



FACULTAD DE
DERECHO



UNIVERSIDAD
DE LA REPÚBLICA
URUGUAY

Derecho penal internacional, imagen e intimidad: Vulneraciones transfronterizas de los derechos de las mujeres mediante tecnología *deepfake*

Martina Lamaita Osano

Monografía Final de Grado para la Licenciatura en Relaciones
Internacionales

de la
Facultad de Derecho

Universidad de la República

martinalamaita@gmail.com

Tutor: Dr. Lic. Marcos Dotta

Montevideo, Uruguay, Mayo de 2025

Agradecimientos

Este trabajo marca el cierre de cuatro años de intenso esfuerzo, en los que el estudio, la dedicación y la superación de desafíos han sido parte fundamental de mi crecimiento personal y académico. A lo largo de este proceso, he contado con el apoyo de personas excepcionales, cuya orientación, compañía e inspiración han sido esenciales para llegar hasta este punto.

En primer lugar, agradezco a mis padres, Verónica y Martín, quienes me enseñaron el valor del esfuerzo, la constancia y la perseverancia. A mis abuelos, Susana y Enrique, en cuyo apoyo y aliento sé que siempre podré confiar. A mi tía Leticia, por su paciencia, contención y ayuda incondicional a lo largo de los años. Han sido un pilar en cada etapa de mi vida.

A Agustín, por su comprensión en los momentos de mayor exigencia académica y por acompañarme sin reservas en este camino. A Camila, mi compañera en esta carrera y una amiga invaluable, por compartir este recorrido con entusiasmo, apoyo mutuo y largas conversaciones que hicieron todo más llevadero.

Extiendo mi gratitud a todos los profesores de la Licenciatura en Relaciones Internacionales, quienes han enriquecido mi formación a través de su enseñanza y vocación. Un reconocimiento especial a mi tutor, Marcos Dotta, quien, junto con su equipo docente, supo transmitir su entusiasmo y pasión por el Derecho Internacional Privado. Su guía, confianza y paciencia fueron fundamentales para la culminación de este proceso.

Gracias a todos.

Índice

Agradecimientos	2
Capítulo I	1
1. Resumen ejecutivo	1
2. Introducción	1
Capítulo II	3
2. Problema objeto de estudio	3
2.1 Justificación	3
2.2 Pregunta de investigación	4
2.3 Objetivos	4
2.3.1 General	4
2.3.2 Específicos	5
2.4 Fundamentación teórica	5
2.4.1 Humanidad en el espejo digital: explorando el impacto de los <i>deepfakes</i> en la privacidad	5
2.4.2 Construyendo significados: el papel de la teoría constructivista de las Relaciones Internacionales para entender los Derechos Humanos	9
2.4.3 Haciendo justicia en el ciberespacio: Derecho Internacional Privado y Penal en acción	11
Capítulo III	18
3. <i>Íter deepfake</i> : proceso a través del cual se genera el contenido <i>deepfake</i>	18
4. ¿Por qué las mujeres?	23
4.1 La brecha de datos de género y la Agenda 2030	23
4.2 Reseña de casos: la mujer en un imaginario falsificado y perverso	29
5. De Budapest a Montevideo: puentes y fisuras en la regulación global de la ciberdelincuencia	33
5.1 El Convenio de Budapest sobre Ciberdelincuencia (2001)	33
5.2 Convención sobre Ciberdelincuencia de Naciones Unidas (2024)	36
5.2.1 Contexto del inicio de las negociaciones y algunas controversias	36
5.2.2 Análisis normativo: algunas comparaciones con el Convenio de Budapest (2001)	37
5.3 Uruguay frente a los desafíos tecnológicos: normativa, estrategias e inteligencia artificial	40
5.3.1 Posicionamiento y estrategias nacionales: hacia una agenda tecnológica inclusiva y ética	40
5.3.2 La Ley N.º 20.327 en perspectiva internacional: un análisis comparativo con el Convenio de Budapest (2001) y la Convención de Naciones Unidas sobre Ciberdelitos (2024)	42
Capítulo IV	47
6. Conclusiones: El papel de las normas internacionales en la protección de los derechos a la imagen y a la intimidad de las mujeres (y de todas las personas)	47
Bibliografía	51

Capítulo I

1. Resumen ejecutivo

El desarrollo de la inteligencia artificial ha intensificado los desafíos en la protección de la privacidad, los derechos de imagen y la intimidad, afectando especialmente a las mujeres a través del uso de deepfakes con fines de explotación. Este trabajo analiza cómo el marco normativo internacional en el Derecho Penal Internacional aborda estas vulneraciones transfronterizas.

Desde un enfoque constructivista y comparativo, se examinan el Convenio de Budapest (2001), la Convención de la ONU sobre Ciberdelincuencia (2024) y la Ley N° 20.327 de Uruguay, identificando sus alcances y limitaciones. Se evidencia que, pese a los avances en la regulación de los ciberdelitos, la protección de las víctimas de deepfakes sigue siendo insuficiente.

El estudio concluye que la falta de un marco normativo unificado y la escasa representación de mujeres en la toma de decisiones obstaculizan regulaciones efectivas. Se resalta la necesidad de un enfoque interdisciplinario que integre el Derecho, las Relaciones Internacionales y la Neurociencia para abordar el impacto de la inteligencia artificial en la reproducción de desigualdades estructurales.

Palabras clave: Inteligencia artificial, *deepfakes*, ciberdelincuencia, Derecho Penal Internacional, privacidad, derechos de imagen, cooperación internacional, brecha de datos de género, violencia digital.

2. Introducción

A lo largo del último siglo, los avances tecnológicos han redefinido no solo las dinámicas sociales y económicas, sino también los marcos legales internacionales. Desde la aparición de las primeras redes digitales hasta el auge de la inteligencia artificial (IA), el desarrollo tecnológico ha traído consigo tanto oportunidades como desafíos éticos y jurídicos. Uno de los fenómenos más recientes y controvertidos es el de los *deepfakes*, contenido audiovisual manipulado que, mediante el uso de algoritmos avanzados, genera simulaciones altamente realistas. Aunque esta tecnología ha encontrado aplicaciones legítimas en sectores como el entretenimiento, también ha sido empleada para fines ilícitos, como la difusión de contenido sexual no consentido, afectando desproporcionadamente a las personas.

El surgimiento de los *deepfakes* marca un punto crítico en la evolución de las tecnologías digitales, donde los límites entre realidad y manipulación se desdibujan. Este fenómeno plantea preguntas fundamentales para el Derecho Penal Internacional y la cooperación transfronteriza, particularmente cuando estas prácticas vulneran derechos de imagen e intimidad de las personas. Además, la proliferación de estas tecnologías facilita el acceso personalizado a contenido pornográfico exclusivo, perpetrando la dependencia y adicción de quienes lo consumen con regularidad. En un contexto globalizado, estas violaciones no se acotan a un solo territorio, lo que exige respuestas normativas que armonicen los marcos legales de distintos Estados y garanticen la protección efectiva de las víctimas, las cuales no se limitan a quienes ven su imagen manipulada, sino que también incluyen a los consumidores adictos.

Sin perjuicio de lo anterior, esta monografía analiza cómo han sido diseñadas las normativas internacionales para abordar las vulneraciones transfronterizas asociadas a la manipulación de imagen e intimidad de las mujeres mediante *deepfakes* pornográficos, teniendo a los autores de los mismos como los criminales a imputar. Para ello, se considerarán instrumentos internacionales como el Convenio de Budapest (2001), la Convención sobre Ciberdelincuencia de Naciones Unidas (2024) y, como normativa nacional, la Ley N° 20.327 de Tipificación de Ciberdelitos en Uruguay. Al incorporar la teoría constructivista de las Relaciones Internacionales, se examinan las dinámicas internacionales que influyen en la creación de estos marcos, así como sus implicancias para los derechos humanos, especialmente teniendo en cuenta la brecha de datos de género y las consecuencias de la normalización del consumo de pornografía en la sociedad internacional.

El análisis se sitúa en un momento histórico donde la tecnología, la justicia y los derechos humanos convergen, destacando la necesidad de un marco legal internacional que no solo responda a las amenazas actuales, sino que también anticipe los desafíos éticos y jurídicos del futuro digital.

Capítulo II

2. Problema objeto de estudio

2.1 Justificación

En un mundo donde los vínculos transfronterizos son parte de la cotidianeidad de los Estados, las relaciones digitales han ascendido en relevancia, interconectando también a los individuos. Es en este contexto que se observa con atención el desarrollo y auge de la inteligencia artificial, en un sistema internacional que debe centrarse en crear un marco jurídico que la ordene y regule.

La ausencia de normas internacionales es un problema si se conjuga con el alza en la variedad de los usos dados a estas tecnologías, así como el incremento en su sofisticación y las complicaciones en la detección de su empleo. La inteligencia artificial (IA) no es, *per sé*, un “mal a erradicar” en el sistema internacional, pero plantea serias amenazas para la protección de ciertos Derechos Humanos fundamentales, generando riesgos y menoscabos tangibles o intangibles (R (UE) 2024/1689 de 13 de junio de 2024). Es decir, la IA puede ser empleada indebidamente, proporcionando herramientas nuevas y poderosas “para llevar a cabo prácticas de manipulación, explotación y control social” (R (UE) 2024/1689 de 13 de junio de 2024). En la actualidad, cualquier persona, o usuarios anónimos, que tenga acceso a una tienda de aplicaciones, en cualquier dispositivo y desde cualquier parte del mundo, puede crear, mediante la fotografía de otro, un video o imagen completamente manipulado. El acceso público a estas tecnologías facilita, sin distinciones económicas, ni necesidad de habilidades tecnológicas extraordinarias (Franganillo, 2022), realizar o finalizar un producto verosímil con pocas o nulas repercusiones jurídicas.

