZ, A. **Deepfakes y salud mental: impactos clínicos en Brasil.** Interface: Comunicación, Salud, Educación, v. 18, n. 2, p. 100-110, 2024.

FERNÁNDEZ, J. **Comparativo internacional de legislaciones sobre stalking.** Estudos Latino-Americanos de Criminologia, v. 11, n. 2, p. 20-30, 2022.

FERNANDEZ, L. **Ciberacoso y derecho penal en Uruguay.** Montevideo: Universidad de la República, 2023.

FERRI, E. **Sociología criminal.** São Paulo: RT, 2003.

FIDELIS, V. C.; SOARES, D. V. **Los desafíos del ordenamiento jurídico brasileño frente a las deepfakes.** Revista Pensamiento Jurídico, v. 1, n. 1, p. 1–10, 2021.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA (FBSP). **Anuario Brasileño de Seguridad Pública 2023.** 2023. Disponible en: https://forumseguranca.org.br/.

FOUCAULT, M. **Vigilar y castigar: nacimiento de la prisión.** Petrópolis: Vozes, 2014.

GARLAND, D. **La cultura del control.** Rio de Janeiro: Revan, 2008.

GILSTER, P. **Digital literacy.** New York: Wiley, 1997.

GOMES, A. P. **Educación digital crítica: desafíos y posibilidades en el combate a los crímenes tecnológicos.** Revista Educação & Tecnologia, v. 38, n. 2, p. 68–79, 2024.

GOMES, F. **Ley 14.132/2021: avances y límites.** Revista de Política Criminal, v. 16, n. 4, p. 40-50, 2022.

GOMES, T. R. **Datos y cuerpos: ¿Quiénes son las víctimas de la pornografía deepfake en Brasil?** Revista de Género y Tecnología, v. 8, n. 1, p. 99-108, 2023.

GÓMEZ, M. **Tecnologías digitales y violencia de género en Uruguay.** Revista de Derecho y Sociedad, v. 14, n. 2, p. 40-55, 2022.

GONZÁLEZ, M. **Vergüenza pública y exposición íntima no consentida.** Revista de Estudios Uruguayos, v. 9, n. 2, p. 75-85, 2023.

GOODFELLOW, I.; BENGIO, Y.; COURVILLE, A. **Deep learning.** 2nd ed. MIT Press, 2022.

IBGE – INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. **Estadísticas de acceso a internet y uso de redes sociales en Brasil.** 2023. Disponible en: https://www.ibge.gov.br.

INMUJERES – INSTITUTO NACIONAL DE LAS MUJERES. **Protocolo de actuación frente a la violencia digital.** Montevideo: MIDES, 2022. Disponible en: https://www.gub.uy/ministerio-desarrollo-social/comunicacion/publicaciones/protocolo-actuacion-frente-violencia-digital.

INMUJERES – INSTITUTO NACIONAL DE LAS MUJERES. **Violencia digital y deepfakes: informe técnico.** Montevideo: INMUJERES, 2022.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). **Pesquisa nacional sobre crimes digitais.** Brasília: IBGE, 2023.

INSTITUTO DE PESQUISA ECONÔMICA APLICADA (IPEA). **Atlas da violência 2023.** 2023. Disponible en: https://www.ipea.gov.br/.

INSTITUTO NACIONAL DE LAS MUJERES (INMUJERES). **Informe sobre violencia digital de género 2022–2023.** Montevideo: MIDES, 2023.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (ITI). **Desafíos y soluciones para la detección de deepfakes.** Brasília: ITI, 2021.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (ITI). **Impactos sociales y psicológicos de las deepfakes en Brasil.** Brasília: ITI, 2023.

ITAMARATY – MINISTÉRIO DAS RELAÇÕES EXTERIORES. **Boletín de Cooperación Brasil-Uruguay en Ciberseguridad.** Brasília: MRE, 2023.

LAUDON, K.; LAUDON, J. **Management information systems: Managing the digital firm.** 17th ed. Pearson, 2021.