Por lo expuesto, el trabajo adopta un diseño de investigación orientado a analizar de forma crítica cómo ha sido diseñado el marco normativo internacional en el Derecho Penal Internacional para responder a las vulneraciones transfronterizas de los derechos de imagen y a la intimidad de las mujeres mediante contenido *deepfake*. Desde una perspectiva constructivista, y a partir de un enfoque comparativo, se analizará el Convenio de Budapest del año 2001, la Convención de las Naciones Unidas sobre Ciberdelincuencia, y la Ley N° 20.327 para la Tipificación de Ciberdelitos del Uruguay como marcos jurídicos potencialmente aplicables a los casos de vulneración de los derechos de imagen e intimidad

de las personas físicas; esto, sin excluir la posibilidad de que se legisle especialmente el uso de inteligencia artificial.

Asimismo, el desarrollo de esta monografía se centrará en la situación de las mujeres; no es una elección al azar, sino por la convicción de que se encuentran en una posición vulnerable y expuesta a la manipulación de su imagen y datos personales en forma dolosa (Cerdán y Padilla, 2019), incrementándose la gravedad de la acción antijurídica por su trascendencia de las fronteras estatales. En este sentido, la proliferación de *deepfakes* pornográficos no solo refuerza dinámicas de violencia digital, sino que también se vincula con el consumo compulsivo de contenido pornográfico, cuya accesibilidad y personalización han intensificado patrones adictivos en la sociedad contemporánea (Wilson, 2014). Este fenómeno, al normalizar la cosificación de las mujeres y perpetuar la brecha de datos de género, plantea desafíos adicionales para la regulación de la IA y la protección de los derechos de imagen y a la intimidad. Por lo tanto, se busca contribuir al entendimiento y discusión académica sobre el Derecho Penal Internacional en el contexto de la inteligencia artificial, promoviendo una mayor conciencia y protección de los derechos de imagen y a la intimidad de las mujeres en este entorno digital en constante evolución, en un sistema internacional que se ha comprometido, entre otras cosas, a lograr la igualdad de género.

2.2 Pregunta de investigación

¿De qué manera la ausencia de una regulación explícita sobre los *deepfakes* en el Derecho Penal Internacional contribuye a la perpetuación de la brecha de datos de género y al refuerzo de patrones de consumo de la pornografía, y qué limitaciones presentan los marcos normativos existentes en la protección de los derechos de imagen e intimidad de las mujeres?

2.3 Objetivos

2.3.1 General

Analizar cómo la ausencia de una regulación explícita sobre los *deepfakes* en el derecho penal internacional impacta en la perpetuación de la brecha de datos de género y en el refuerzo de patrones de consumo de la pornografía, identificando las limitaciones de los marcos normativos existentes en la protección de los derechos de imagen e intimidad de las mujeres.

2.3.2 Específicos

- a. Describir el *iter criminis* seguido por los ejecutores de la generación de contenido *deepfake*.
- b. Justificar por qué las mujeres son sujetos expuestos a la manipulación de sus derechos e imagen y a la intimidad por medio de creación de contenido pornográfico a través de tecnología *deepfake*, en el contexto de la Agenda 2030 y el Pacto para el Futuro.
- c. Estudiar comparativamente el Convenio de Budapest (2001), la Convención sobre Ciberdelitos de la ONU (2024) y la Ley N° 20.327, indicando sus debilidades y fortalezas en la responsabilización de los ejecutores de la generación de contenido *deepfake* pornográfico.
- d. Analizar cómo el papel de las normas internacionales, en clave constructivista, puede aportar al desarrollo y amparo de los derechos a la imagen y la intimidad contemplando la brecha de datos de género, en contribución a la Agenda 2030.

2.4 Fundamentación teórica

2.4.1 Humanidad en el espejo digital: explorando el impacto de los *deepfakes* en la privacidad

Antes de poder iniciar con la articulación de las teorías propiamente dichas que sustentan el presente trabajo, parece pertinente definir preliminarmente algunos conceptos auxiliares. En primer lugar, se debe delimitar qué se entenderá por inteligencia artificial (IA). El concepto fue empleado por primera vez en 1955 en un proyecto de investigación del Dartmouth College, pero es de mayor relevancia el hecho de que la ciencia jurídica lo explora desde 1960. Mendoza (2020) indica que la misma se compone de: “sistemas que manifiestan un comportamiento inteligente, al ser capaces de analizar el entorno y realizar acciones, con cierto grado de autonomía, con el fin de alcanzar objetivos específicos” (p. 182). La autora advierte que actualmente existen nuevas ramas derivadas de este concepto, por lo que su alcance irá “evolucionando a la par de los avances tecnológicos en la materia” (p. 182).

Recientemente, la Unión Europea publicó el Reglamento de la Inteligencia Artificial, y en su artículo 3, inciso 1, se entiende por sistema de IA:

un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones,

contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales;

Como se puede ver, esta definición complementa a la anterior, ya que incorpora la idea de que el accionar de la IA no sólo tiene influencia en el ciberespacio, sino también en el plano físico. Tener en cuenta esto último será de capital importancia, pues, como se verá, el ciberespacio y el mundo físico ya no son cosas separadas.

En segundo lugar, se empleará el concepto de *deepfake*¹ entendiéndolo como una de estas ramas derivadas. Así, siguiendo a Franganillo (2019), el *deepfake* es:

la técnica de inteligencia artificial capaz de generar vídeos manipulados con un aspecto tan realista que hace difícil notar que han sido falseados. Para ello se emplea una clase de algoritmos conocida como “redes generativas antagónicas”, que a través del aprendizaje profundo pueden generar, sin intervención humana, imágenes o voces que parecen auténticas (p. 3).

Finalmente, se parte de la hipótesis de que, en ausencia de un marco jurídico especial, la tecnología de IA generativa resulta alarmante para la protección de Derechos Humanos fundamentales tales como la imagen y la intimidad en línea, ya que pueden generarse audiovisuales falsos que parecen auténticos, incluso en representación de personas físicas reales en situaciones falsas o comprometedoras. Como sostiene Trujillo Cabrera (2024), estos audiovisuales están basados en redes neuronales que “analizan grandes conjuntos de muestras de datos para aprender a imitar las expresiones faciales, los gestos, la voz y las inflexiones de una persona.” (p. 82)². Agregando que el uso de dicha tecnología no está reservado a un grupo de expertos exclusivo, plantea serias implicaciones para la integridad de la información y la reputación de las personas, así como la protección de su privacidad y dignidad, excediendo al Estado como actor central. De hecho, según el Libro Blanco sobre la IA (que reseña el enfoque europeo orientado a la excelencia y la confianza), el impacto de los usos de estos sistemas de IA se debe considerar desde la perspectiva de la sociedad en su conjunto. Asimismo, el nuevo Reglamento de la Unión previamente citado menciona numerosas veces en su preámbulo la necesidad de desarrollar a la IA centrada en el ser humano.

Previamente se mencionaron los derechos a la imagen y a la intimidad, por lo cual parece lógico continuar definiendo qué se entenderá por tales. De acuerdo con Acale Sánchez (2013) la imagen personal refleja ante uno mismo, terceros y la sociedad entera una serie de

¹ En español, “contenido ultrafalso”, siendo uno de los posibles productos de la IA generativa.

² En el siguiente capítulo se informará en profundidad respecto de la creación de *deepfakes*, de su funcionamiento y del papel que desempeña la figura humana en éste.

datos que identifica e individualiza a las personas del resto, y ata este concepto al de intimidad, pues entiende que a través de la imagen “viaja” la intimidad. Seguidamente, la autora indica que ambas son facetas de la personalidad que permiten a los individuos desarrollarse libremente, con la posibilidad de reservar parte de sí mismos al mundo, ejerciendo la voluntad privada.

Con el mismo sentido, Sáez Tapia (2017) agrega que el derecho a la imagen se vincula estrechamente con el concepto kantiano de dignidad humana, y es parte de una nueva formación de derechos subjetivos que se ha consolidado con el desarrollo de las nuevas tecnologías, en virtud de lo cual las personas ya no sólo consumen información y contenido en general, sino que actualmente son objeto y protagonistas del universo virtual, dando forma a la construcción de una imagen propia en el ciberespacio. La autora indica que la protección de este derecho se encuentra orientada a la dimensión moral de las personas, atribuyendo a su titular un derecho a determinar la información generada por sus rasgos y su personalidad, que pueden tener difusión pública.

En la Constitución de la República, los artículos 72 y 332 reconocen implícitamente estos derechos, por lo que se puede decir que el ordenamiento jurídico uruguayo está inclinado a protegerlos. Dicen los mencionados artículos:

(Artículo 72) - La enumeración de derechos, deberes y garantías hecha por la Constitución, no excluye los otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno.

(Artículo 332) - Los preceptos de la presente Constitución que reconocen derechos a los individuos, así como los que atribuyen facultades e imponen deberes a las autoridades públicas, no dejarán de aplicarse por falta de la reglamentación respectiva, sino que ésta será suplida, recurriendo a los fundamentos de leyes análogas, a los principios generales de derecho y a las doctrinas generalmente admitidas.

Siguiendo a Fagioli y Sanguinetti (2019), lesionar este derecho supone un “avasallamiento a la propia personalidad, dado que priva al sujeto de decidir sobre la divulgación o no de su retrato” (p. 1). Asimismo, las autoras mencionan el artículo 21 de la ley 9.739 del 17 de diciembre de 1937, el cual regula de forma expresa la situación del titular del derecho a la imagen, profundizando la protección genérica que le otorga la Constitución. El principio general allí establecido es que la imagen de un sujeto no puede ser divulgada sin

su consentimiento expreso, sin perjuicio de que existe un régimen de publicaciones libres, el cual no es objeto del presente trabajo.

En aras de integrar los artículos constitucionales mencionados, y recordando que es la voluntad del Estado uruguayo obligarse por éste instrumento internacional, parece pertinente mencionar el artículo 12 de la Declaración Universal de Derechos Humanos de 1948:

Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

Es citado el anterior tratado, sin perjuicio de que se reporta la existencia de otros instrumentos con la misma vocación, que han sido ratificados por el Uruguay y que por tanto lo obligan en el mismo sentido. Son algunos ejemplos, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos de 1966, el Pacto de San José de Costa Rica de 1970, entre otros. Sin embargo, ninguno de estos textos aporta una noción clara del significado del derecho a la intimidad o del derecho a la propia imagen, por lo que es pacíficamente aceptado que su conceptualización ha venido de la mano de la jurisprudencia de los tribunales (Morales Montilla, 2020). En tal sentido, la autora menciona, para definir el derecho a la propia imagen, un pronunciamiento dado por el Tribunal Supremo de España, el cual divide al nombrado derecho en dos facetas: “una positiva que ‘atribuye a su titular la facultad de disponer de la representación de su aspecto físico que permita su identificación y le permite determinar qué información gráfica generada por sus rasgos físicos personales puede tener dimensión pública’” y otra negativa que “impide la obtención o publicación de la imagen sin consentimiento expreso de su titular, independientemente del fin y del tercero que la exponga” (Morales Montilla, 2020, p. 10).

En cuanto al derecho a la intimidad, el Tribunal Constitucional español lo define como “la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario —según las pautas de nuestra cultura— para mantener una calidad mínima de la vida humana” y que inicia a considerarse como un bien y poder jurídico, agregándose “la facultad de imponer a terceros (sean estos simples particulares o poderes públicos), su voluntad de no dar a conocer dicha información, prohibiendo su difusión no consentida” (Morales Montilla, 2020, pp. 9-10).

A razón de lo desarrollado en la presente sección, el uso de redes sociales (es decir, X —antes Twitter—, Instagram, Facebook y TikTok, entre otras), aumenta la facilidad para publicar información de forma automática y anónima, así como la velocidad a la que se

comparte la misma. Esto contribuye a un fenómeno conocido como “hiperdesarrollo fáctico de las libertades de información y expresión”, que se caracteriza por romper con el equilibrio que existía con los derechos de la personalidad, llevando a nuevas amenazas que dan pie a nuevas versiones de difamación internacional: en la actualidad no es necesario que existan vínculos entre el Estado del creador, el difusor, el lugar de la infracción de los derechos de la personalidad o el del domicilio del sujeto sobre el que versa el propio contenido. La conclusión lógica de la articulación de estos conceptos es que las víctimas se encuentran en una posición de especial vulnerabilidad cuando la violación a su derecho a la intimidad y a la propia imagen es llevado a cabo mediante el ciberespacio, donde se puede acceder al contenido dañino de forma global (Morales Montilla, 2020).

Seguidamente se pasará a estructurar el marco teórico que soportará el estudio de la situación previamente ilustrada. Para esto, se desarrollarán conceptos propios de la disciplina del Derecho Internacional Privado, entendiendo que es en su rama Penal que se debe buscar una verdadera solución a este fenómeno al que se enfrenta la sociedad internacional. Asimismo, será de gran ayuda el aporte que la Teoría Constructivista de las Relaciones Internacionales hace al entendimiento de la manera en que las normas jurídicas forman el sistema internacional.

2.4.2 Construyendo significados: el papel de la teoría constructivista de las Relaciones Internacionales para entender los Derechos Humanos

Los argumentos de esta monografía se sustentarán en la teoría constructivista, dentro de la Teoría de las Relaciones Internacionales. Sanahuja (2015) la define como la “aproximación teórica que se ocupa de la conciencia humana y de su papel en la vida internacional. El estudio de los hechos sociales, como hechos que existen a partir de sus acuerdos colectivos que se mantienen a través de instituciones” (p. 189). El enfoque está puesto, en palabras del autor, en la dimensión ideacional de la sociedad y la política, colocando esta teoría en el campo más reflectivista de las Relaciones Internacionales.

Surgido al final de la Guerra Fría (en un momento en el que las teorías tradicionales neorrealistas y neoliberales fueron tachadas de incapaces de predecir el desenlace de dicho conflicto), en tanto que viraje en el rumbo de la política internacional, el constructivismo posee una serie de pilares, reseñados en la obra de Sanahuja (2015). Uno de ellos es, como descrito anteriormente, la centralidad de las ideas y los valores; estos son considerados elementos esenciales para comprender el comportamiento de los actores políticos. En este aspecto, se separa de las teorías dominantes como el realismo y el liberalismo, ya que estas

los toman como factores explicativos ya dados. Para el constructivismo, las ideas son las razones orientadoras de las acciones, más que una causa para explicar el comportamiento de los actores.

Otro de los pilares que sostienen esta teoría es la influencia que tienen las normas y las instituciones. Los exponentes del constructivismo indican que estas son las que posibilitan la existencia del orden internacional, en tanto que constituyen los intereses y las identidades de sus actores (especialmente, de los Estados). Concretamente, Martha Finnemore explora esta noción en profundidad en su obra *National Interests in International Society* (1996); en este libro, Finnemore explica que los Estados, como los individuos, son “socializados” a través de la interacción en el sistema internacional y, mediante ella, logran construir las normas, roles y reglas “culturalmente” determinadas, que definen las preferencias (acciones que son valiosas, apropiadas y necesarias). Aquí puede observarse el tercer pilar de la teoría.

El escenario preferido para la construcción de valores comunes es la organización internacional (entendida como actor del sistema), las cuales son centrales en la obra de Finnemore porque las identifica como “los agentes de cambio” en el comportamiento. Esta perspectiva del constructivismo será de capital importancia para la robustez de este planteo teórico, ya que una de las críticas fundamentales que se le hace al constructivismo es la imposibilidad de aplicación empírica. Esto deriva de que la sustancia a analizar es abstracta: ¿cómo medir las ideas? ¿cómo cuantificar las reorientaciones coordinadas y sistémicas de los intereses estatales? Esto es salvado por el análisis de Finnemore, quien desbanca totalmente esta argumentación al presentar tres casos empíricos en los que este enfoque teórico es explicativo de los fenómenos estudiados por las Relaciones Internacionales.

Este último aspecto (la posibilidad de comprobar empíricamente los supuestos de la teoría) es el motivo central por el cual este estudio elige basarse en la obra de Finnemore; lo que se busca aquí es argumentar que la teoría constructivista de las Relaciones Internacionales no sólo puede ser comprobada en el campo empírico, sino que además la misma puede aplicarse perfectamente al Derecho Internacional Privado y a su parte Penal.

A partir de lo anterior, pueden desprenderse los otros pilares; en primer lugar, la noción de intersubjetividad es fundamental, ya que “el significado de las cosas se encuentra tanto en el comportamiento (...) como en la interpretación que el observador hace de él” (Sanahuja, 2015 p. 203). Citando a Adler, estos significados no son sólo la suma de creencias de los actores, sino que existen como conocimiento colectivo que trasciende a los actores y que se encuentra imbricado en las rutinas y prácticas reproducidas por intérpretes que

participan en su producción y funcionamiento (Sanahuja, 2015). En segundo lugar, a través de este significado intersubjetivo e intencionalidad colectiva es que se constituyen mutuamente los agentes y las estructuras, aunque sean ontológicamente diferenciadas (Sanahuja, 2015).

Como se mencionó anteriormente, el constructivismo parte de la dimensión ideacional de las relaciones internacionales. En este sentido, lo que argumenta la teoría es que estas influyen la formación normativa que las regula. Por lo tanto, las redefiniciones de los intereses estatales se forman por normas compartidas internacionalmente, así como valores que estructuran y dan sentido a la vida política internacional. Finnemore (1996) indica que

los intereses estatales se definen en el contexto de las normas y entendimientos celebrados a nivel internacional sobre lo que es bueno y apropiado. Ese contexto normativo influye en el comportamiento de los responsables de la toma de decisiones y de las masas que pueden elegir y restringir a esos tomadores de decisiones. El contexto normativo también cambia con el tiempo, y a medida que cambian las normas y valores internacionales, crean cambios coordinados en los intereses y comportamientos estatales en todo el sistema (p. 2).

Gracias a esto, es pertinente indicar que el constructivismo puede ser marco explicativo tanto del surgimiento de los Derechos Humanos, como de la concepción propia de los derechos a la imagen y a la intimidad, así como la vulnerabilidad de los usuarios de redes sociales y del ciberespacio en general, pasibles de ser objeto de violaciones transfronterizas mediante tecnología *deepfake*. Es en este sentido que la teoría constructivista de las Relaciones Internacionales se emplea como apoyo de la hipótesis central de este trabajo: que esta “cuarta Revolución Industrial”, como se le ha llamado en varias oportunidades, puede conllevar a un viraje, además de renovaciones propias al sector productivo, también en lo que respecta a la creación normativa, tendiente a proteger determinados valores que se han construido, por ejemplo, en la formulación de los Objetivos para el Desarrollo Sostenible (ODS) en el marco de la Agenda 2030.

2.4.3 Haciendo justicia en el ciberespacio: Derecho Internacional Privado y Penal en acción

El Derecho Internacional Privado (DIPr) afronta en internet una amenaza a su “estructura profunda” por el desafío que conlleva para todos los países el crecimiento de la red y la falta de regulación de las nuevas situaciones electrónicas. Este escenario sobrepasa las bases tradicionales del Derecho Privado convencional y puede conllevar vacíos legales

(Morales Montilla, 2020). Como se mencionaba anteriormente, las situaciones privadas que ocurren en la esfera digital tienden a ser globales, y como tales, exigen soluciones globales.