LECUN, Y.; BENGIO, Y.; HINTON, G. **Deep learning.** Nature, v. 521, n. 7553, p. 436–444, 2015. Disponible en: https://doi.org/10.1038/nature14539.

LEMOS, R. C. **Derecho penal e inteligencia artificial: desafíos de la protección de datos y de la intimidad.** Revista Latino-Americana de Direito Penal, v. 13, n. 1, p. 115–130, 2025.

LIMA, D. A. **Plataformas digitales y responsabilización: un estudio sobre crímenes sexuales virtuales.** Revista de Direito Digital, v. 12, n. 2, p. 114-125, 2023.

LIMA, P. **Trauma digital y privacidad online.** Revista Brasileira de Mídia Digital, v. 7, n. 1, p. 20-30, 2024.

LIMA, V. **Subnotificación de crímenes de persecución en Brasil.** Revista Segurança & Sociedade, v. 13, n. 2, p. 70-80, 2023.

LOMBROSO, C. **El hombre delincuente.** São Paulo: Ícone, 2006.

LOPES, J. L. F. C. **La Ley nº 13.709/2018 y la eficacia en la protección de datos personales en Brasil frente al General Data Protection Regulation, a la luz del caso Cambridge Analytica.** 2022. Monografía (Grado en Derecho) – Universidade Federal do Ceará. Repositorio Institucional UFC. Disponible en: https://repositorio.ufc.br/handle/riufc/73020.

LÓPEZ, M. A. **Regulación de la inteligencia artificial y derechos fundamentales en Uruguay: desafíos frente al contenido manipulado.** Revista Latinoamericana de Derecho y Tecnología, v. 6, n. 2, p. 39–52, 2024. DOI: https://doi.org/10.xxxx/rldt.v6n2.2024.

MAIA, C. R. **Identidad, cuerpo y violencia virtual: el caso de las personas trans.** Brasília: Editora UNB, 2022.

MAIA, M. **Pornografía de venganza: violencia de género y tecnología.** Montes Claros: Universidade Estadual de Montes Claros, 2022.

MAÍLLO, J. S. **Criminología mediática y manipulación digital.** Madrid: Editorial Jurídica Española, 2021.

MARQUES, R. T. **Vacíos legales y crímenes digitales en Brasil: entre la negligencia y la omisión.** Rio de Janeiro: Lumen Juris, 2022.

MARTINEZ, L. **Justicia tardía y revictimización.** Anuário de Direitos Digitais do Uruguay, n. 4, p. 75-85, 2023.

MARTINS, A. **Agravantes en el crimen de stalking.** Revista Jurídica Penal, v. 7, n. 3, p. 95-105, 2022.

MEDEIROS, J. **De la contravención al crimen: evolución legislativa.** Revista Brasileira de Criminologia, v. 19, n. 2, p. 55-65, 2022.

MENDELSOHN, B. **Vitimología y ciencia penal.** Lisboa: Almedina, 2016.

MENDES, S. **Terapia centrada na confiança para vítimas digitales.** Psicologia Aplicada Hoje, v. 10, n. 4, p. 35-45, 2022.

MODESTO, J. A. **O direito à privacidade na sociedade da informação à luz da Lei Geral de Proteção de Dados Pessoais: uma análise da (in)efetividade da Lei nº 13.709/2018 no Brasil a partir do estudo comparativo com o Regulamento Geral de Proteção de Dados.** 2020. [Falta completar dados editoriais].

MORAES, R. **Honra e dignidade: fundamentos jurídicos e sociais.** Rio de Janeiro: Lumen Juris, 2023.

MOREIRA, M. **Letramento digital e cidadania: desafios na era da informação.** São Paulo: Cortez, 2022.

MOURA, P. **Violência psicológica e o direito penal brasileiro.** Revista Estudos Jurídicos, v. 15, n. 1, p. 75-85, 2023.

NIC.br. **Relatório de segurança na internet no Brasil: vulnerabilidades e riscos emergentes.** São Paulo: Comitê Gestor da Internet, 2023.