En aras de esclarecer las afirmaciones anteriores y darle un soporte teórico y jurídico al presente trabajo, se entenderá por DIPr a la rama del derecho encargada de reglar y dar continuidad a las relaciones privadas internacionales entre las personas físicas o jurídicas, con elementos de extranjería relevantes. El mismo posee tres objetivos: determinar la ley aplicable a esta relación; establecer el juez competente internacionalmente para conocer en dicho caso y, finalmente, determinar las condiciones para que una sentencia dictada en el extranjero pueda ser reconocida y ejecutada (Fresnedo, 2022).

Diversas discusiones doctrinarias han tratado el objeto de esta disciplina. Desde una perspectiva clásica o conflictualista, el objeto del DIPr sería solamente el conflicto de leyes. Como cada Estado posee sus normas (válidas exclusivamente dentro de su territorio), al extenderse fuera de sus fronteras, lo que ocurre es que debe resolverse el conflicto entre leyes nacionales vinculadas mediante la elección de una de ellas. Sin embargo, esto generaría que el DIPr sólo se formaría por normas formales o de conflicto, sin tener en cuenta a las normas materiales; Fresnedo (2022) lo define como exclusivismo metodológico.

La concepción sustancialista (también conocida como privatista) plantea que el objeto del DIPr es la elaboración de un derecho material específico para las relaciones jurídicas internacionales, que se adecúe a estas. La existencia de diferentes y variados órdenes jurídicos estatales que se relacionan entre sí no impediría, de acuerdo con esta concepción, una armonización entre ellos, a través de la creación de una suerte de orden jurídico supranacional. Sin embargo, Fresnedo (2022) advierte que esta concepción también conduciría a un exclusivismo metodológico.

Siguiendo a Talice, el objeto regulado por las normas del DIPr es la relación privada internacional, la cual se caracteriza por la presencia del elemento extranjero, aunque este no siempre aparezca en el mismo momento del transcurso de la relación jurídica. Por lo mismo, Herbert plantea que el objeto de esta disciplina jurídica es la persona y las relaciones que ella entabla, centrándose en los aspectos dinámicos de la relación jurídica que hacen a su continuidad (Fresnedo, 2022).

Finalmente, el pronunciamiento de Opertti indica que el DIPr se ocupa de las relaciones jurídicas privadas, con puntos de localización en distintos Estados y que, por lo tanto, el legislador internacional debe resolver las distintas necesidades de regulación que plantean. De acuerdo con este teórico, los objetivos del DIPr serán alcanzados tanto por las

normas formales como por las normas materiales; a decir de Opertti “coordinación y regulación directa como objetivos normativos pueden llevar al DIPr a alcanzar, respectivamente, la seguridad jurídica y la adopción de las soluciones más adecuadas” (Fresnedo, 2022, p. 84).

Este enfoque es el que parece más adecuado para el presente trabajo. El mismo debe vincularse con la rama Penal de dicha disciplina jurídica. Antes de dar una definición propiamente dicha de lo que se entenderá por Derecho Penal Internacional (DPI), parece oportuno hacer algunas aclaraciones sobre el derecho penal a secas. En primer lugar, se hablará a lo largo del presente trabajo de “delito”; por tal se entenderá toda acción típica (es decir, contenida en una norma escrita, que a su vez prevé una sanción para la misma), antijurídica y culpable. Será de especial consideración la definición dada por el artículo 2 del Código Penal del Uruguay:

Los crímenes son los ilícitos de competencia de la Corte Penal Internacional de acuerdo a lo dispuesto en el artículo 5 del Estatuto de Roma y además todos los que por su extrema gravedad se rijan por leyes especiales, por este Código y las normas de derecho internacional en cuanto le sean aplicables. Los delitos son todos los demás que no revistan la gravedad indicada en el párrafo anterior. Las faltas se rigen por lo dispuesto en el libro III del presente Código.

A partir del Estatuto de Roma citado por el Código Penal uruguayo, se distinguen dos niveles en la misión del DPI: el aspecto individual y el aspecto colectivo. Para el presente análisis, es relevante el nivel individual, ya que es el que destina el fin del DPI a la protección de los Derechos Humanos fundamentales a través de la persecución y castigo de crímenes internacionales que violan esos derechos. Claramente, esto debe ser matizado; no es la intención aquí plasmada la de poner en un mismo nivel las violaciones transfronterizas de los derechos a la imagen y la intimidad, en general, y en particular, de las mujeres, con crímenes internacionales tipificados como el genocidio. Simplemente, esta concepción sirve de fundamento para aplicar al estudio de dichas violaciones transfronterizas el marco del Derecho Penal Internacional dentro del Derecho Internacional Privado, ya que se entiende que el sistema de control indirecto es el ideal para enfrentar las mismas y hacer que los autores respondan por ellas, garantizando no sólo el respeto de los derechos mencionados anteriormente, sino también el de acceso a la justicia, enunciado en el artículo 8 de la Declaración Universal de Derechos Humanos.

Siguiendo con el análisis del Código Penal uruguayo, en él se establecen una serie de principios básicos del derecho penal; en primer lugar, se define en sus artículos 9 y 10 la territorialidad de las leyes penales. Esto quiere decir que los delitos cometidos en el territorio uruguayo (junto con algunas excepciones de delitos cometidos tanto por uruguayos como por extranjeros en el extranjero), serán castigados por la ley uruguaya, con independencia de la nacionalidad del autor y ateniéndose a lo dispuesto por las reglas internacionales. Otro principio enunciado en el Código es el de irretroactividad de la ley penal, establecido en su artículo 15. Esto implica que sólo serán delitos las conductas tipificadas como tales luego de la entrada en vigor de la ley.

Asimismo, otro principio básico del derecho penal uruguayo es la prohibición, a nivel constitucional, de la pena de muerte y el juicio en rebeldía (artículos 21 y 26 de la Constitución de la República). Finalmente, son principios generales del derecho penal los enunciados por los latinazgos *non bis in idem* e *in dubio pro reo*. El primero de ellos indica que no se puede juzgar a un mismo individuo dos veces por el mismo delito. El segundo es más conocido comúnmente como “todos son inocentes hasta que se demuestre lo contrario”, es decir, se debe dilucidar si se ha configurado o no un delito.

Se considerará al Derecho Penal Internacional como aquella rama del sistema jurídico internacional que configurará una de las estrategias empleadas para conseguir, “respecto de ciertos intereses mundiales, el más alto grado de sujeción y conformidad a los objetivos mundiales de prevención del delito, protección de la comunidad y rehabilitación de los delincuentes” (Bassiouni, 1982, p. 6). Esto se vincula perfectamente con la seguridad jurídica y las soluciones más adecuadas planteadas por Opertti respecto del DIPr. Entonces, el objeto del cuerpo normativo del DPI será

delimitar las conductas específicas que se consideran atentatorias de un interés social de trascendencia mundial dado, para cuya protección parece necesaria la aplicación a sus autores de sanciones penales impuestas por los Estados miembros de la comunidad a través de actuaciones nacionales o internacionales, colectivas o de cooperación (Bassiouni, 1982, p. 6).

El DPI es el resultado de la convergencia entre los aspectos internacionales de la legislación penal nacional de los Estados soberanos y de los aspectos penales de la legislación internacional. Las primeras tienen su origen en los sistemas de cooperación interestatal respecto de las personas buscadas por la comisión de delitos contra el orden jurídico estatal interno (extradición), mientras que las segundas comprenden “una serie de disposiciones

internacionales establecidas por vía consuetudinaria o acordada, incriminadora de ciertos tipos de conducta independientemente del hecho de que su aplicación se lleve a cabo interna o externamente” (Bassiouni, 1982, p. 9). El presente análisis se basará, a este respecto, en una definición del DPI centrada en los aspectos penales del Derecho Internacional, entendido como:

Los aspectos del sistema jurídico internacional que regulan a través de obligaciones jurídicas internacionalmente asumidas, las conductas cometidas por individuos, personalmente o en su calidad de representantes o por colectividades, que violan prohibiciones internacionalmente definidas para las que se prevé una sanción penal (Bassiouni, 1982, p. 35).

En cuanto disciplina científica, el DPI surge de la conjugación entre el Derecho Internacional y el Derecho Penal, como se ha dejado entrever en la citada definición. Estas ramas del Derecho conllevan una serie de dicotomías atadas a sus premisas doctrinales de base, las cuales han determinado que el DPI se configure como una “personalidad dividida”, lo cual ha dificultado su desarrollo (Bassiouni, 1982). Ambos sistemas se diferencian en sus fines, enfoques, métodos y resultados, lo que explicaría su falta de cohesión y sentido de dirección en el desarrollo del DPI; por éste motivo, los internacionalistas analizarán el DPI en base a las obligaciones asumidas a través de tratados internacionales, así como prácticas consuetudinarias internacionales de los Estados en orden al cumplimiento de los mandatos del DPI a través de sus sistemas penales internos. Por otro lado, los penalistas buscarán construir un modelo de ejecución internacional paralelo al sistema interno de los Estados y se preocuparán de la codificación de las normas penales internacionales y su aplicación mediante un sistema de justicia penal internacional (Bassiouni, 1982). Ambas perspectivas serán tomadas en cuenta en el desarrollo de este análisis, bajo el paraguas del pensamiento de Goldschmidt (1951) “la concepción normológica del DIPr nació psicológicamente bajo la influencia del modelo del Derecho Penal”.

El desarrollo del DPI ha conllevado, en primer lugar, la tipificación de delitos internacionales mediante convenios multilaterales y, en segundo, la delegación de su aplicación y la imposición de las sanciones previstas en el Derecho penal interno de los Estados signatarios. Esto, de acuerdo con la clasificación de los tipos de crímenes elaborada por Schwarzenberger, podría conocerse en la actualidad como DPI que regula “crímenes ‘internacionales’ o ‘transnacionales basados en tratados’” (Ambos, 2013, p. 7). No se prevén, por tanto, en el sistema jurídico internacional, sanciones para la violación del DPI. A raíz de

esto, puede afirmarse que este sistema de control es “indirecto”, al carecer de una estructura supranacional (se debe tener presente que la Corte Penal Internacional, surgida del Estatuto de Roma en 2003, sólo tiene jurisdicción en los Estados ratificantes el mismo). Citando a Bassiouni (1982), la única *civitas máxima*³ existente en la actualidad en el Derecho Penal Internacional es la que propuso Grocio: *aut dedere, aut iudicare*⁴.

Tomando como base el estudio realizado por Kai Ambos (2013) sobre la cuestión del *ius puniendi*⁵ en el marco del DPI, se enfocará el presente análisis en el apartado que el autor destina respecto de la protección que éste debe hacer de los Derechos Humanos fundamentales. Tras la lectura del primer párrafo, a priori, parecería que la argumentación de Ambos podría articularse con la argumentación anterior realizada respecto de la imagen y la intimidad como Derechos Humanos personalísimos, la cual también se apoya en Kant. Ambos indica que existe un orden normativo internacional basado en valores dignos de ser protegidos, lo que se remonta a la idea de dignidad humana desarrollada por Kant. Para él, la dignidad es lo opuesto del valor, ya que todo lo reemplazable tiene un valor relativo, mientras que la dignidad entraña la imposibilidad de ser reemplazada. Así entendida, la dignidad humana es un concepto que reclama ser reconocido y respetado por las personas en base a su condición de seres humanos. Esta formulación ha quedado plasmada en la Declaración Universal de los Derechos Humanos, entre otros instrumentos de similar carácter, como ya se ha mencionado. Entonces, desde este punto, asegurar la protección de los Derechos Humanos es el deber más importante del DPI.

Al contarse con un marco teórico sólido, es posible progresar en el desarrollo del análisis que es fundamento de esta monografía final de grado: las vulneraciones transfronterizas de los derechos a la imagen y a la intimidad de las mujeres y el marco jurídico internacional en el que se inscribe su tutela. Para lograr este objetivo, se procederá a la construcción de lo que se ha denominado *iter deepfake*, para luego justificar por qué se entiende que son las mujeres y sus derechos los que se ven especialmente interpelados por esta cuarta revolución industrial que está transitando la humanidad. Posteriormente, se analizará el acuerdo del Consejo de Europa sobre ciberdelincuencia (Budapest, 2001), así como la Convención sobre Ciberdelincuencia de Naciones Unidas, aprobada en diciembre de 2024 por la Asamblea General. Finalmente, se concluirá el análisis con una perspectiva constructivista de la influencia que tienen estas normas (y otras) en las prácticas

³ En español, “Estado universal”.

⁴ En español, “o extraditar, o juzgar”. Este es un principio propio del DIPr, por el cual no se deben dejar impunes los delitos cometidos cuando no se extradita al sospechoso ubicado en el Estado requerido.

⁵ En español, “derecho a penar”.

internacionales de los Estados y cómo estos, desempeñando su papel de legisladores en el Sistema Internacional, podrían proteger más eficientemente los Derechos Humanos en el contexto de la IA generativa.

Capítulo III

3. *Iter deepfake*: proceso a través del cual se genera el contenido *deepfake*

Como indica el título del presente apartado, se procederá a la caracterización de lo que se ha elegido denominar *iter deepfake*. Esta designación surge del latinazgo *iter criminis*, que referencia la rama del Derecho Penal para llamar al “camino del delito”, es decir, los pasos que siguió el autor, desde que el mismo surge en su mente (fase interna), hasta que se lleva a cabo, suponiendo que se produzca su materialización (fase externa). Estas dos fases ocurren en un proceso ininterrumpido, y se componen de varias etapas (Cairolí, 2003). A continuación, se profundizará en estas cuestiones, para lograr una elaboración y entendimiento lo más completo posible del *iter deepfake* que aquí se presenta.

A razón de lo anterior, se entenderá que la fase interna del *iter criminis* es aquella desempeñada enteramente en el fuero interno del autor, es decir, en su mente. Debido a esto, durante la misma no operan las sanciones previstas en la ley penal porque no se configuran materializaciones del delito; sancionar los procesos que ocurren en el imaginario de los individuos constituiría una violación del principio *cogitationis poena noemo patitur*⁶, por no hablar del derecho de la libertad de expresión, tutelado por el orden jurídico uruguayo. De acuerdo al mismo, el derecho penal está destinado a castigar exclusivamente los hechos externos (Cairolí, 2003).

De acuerdo con Cairolí (2003), las etapas de la fase interna son la ideación, la deliberación y la resolución. En la primera de ellas se concibe la idea delictiva en la mente del sujeto; en la segunda, el mismo realiza una ponderación de los aspectos negativos y positivos del propósito de llevar a cabo dicha acción ideada. Finalmente, la tercera etapa marca el fin de la fase interna, pero aún no configura su comienzo externo: simplemente, se tomó la decisión de materializar la idea.

En la fase externa se dan las manifestaciones propias del pensamiento delictivo desarrollado previamente. En esta sí se configuran las acciones que derivarían en un castigo penal (Cairolí, 2003). Las etapas propias de esta fase son la resolución manifestada, los actos preparatorios, la tentativa, la consumación y el agotamiento. Se desarrollarán algunas particularidades de las mismas a continuación.

⁶ En español, “nadie puede ser penado por sus pensamientos”.

En primer lugar, la resolución manifestada es toda confesión, anuncio o jactancia que implique una manifestación firme de voluntad por parte del individuo de la realización de un delito. Ella puede subdividirse en proposición y conspiración: la primera no suele castigarse, exceptuando delitos contra la soberanía o el Orden Público Interno del Estado, mientras que la segunda constituye un estado más avanzado de un concierto o acuerdo entre dos o más personas (Cairolí, 2003).

Seguidamente, los actos preparatorios existen cuando el designio criminal se concreta por acciones externas, pero igualmente anteriores a la ejecución. En esta parte del *iter criminis*, el delito sólo será punible en los casos en que la ley lo tipifique específicamente. Siguiendo a Cairolí (2003), respecto de esta etapa y la siguiente (tentativa), la dogmática experimenta una dificultad interpretativa, ya que el ejercicio llevado a cabo implica estimar el grado de objetividad al que ha llegado la resolución criminal al mundo exterior, para dar lugar a la sanción. A ese respecto, la ley penal uruguaya designa como criterio interpretativo el del comienzo de ejecución.

En tercer lugar, la tentativa implica el esfuerzo por parte del autor por lograr la consumación del delito, ejecutando todos los actos externos planificados, pero donde la existencia de obstáculos (ajenos a su voluntad, de orden físico, material o psíquico) le impiden lograr tal fin. Esta etapa, configura una “infracción perfecta” porque se confirma el daño de un bien jurídico tutelado, aunque la pena prevista sea menor. Usualmente, es equiparada con la frustración (Cairolí, 2003).

La cuarta etapa es la consumación, cuando se cumple la adecuación al tipo penal. Esto quiere decir que la conducta del autor del delito se adecúa en forma directa y plena con la descripción del tipo hecha por el legislador en la norma penal. La última etapa de la fase externa es el agotamiento, momento en el que el delito produjo todos los efectos dañosos que son consecuencia de la violación y a los que tendía la conducta del agente, quien no puede impedir sus efectos.

Antes de poder continuar con la elaboración del *iter deepfake*, sería prudente realizar algunas aclaraciones fundamentales. En primer lugar, los delitos aquí estudiados suceden en el ciberespacio, como lo denomina Gaimari (2021), el “no lugar”, una esfera en la que las fronteras territoriales pierden significado y donde la atribución de jurisdicción penal se vuelve compleja. Asimismo, el producto final (contenido *deepfake*) es generado por algoritmos, dos hechos que configuran un desafío para el derecho

en el análisis de la conducta, entendida en la teoría del delito, como aquella realizada por el hombre, habiendo analizado (...) que las respuestas que un sistema de inteligencia artificial, como su nombre lo dice es artificial, es decir premeditada por intervención de la mano del hombre, cuando crea el algoritmo “madre” (Gaimari, 2021, p. 42)

En este contexto, la teoría de la ubicuidad (Moscoso Restovic, 2010), aplicada en algunos ordenamientos jurídicos, permite considerar que la comisión del delito ocurre tanto en el lugar desde donde se realiza la acción (*lex loci delicti commissi*) como en aquel donde se producen sus efectos (*lex loci damni*), otorgando mayor flexibilidad a las víctimas para acceder a la justicia en lo referente a la identificación de la ley aplicable (Fresnedo, 2022). Esto es porque se logra evitar que los responsables se beneficien de vacíos legales en una u otra legislación.

Por otro lado, desde la perspectiva de la determinación del juez competente, existirían tres foros competentes: el del juez en cuyo país se creó el *deepfake* (es decir, donde se configuró el acto ilícito); el del juez donde se difundió el *deepfake*; y, finalmente, el juez del país donde la víctima sufrió los daños (el cual puede ser tanto su lugar de residencia, como donde se produjeron los efectos perjudiciales de la difusión) (Fresnedo, 2022). Sin embargo, teniendo en cuenta lo analizado hasta el momento, el segundo criterio para determinar el juez competente, en estos casos, pierde validez. Esto es porque no hay un lugar que pueda ser determinado como “origen” de la difusión del *deepfake*, pues el mismo se difunde desde un servidor web o una red social, que existen sólo en el ciberespacio, en el “o lugar”.

Adicionalmente, ambas instancias (definir ley aplicable y juez competente) enfrentan el desafío significativo de verse a la merced de la voluntad de los Estados soberanos. Esto es así porque, por un lado, el sistema internacional aún no ha alcanzado la armonización normativa necesaria como para garantizar la aplicación homogénea de estos criterios; mientras que, por el otro, está la posibilidad de que se genere un conflicto de jurisdicción o de *forum shopping*. Para evitar estos problemas es que es fundamental que se fortalezcan los mecanismos de cooperación judicial, así como acuerdos de extradición y reconocimiento de sentencias, garantizando que la multiplicidad de jurisdicciones no conduzcan a la impunidad.