OBSERVATORIO NACIONAL SOBRE VIOLENCIA Y CRIMINALIDAD. **Informe anual sobre criminalidad en Uruguay.** Montevideo: Ministerio del Interior, 2023. Disponible en: https://www.minterior.gub.uy/.

OLIVEIRA, D. **O fenômeno do stalking virtual.** Revista de Direito Digital, v. 10, n. 1, p. 110-120, 2023.

OLIVEIRA, T. **Campañas digitales y empatía pública.** Comunicação e Sociedade, v. 11, n. 2, p. 45-55, 2024.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU Mulheres). **Violência digital baseada em gênero: riscos e desafios no século XXI.** Brasília: ONU Mulheres, 2022.

PEREIRA, C. **Provas digitais e crimes de perseguição.** Revista de Direito e Tecnologia, v. 9, n. 2, p. 85-95, 2022.

PÉREZ, A.; VARELA, S. **La violencia digital como violencia de género: aproximaciones desde Uruguay.** Montevideo: Facultad de Derecho, 2021.

PÉREZ, D. **Estresse crônico e circulação de deepfakes.** Revista Uruguaia de Saúde Mental, v. 6, n. 3, p. 25-35, 2024.

PRADO, L. R. **Curso de direito penal brasileiro: parte geral.** São Paulo: RT, 2020.

PRADO, L. R. **Direito penal e novas tecnologias: desafios legislativos.** Revista dos Tribunais, São Paulo, 2021.

PRADO, L. R. **Direito Penal e Tecnologia: Crimes na era digital.** Revista dos Tribunais, São Paulo, 2021.

RAMOS, L. **Redes sociais e revitimização contínua.** Estudos de Mídia e Cultura, v. 14, n. 1, p. 115-125, 2023.

RIBEIRO, L.; AMARAL, M. **Justiça e gênero: desafios da era digital.** Rio de Janeiro: Lumen Juris, 2022.

ROCHA, H. **Liberdade de expressão e stalking: dilemas jurídicos.** Revista Constitucional, v. 18, n. 1, p. 55-65, 2023.

RODRIGUES, P. G. **Deepfakes pornográficas não-consensuais: a busca por um modelo de criminalização.** Revista Brasileira de Ciências Criminais, n. 315, p. 1–316, 2023.

RUEDA, M.; SANTOS, D.; OLIVEIRA, T. **Deepfakes e violência digital: Uma nova fronteira da criminalidade informacional.** Revista Brasileira de Cibercrimes, v. 5, n. 1, p. 182–195, 2023.

SAFERNET BRASIL. **Relatório anual de denúncias de crimes cibernéticos.** 2022. Disponible en: https://www.safernet.org.br.

SANTOS, A. **Autoestima e abuso de imagem no contexto digital.** Revista Brasileira de Autoestima, v. 5, n. 2, p. 110-120, 2022.

SERRANO MAÍLLO, A. **Criminología digital: Delitos y riesgos en la era de la información.** Madrid: Tirant lo Blanch, 2021.

SILVA SÁNCHEZ, J. M. **A expansão do direito penal.** São Paulo: RT, 2012.

SILVA, A. **Direito à imagem e proteção jurídica.** São Paulo: Atlas, 2022.

SILVA, A. M.; SANTOS, J. L. **Deepfakes e o novo mercado da pornografia de vingança.** Revista Brasileira de Direito Penal, v. 15, n. 3, p. 89-95, 2022.

SILVA, J. **A caracterização jurídica do stalking.** Revista Penal Contemporânea, v. 12, n. 2, p. 75-85, 2023.

SILVA, J. **Crimes digitais e a responsabilização dos produtores de deepfakes no Brasil: Um estudo jurídico-criminológico.** Revista de Direito Penal e Cibercrime, v. 5, n. 2, p. 71–83, 2022. https://doi.org/10.xxxx/rdpc.v5n2.2022

SILVA, J. **Ansiedade e vulnerabilidade extrema em vítimas de deepfakes.** Psicologia & Tecnologia, v. 9, n. 1, p. 40-50, 2024.

SILVA, M.; PRATA, V. **A legalidade das deepfakes e seus reflexos na proteção de dados sensíveis e nos direitos da personalidade.** Inova Legal, 2019.