En definitiva, lo que existe aquí es una conducta humana (fase interna) que utiliza como medio la tecnología para realizar la fase externa del camino del delito. Se entenderá por tal, en el presente desarrollo, el de violación de imagen de manera directa, y a la intimidad de

manera indirecta (Trujillo Cabrera, 2024). Dejado esto aclarado, se procederá a realizar el *iter deepfake*.

Sin perjuicio de que todo el análisis de la fase interna se realiza a partir de supuestos, se entiende que la etapa de ideación se lleva a cabo cuando al individuo autor del delito le surge la idea de satisfacer su objetivo de obtener contenido *deepfake* retratando a una persona en una situación determinada, al tener ante sí la posibilidad de acceder fácilmente a IA generativa o, de lo contrario, de programar un software en tal sentido. La deliberación se desarrollará en su fuero interno, donde ponderará tanto la factibilidad de acceder o programar dicho software, la creación de contenido *deepfake* y que el mismo sea creíble (lo cual media la obtención de una serie de videos, imágenes y, potencialmente, audios de las víctimas) y, finalmente, la eventualidad o no de ser rastreado e identificado como autor y difusor del mismo. Aquí se da la posibilidad de que el autor entienda que consumir el delito no valga la pena y se produzca un desistimiento (Cairolí, 2003). Si el individuo opta por confiar tanto en el acceso a los medios para la creación del contenido *deepfake*, como la escasa o nula posibilidad de ser rastreado e identificado como su creador y difusor, puede decirse que transitó a la etapa de resolución.

Teniendo noción de que han ocurrido casos de *deepfakes* en la vida real, al describir la fase externa, ya puede sostenerse que el camino detallado a seguir por el autor del delito es más previsible y, por lo tanto, las afirmaciones que se realizarán serán más fidedignas.

En la etapa de resolución manifestada, el autor podría concretarla mediante amenazas a la víctima, una publicación en redes sociales o comentarlo a través de mensajes en su grupo de pares. Se recuerda que si en este último medio el autor se expresa mediante una proposición, no será pasible de recibir sanciones. En cambio, si se concreta una conspiración, la ley penal ya tiene razones para penar al individuo.

Los actos preparatorios consistirán, primeramente, en la búsqueda o programación de un sistema de software que permita la creación de contenido *deepfake*. Asimismo, se deberá contar con la suficiente cantidad de datos de la víctima en formato audiovisual (videos con sus expresiones faciales y gestos, audios con cadencias de voz y tonos específicos, así como fotos de múltiples ángulos); esto es facilitado enormemente hoy en día, no sólo por la existencia de personalidades públicas, como pueden ser las celebridades o los políticos, sino porque muchas personas cuentan, actualmente, con perfiles en diferentes redes sociales que son de carácter público.

Para comprender un poco mejor esta etapa de la fase externa, se seguirá los planteos de Trujillo Cabrera (2024), quien explica de forma muy clara de qué forma operan los sistemas de IA generativa empleados en este proceso. El autor indica que este contenido se genera a partir de un análisis de los datos, en este caso, en formato audiovisual, que son ingresados en un algoritmo *deep learning*⁷. En él, las redes neuronales (GAN)⁸ buscan “aprender a imitar las expresiones faciales, los gestos, la voz y las inflexiones de una persona” (Trujillo Cabrera, 2024, p. 82).

Si este delito se pretendiera cometer contra los derechos de imagen e intimidad de una persona que no siendo famosa, tampoco tiene un perfil público en redes sociales, ni se tiene conocimiento a título personal de la misma, entonces la ejecución de los actos externos para consumar el delito podría verse truncado en la etapa de tentativa; esto porque toda la “operación” dependería de que la víctima aceptara, de una u otra forma, o una solicitud de “seguir” su perfil en redes sociales (y por ende, acceso a una parte de su intimidad), o compartir mediante un chat su imagen, audios o videos. Son también hechos que pueden llevar a que el autor quedara en la etapa de tentativa la imposibilidad de acceder al software, ya sea porque éste es pago o porque no se tiene los conocimientos para programar uno. Como ya se ha mencionado, esta posibilidad es de difícil concreción, ya que una de las características centrales de la alerta que entraña el advenimiento de la IA generativa es su fácil acceso. Asimismo, fallas en la creación del contenido audiovisual *deepfake*, como la falta de autenticidad derivada de la propia recopilación de insumos podría favorecer el estancamiento en la etapa tentativa. Finalmente, de ser publicado el contenido, podría ocurrir que el mismo fuera dado de baja por incumplir los reglamentos de uso de la plataforma antes de lograr una difusión masiva del mismo.

La consumación, por su parte, se completaría cuando el *deepfake*, una vez creado y publicado, traspasara las fronteras virtuales sin ningún impedimento sancionatorio por parte de las plataformas digitales por no considerarse dañino o violatorio de sus políticas, siendo difundido por todas ellas. Si llegara a difundirse en medios de prensa, además de en redes sociales, esto sin dudas configuraría la lesión efectiva del derecho a la imagen y a la intimidad de la víctima. En este sentido, coincide con la etapa de agotamiento, pues una vez que el autor

⁷ Consiste en una forma más especializada de aprendizaje automático que funciona a través de arquitecturas de procesamiento inspiradas en las neuronas biológicas. Los datos que se ingresan en estos algoritmos pasan por diferentes capas “ocultas” de funciones de procesador discretas e interconectadas, donde cada una sintetiza y procesa la información de la capa anterior antes de transmitirla a la siguiente (Trujillo Cabrera, 2024).

⁸ En inglés, *generative adversarial networks*, las cuales funcionan por el enfrentamiento de dos redes neuronales: una que discrimina el contenido (en este caso, qué es realista y qué no lo es) y otra que genera los datos para vencer al discriminador (Trujillo Cabrera, 2024).

publica el contenido *deepfake*, ya no puede impedir que otros usuarios o plataformas lo sigan difundiendo por otros canales.

Partiendo de la base de este “camino del *deepfake*” que se ha explicado en el presente apartado, a continuación se buscará fundamentar por qué motivo se seleccionó a la mujer como principal sujeto afectado en la creación de contenido *deepfake*, aportando una visión propia del constructivismo y del Derecho Internacional Privado.

4. ¿Por qué las mujeres?

Esta sección se centrará, primeramente, en una contextualización de la situación de la mujer y la percepción de la misma a nivel de la sociedad internacional. Para esto, el relato se basará en el libro *La mujer invisible: descubre cómo los datos configuran un mundo hecho por y para las mujeres*, de Caroline Criado Pérez, así como en una reseña de diversos artículos y del Objetivo para el Desarrollo Sostenible número 5. En segundo lugar, se pasará a reportar una serie de casos ocurridos en el pasado reciente, así como una recopilación de datos estadísticos referentes a la presencia de contenido *deepfake* doloso para la imagen y la intimidad de las mujeres.

4.1 La brecha de datos de género y la Agenda 2030

Gran parte de la historia documentada sufre de un importante vacío de datos. La elección de la obra *La mujer invisible*, no es casual; a este propósito, se entiende que dicho libro es una investigación dedicada a evidenciar cómo las brechas de datos de género y los sesgos en el diseño de sistemas tecnológicos perpetúan desigualdades estructurales, lo que resulta especialmente pertinente en el análisis de los *deepfakes*. El enfoque constructivista adoptado, permite interpretar cómo las normas y valores sociales se reflejan en los sistemas tecnológicos, convirtiéndolos en herramientas que amplifican formas contemporáneas de violencia de género. Estas brechas afectan la elaboración de los marcos jurídicos internacionales, generando dificultades para abordar estos fenómenos contemporáneos garantizando el respeto a los derechos humanos y garantizando seguridad jurídica.

Siguiendo a Criado Pérez (2019), los seres humanos estamos inmersos en un mundo construido sobre la base de una brecha de datos de género. Es importante establecer la premisa de que, desde el inicio de su ensayo, la escritora aclara que esta brecha no es maliciosa ni deliberada; se podría afirmar que no es más que una construcción social, una forma de pensar, generalizada por milenios: a los hombres se los da por supuestos y a las

mujeres no se las menciona. A razón de esto, Criado Pérez cita a Simone de Beauvoir (1949): “La humanidad es macho, y el hombre define a la mujer no en sí, sino respecto de él; no la considera como un ser autónomo (...). Él es el Sujeto, él es lo Absoluto; ella es el Otro” (2019, p. 14). Complementariamente, Méndez Hernández (2021) cita a varios autores que definen esta brecha de datos como “una estratificación social basada en la dominación masculina cuyo paradigma es el varón frente a la subyugación de las mujeres”. No incluir la perspectiva de la mujer, por lo tanto, perpetra este sesgo masculino no intencionado que suele pasar como “neutro”. La brecha de datos de género es a la vez causa y consecuencia del no pensar que concibe a la humanidad como casi exclusivamente masculina (Criado Pérez, 2019, pp. 17, 18).

A razón de lo anterior, se tomará como definición de la brecha de datos de género aquél vacío sistémico y persistente en la recolección y el análisis de datos específicos sobre mujeres, perpetuando desigualdades y reforzando un sesgo androcéntrico en la toma de decisiones y el desarrollo de políticas.

Debido a este fenómeno estructural, se ha asistido a la exclusión de las mujeres de la historia cultural, provocando opiniones sesgadas en contra de ellas. El derecho no escapó de este mal; de acuerdo con Méndez Hernández (2021), en sus orígenes este establecía un tratamiento discriminatorio o denigrante de las mujeres, ya fueran tratadas como víctimas o como criminales. Esto deriva del sesgo androcéntrico perpetrado por la brecha de datos de género, causando que el empleo de la ciencia jurídica se hiciera con fines opresivos y de subordinación de la mujer. La raíz de todo se encuentra localizada en el *Malleus Maleficarum*⁹, considerado por algunos autores como el “tratado fundacional de las ciencias penales modernas” (Méndez Hernández, 2021, p. 234); la citada autora refiere que su contribución ha sido “imprescindible en la construcción del discurso de desprecio e inferioridad hacia las mujeres en el poder punitivo al considerar que por naturaleza tienen mayor carnalidad, debilidad y mayor tendencia al mal” (Méndez Hernández, 2021, p. 234), y que esta se vincula con la trasgresión de los roles impuestos a la feminidad. Posterior a la reforma ilustrada, se incorpora a esta noción la idea de que la función de la pena impuesta a las mujeres delincuentes era reeducarlas en los roles mencionados. Finalmente, la llegada del positivismo supuso el nacimiento de la criminología, la cual se ha nutrido de premisas sesgadas por la brecha de datos de género. En este contexto, las mujeres son excluidas,

⁹ También conocido como “El martillo de las brujas”, escrito por frailes dominicos y publicado en 1487.

situadas en la alteridad o anormalidad, o tratadas peyorativamente (Méndez Hernández, 2021, p. 236).

El capítulo catorce de la obra de Criado Pérez tiene un título instrumental para los objetivos de este trabajo: “Los Derechos Humanos son derechos de las mujeres”. En él se describe cómo la presencia de las mujeres en la gobernanza es esencial para la promoción de leyes e iniciativas tendientes a proteger los Derechos Humanos; indica Cárdenas Aravena (2021) que incrementar la participación femenina en la primera línea de los tribunales penales internacionales ha sido fundamental en la incorporación de consideraciones de género en sus sentencias. Dice Criado Pérez: “(...) cuando se trata de gobernar, lo mejor (...) significa un grupo de trabajo concebido como un todo. Y en este contexto lo mejor significa diversidad” (p. 384). Con los datos recopilados hasta el año 2019, hay suficiente claridad para afirmar que las políticas no funcionan en igualdad de condiciones porque “el sistema está sesgado en favor de la perpetuación de la brecha de datos de género en el liderazgo mundial” (Criado Pérez, 2019, p. 384). En 2024, sólo el 26,8% de todos los parlamentarios nacionales eran mujeres, representando un ligero aumento frente al 11,3% del año 1995 (ONU, s.f.). Está claro que “los datos acumulados a lo largo de toda una vida siendo mujer son importantes” (Criado Pérez, 2019, p. 384), y que, por lo tanto, legislar (no teniendo en cuenta la brecha de datos de género, sino incluyendo la participación activa de las mujeres) el uso de IA generativa, es de capital importancia.

Esto último es especialmente relevante para la Agenda 2030 para el Desarrollo Sostenible, adoptada por las Naciones Unidas en el año 2015. Ésta establece un marco global compuesto por diecisiete Objetivos de Desarrollo Sostenible (ODS), diseñados para abordar desafíos urgentes como la pobreza, la desigualdad y el cambio climático. Su enfoque es integral, interrelacionando dimensiones sociales, económicas y ambientales para la promoción del bienestar humano y la sostenibilidad planetaria, con el año 2030 como meta. El compromiso global de los Estados miembros implica la implementación de políticas públicas que faciliten el cumplimiento de estas metas en todos los niveles de gobernanza (ONU, 2015).

Entre los objetivos adoptados, el ODS 5: Igualdad de género, destaca por su enfoque en la eliminación de todas las formas de discriminación y violencia contra las mujeres y niñas, tanto en ámbitos públicos como privados. Este objetivo es especialmente relevante en contextos donde nuevas tecnologías, sobre todo la IA, son empleados para vulnerar los derechos de las mujeres, exacerbando la violencia de género en entornos digitales, por ejemplo, a través de los *deepfakes*. Además, el ODS 5 promueve la participación plena de las

mujeres en todos los niveles de toma de decisiones y busca asegurar la igualdad de oportunidades económicas y políticas, abordando las desigualdades estructurales que perpetúan la subordinación femenina (ONU Mujeres, 2020).

La meta 5.2 del ODS 5 se focaliza en eliminar todas las formas de violencia contra las mujeres, incluidas las digitales. Asimismo, la meta 5.b promueve el uso de tecnologías que empoderen a las mujeres, garantizando su acceso a herramientas digitales de forma segura y equitativa; esto permitirá no sólo proteger los derechos de imagen y a la intimidad de las mujeres, sino que fomentará su participación activa en el desarrollo y gobernanza de las nuevas tecnologías, promoviendo un entorno tecnológico más justo. Finalmente, la meta 5.c insta a la adopción de marcos normativos sólidos que tengan en cuenta la brecha de datos de género en la legislación, un elemento fundamental para cualquier acuerdo internacional sobre ciberdelincuencia.

De igual manera, encuentra respaldo en el Pacto para el Futuro aprobado en 2024. El mismo refuerza el sistema multilateral al reconocer que el desarrollo sostenible, la paz y los Derechos Humanos están interconectados. Su énfasis en la cooperación internacional y la protección de las víctimas de violencia digital complementa la propuesta de regular de manera explícita los delitos relacionados con los *deepfakes*, como lo sugiere el trabajo. Además, el Pacto promueve la creación de mecanismos internacionales efectivos para identificar, retirar y sancionar la difusión no consentida de contenido íntimo, reflejando la importancia de una respuesta global a delitos que trascienden fronteras (Pacto para el Futuro, ONU, 2024).

Tanto el Pacto como las metas del ODS 5 refuerzan la idea de que las vulneraciones a los derechos de imagen e intimidad de las mujeres en el ciberespacio pueden constituir formas de violencia estructural. En este marco, el Pacto para el futuro hace un llamado a los Estados para que “adopten medidas legislativas que protejan a las víctimas, asegure la eliminación inmediata del contenido dañino y sancionen de manera efectiva a los responsables” (Asamblea General de la ONU, 2024, p. 11). La naturaleza global de los ciberdelitos dificulta su persecución, especialmente cuando las jurisdicciones implicadas carecen de marcos de cooperación claros. En este sentido, el Pacto para el Futuro resalta la importancia de “fortalecer los sistemas de intercambio de información y asistencia judicial mutua” (p. 12). Estas disposiciones complementan las propuestas de este trabajo, que abogan por un marco que facilite la remoción de contenido perjudicial y garantice la reparación integral de las víctimas. Como indica Naciones Unidas (2024), “las leyes deben reflejar no solo las

necesidades actuales, sino también los valores de inclusión, equidad y justicia que aspiramos construir” (p. 16).

Adicionalmente, es pertinente analizar el rol que juega la pornografía en la construcción de imaginarios sexuales. Su influencia se extiende más allá del ámbito privado, moldeando actitudes, expectativas y comportamientos. La consolidación de la pornografía digital ha amplificado este fenómeno, facilitando la accesibilidad del contenido (Zillmann y Bryant, 1988). Siguiendo a Fagan (2009), el consumo prolongado de pornografía genera un proceso de desensibilización y cosificación, lo que refuerza la objetivación de las mujeres y la aceptación de narrativas de violencia de género.

En este contexto, los *deepfakes* pornográficos representan una amenaza adicional, ya que no sólo perpetúan la explotación visual de las mujeres, eliminando cualquier posibilidad de consentimiento y convirtiéndolas en víctimas de una forma de violencia digital, sino que además, se ha identificado que la exposición repetida a este contenido genera modificaciones en el sistema de recompensa del cerebro¹⁰. Uno de los efectos más estudiados en este contexto es el efecto Coolidge, un fenómeno presente en los mamíferos machos, que se traduce en una predisposición biológica a mantener un estado de excitación permanente cuando se les expone a estímulos sexuales novedosos. Este mecanismo explica por qué la pornografía digital genera patrones de consumo compulsivo, ya que proporciona un flujo inagotable de contenido nuevo, favoreciendo la escalada del consumo hacia material cada vez más extremo (Pitchers et al., 2013). En el caso de los *deepfakes* pornográficos, esta tecnología permite la creación de contenido "a medida", lo que refuerza la personalización de la experiencia y fortalece los patrones adictivos.

Dada la intersección entre la adicción a la pornografía, la violencia de género y la falta de regulación de los *deepfakes*, es posible vincular esta problemática con los Objetivos de Desarrollo Sostenible (ODS) de la Agenda 2030. El ODS 3 (Salud y Bienestar) enfatiza la necesidad de abordar los problemas de salud mental derivados de adicciones conductuales, incluyendo aquellas relacionadas con el consumo compulsivo de pornografía y su impacto en las relaciones interpersonales. Asimismo, el ODS 5 (Igualdad de Género) busca eliminar todas las formas de violencia contra las mujeres y las niñas, lo que implica enfrentar la proliferación de contenido pornográfico no consentido que vulnera su derecho a la imagen y

¹⁰ La pornografía actúa como un estímulo supernormal, es decir, un estímulo artificialmente exagerado que genera una respuesta más intensa en el organismo que los estímulos naturales (Tinbergen, 1973). Esta hiperestimulación es posible debido al acceso ilimitado a contenido novedoso y a la exposición constante a imágenes sexualmente explícitas, lo que genera una liberación masiva de dopamina en el cerebro (Kühn y Gallinat, 2014).

la intimidad. En este sentido, la regulación efectiva de los *deepfakes* pornográficos no solo contribuiría a la protección de las víctimas, sino que también podría incidir en una reducción del consumo problemático de pornografía, mitigando los efectos negativos que este tiene en la percepción de las relaciones sexuales y en la estructura social en general. Además, el ODS 4 (Educación de Calidad) resalta la importancia de integrar la alfabetización digital y la educación sexual integral en las estrategias de prevención, permitiendo que las nuevas generaciones comprendan los riesgos asociados a la exposición temprana a la pornografía digital y desarrollen herramientas para un consumo más informado y crítico.