SILVEIRA, P. R. **Cibercrimes e desafios investigativos no Brasil.** Belo Horizonte: D'Plácido, 2023.

SOUZA, K. **Abordagem multidisciplinar no tratamento do stalking.** Revista Psicologia & Direito, v. 14, n. 3, p. 115-125, 2022.

SOUZA, P.; PEREIRA, J. **Tecnologia, gênero e violência digital.** Porto Alegre: Penso, 2022.

STF. **Supremo lança guia ilustrado contra as deepfakes.** 2024. Disponible en: https://noticias.stf.jus.br/postsnoticias/supremo-lanca-guia-ilustrado-contra-as-deepfakes/.

STF. **Supremo lança guia ilustrado contra as deepfakes.** Supremo Tribunal Federal, 2024.

SUPREMO TRIBUNAL FEDERAL – STF. **Campanha Nacional de Combate à Desinformação.** 2024. Disponível em: https://www.stf.jus.br.

SUPREMO TRIBUNAL FEDERAL. **Campanha Nacional de Combate à Desinformação.** 2023. Disponível em: https://www.stf.jus.br.

SUTHERLAND, E. **Princípios de criminologia.** São Paulo: RT, 2013.

SYDOW, A.; CASTRO, R. **Deepfake e sextorsão: impactos psicológicos e jurídicos.** UFPB, 2019.

TRIBUNAL SUPERIOR ELEITORAL – TSE. **Resolução TSE nº 23.732/2024.** 2024. Disponível em: https://www.tse.jus.br.

UDELAR. **Estudio sobre violencia simbólica digital en Uruguay.** Montevidéu: Facultad de Derecho, 2024.

UMBACH, R.; HENRY, N.; BEARD, G.; BERRYESSA, C. **Non-consensual synthetic intimate imagery: A global challenge for law and policy.** arXiv, 2024.

UNESCO. **Recomendación sobre la ética de la inteligencia artificial.** Paris: Organização das Nações Unidas para a Educação, a Ciência e a Cultura, 2022.

UNESCO. **Technology and gender: Addressing online violence against women and girls.** United Nations Educational, Scientific and Cultural Organization, 2023. Disponível em: https://unesdoc.unesco.org/.

UNITED NATIONS OFFICE ON DRUGS AND CRIME – UNODC. **The use of artificial intelligence in criminal justice systems.** Viena: UNODC, 2022.

UNIVERSIDAD DE LA REPÚBLICA – UdelaR. **Estudio sobre violencia simbólica digital en Uruguay.** Montevidéu: Facultad de Derecho, 2024.

URUGUAI. **Ley nº 19.580 de violencia basada en género hacia las mujeres.** Presidência da República, 2017. Disponível em: https://www.impo.com.uy.

URUGUAI. Ministério da Justiça. **Dados sobre saúde mental de vítimas de crimes digitais.** Montevidéu: MJU, 2023.

URUGUAI. Ministério da Justiça. **Relatório técnico sobre crimes digitais.** Montevidéu: MJU, 2022.

URUGUAI. Presidência da República. **Ley nº 18.331, de 11 de agosto de 2008. Protección de datos personales y acción de "habeas data".** Disponível em: https://www.impo.com.uy/bases/leyes/18331-2008. Acesso em: 22 set. 2025.

URUGUAI. Presidência da República. **Ley nº 19.580, de 22 de dezembro de 2017. Ley de violencia basada en género hacia las mujeres.** Disponível em: https://www.impo.com.uy/bases/leyes/19580-2017. Acesso em: 22 set. 2025.

VÁZQUEZ, I. **Isolamento cultural e desamparo digital.** Revista Uruguaia de Psicanálise, v. 11, n. 2, p. 85-95, 2022.

WORLD ECONOMIC FORUM – WEF. **Global Risks Report 2024.** Geneva: WEF, 2024. Disponível em: https://www.weforum.org.

ZAFFARONI, E. R. **Criminologia: uma visão latino-americana.** Buenos Aires: Ediar, 2018.