Es en este marco que se inserta el binomio *deepfake*-violencia de género (Simó Soler, 2023, p. 500), donde pueden incluirse fenómenos como la violación transfronteriza de los derechos de la mujer a la imagen y a la intimidad. Antes de pasar a la reseña de los casos, parece oportuno seguir a la citada autora en las categorías problemáticas identificadas por ella: el desprestigio, la suplantación de identidad y la simulación de situaciones ficticias constitutivas de delito, con especial énfasis en las dos primeras.

El desprestigio se configura atendiendo a un componente de género y a un elemento subsumido en una cuestión de clase (Simó Soler, 2023). Citando a Cerdán Martínez y Padilla Castillo (2019):

mientras ellas protagonizan falsas escenas eróticas y pornográficas; ellos, discursos y circunstancias relacionados con el humor o con la política, apareciendo normalmente vestidos. Ellas asoman en espacios privados e íntimos; ellos, en espacios públicos, ostentando el poder o un protagonismo sano. Ellas son cosificadas y sus rostros se pegan al cuerpo de una actriz despersonificada. Ellos tienen otro cuerpo, u otra voz, pero no pierden su esencia personal ni son tratados como objetos porque lo llamativo es lo que dicen o hacen. Ellas son sujetos pasivos; ellos son protagonistas activos y mueven la acción (pp. 516-517).

Simó Soler (2023) indica que esto perpetra un descrédito que se vincula con “la sexualidad por la incapacidad cosustancial de la naturaleza femenina de alcanzar esferas públicas más elevadas como la comedia o la política y el retorno al enclaustramiento privado de cuatro paredes” (pp. 501-502). Por su parte, el factor de clase se vincula con la posición de las mujeres en la sociedad: no existe un principio de *in dubio pro mulier*¹¹ que pueda ofrecer margen para modificar el mensaje o defenderse en el espacio público (Simó Soler, 2023, p. 502).

¹¹ En español, “en caso de duda, a favor de la mujer”.

La suplantación de identidad, por su parte, se categoriza bajo la creación de perfiles o espacios falsos en los que la víctima comparte vídeos íntimos y realiza demandas y ofertas sexuales explícitas (Simó Soler, 2023, pp. 502-503). Con los nuevos desarrollos de las GAN, hay aplicaciones que desnudan a las mujeres, como *DeepNude*, que a partir de una base de datos de 10.000 fotos de mujeres desnudas tomadas en internet, añade un cuerpo desnudo a un rostro retratado (Simó Soler, 2023, p. 503).

Finalmente, la simulación de situaciones ficticias son reseñadas por la autora como la posibilidad por parte de un individuo que, al conocer que una mujer le ha interpuesto una denuncia, como represalia utilizaría en la contradenuncia un vídeo de dicha mujer cometiendo un delito contra su persona. Esto no sólo despertaría represalias jurídicas contra ella, sino también sociales (aislamiento de su círculo cercano, amistades, familiares, laborales, etc.).

4.2 Reseña de casos: la mujer en un imaginario falsificado y perverso

Como se ha construido a lo largo de este documento, la posibilidad de crear contenido *deepfake* está a la mano de cualquier persona con una computadora. El primero en realizarlo, en el año 2017, fue un usuario de la plataforma Reddit¹² que se hacía conocer como *Deepfakes* (Cerdán Martínez y Padilla Castillo, 2019). El algoritmo de *machine learning* creado por este individuo puede ser descargado por cualquiera en internet; al mismo se cargaron los rostros de diversas celebridades que fueron incorporados a los cuerpos de varias actrices del cine pornográfico. Los videos resultantes fueron compartidos en la plataforma ya mencionada.

Es en esta web que los primeros videos *deepfake* se hacen virales. Cerdán Martínez y Padilla Castillo (2019), citando a Beamonte (2018), indican que la nueva moda ganó tantos seguidores que *Deepfakes* creó un subreddit¹³ con su nombre de usuario para la puesta en común de dichos videos: en sólo dos meses tenía 15.000 suscriptores. Por si esto fuera poco, en aras de simplificar aún más la creación de estos videos, otro usuario llamado *Deepfakeapp* se encargó de crear una aplicación conocida como *FakeApp*. La misma funciona en base a los algoritmos originales creados por *Deepfakes* y, si bien se puede crear cualquier tipo de video a partir de ella, “la gente parece más interesada en seguir creando pornografía falsa” (Cerdán Martínez y Padilla Castillo, 2019, p. 506). Simó Soler (2023) indica que otros modelos generativos que ofrecen al usuario “una experiencia sencilla y directa” son Dall-E, Midjourney, Stable Diffusion y aplicaciones como *FaceSwap* y *DeepFaceLab*. La misma

¹² Sitio de noticias sociales donde los usuarios crean y comparten contenido, muchas veces adecuado sólo para mayores de 18 años y marcado como NSFW (no seguro para el trabajo, en español).

¹³ Son categorías dentro de Reddit; constituyen comunidades donde se habla de un tema específico.

autora indica que el primer sitio web de pornografía *deepfake* es registrado en febrero de 2018, y que contaba con más de 134 millones de visualizaciones (p. 498).

A continuación del surgimiento de este fenómeno, este se popularizó en los principales portales de contenido pornográfico. Es imprescindible para el argumento aquí presentado la noción de que los mismos no sólo afectan a celebridades, sino que también hay constancia de denuncias realizadas por mujeres anónimas. Si bien estas no son imágenes o audiovisuales íntimos reales, su creación perjudica a la mujer en su vida privada, lesionando su imagen e intimidad con fines de descrédito, manipulación, burla y/o lucro (Cerdán Martínez y Padilla Castillo, 2019). Esto marca una tendencia hacia la manipulación de la imagen de las mujeres, sin su consentimiento, lo que deriva en la lesión de la misma y a su intimidad.

Simó Soler (2023) confirma que el 98% de las *deepfakes* publicadas, de contenido sexual, son protagonizados por mujeres. Siguiendo con su fundamentación, la empresa holandesa Deeptrace¹⁴ ha alertado sobre la proliferación de *deepfakes*, así como el incremento de su sofisticación y del impacto que tienen en la sociedad. Los datos presentados por esta compañía indican que el número total de videos *deepfake* ha aumentado casi en un 100% desde diciembre de 2017 a diciembre de 2018, con una cifra de 14.678. De acuerdo con un reporte publicado por Security Hero (febrero de 2024) titulado *2023: state of deepfakes*, los videos contabilizados en línea para el año estudiado era de 95,820; 98% de ese contenido es pornográfico, y 99% de sus protagonistas son mujeres.

Como ya se ha mencionado, las mujeres mayormente afectadas son aquellas que se encuentran sujetas a exposición pública, siendo en 2023 el 94% de los casos (Security Hero, 2024). Sin embargo, debe reiterarse nuevamente que ellas no son las únicas expuestas; el Wall Street Journal publicó en agosto de 2024 una nota titulada “*Anyone can be a victim: sprawling AI fake nudes crisis hits South Korea*” donde se reporta el descubrimiento de una red de Telegram donde varios usuarios anónimos compartían fotos de mujeres y niñas (profesoras, oficiales del ejército, universitarias y escolares) de Corea del Sur con el fin de crear imágenes y videos explícitos, los cuales eran luego visualizados por miles de personas. Esto también es coherente con el reporte que ya se ha mencionado, pues el mismo indica que 53% de las mujeres que ven su imagen manipulada por esta tecnología son de nacionalidad surcoreana.

De la misma manera, en octubre de 2024, en Reino Unido un hombre fue condenado a 18 años de prisión por utilizar inteligencia artificial para crear (y luego vender) imágenes de

¹⁴ Empresa holandesa, dedicada a la detección y supervisión de materiales creados artificialmente.

abuso sexual infantil a partir de fotografías de menores de edad reales; las mismas le eran proporcionadas directamente por los interesados. Durante las investigaciones, se identificaron sospechosos y víctimas en países como Francia, Estados Unidos e Italia (RaiNews, 2024). Por otro lado, durante el mismo mes, en Turquía, una árbitro fue suspendida de por vida por la Federación Turca de Fútbol (TFF), debido a la liberación de un video sexual que presuntamente la incluía a ella y al inspector de árbitros de la Superliga. La joven negó desde el principio que la mujer que aparecía en dicho video fuera ella, alegando que el mismo fue creado enteramente con IA (El Mundo, AS, 2024).

Por otro lado, es relevante una noticia publicada en febrero de 2025 por la BBC, la cual relata cómo una profesora australiana fue víctima de *deepfakes* pornográficos creados y difundidos sin su consentimiento por un amigo cercano, Andrew Hayler. Dicha profesora recibió un correo electrónico anónimo con un enlace a una página web titulada “La destrucción de Hannah”, donde aparecían imágenes manipuladas en las que su rostro había sido insertado en contenido sexual explícito. Además de las imágenes, dicho sitio web incluía amenazas de violencia sexual, así como información personal de la víctima (su número de teléfono y su cuenta de Instagram). En este caso, la víctima realizó indagaciones por su cuenta, y fue ella quien descubrió que el responsable era uno de sus amigos más cercanos. Sin embargo, cuando acudió a la policía, su denuncia fue inicialmente desestimada, conduciendo a que ella tuviera que contratar expertos forenses (lo que le insumió un gasto de más de 20.000 dólares australianos¹⁵) para recopilar pruebas. Finalmente, frente al expediente ya armado por la víctima, la policía llevó a cabo una redada en la casa del autor de los *deepfakes*, quien confesó el delito. En un juicio calificado como histórico, Hayler fue condenado a nueve años de prisión, marcando un precedente en la legislación australiana sobre *deepfakes* pornográficos (BBC, 2025).

A raíz de este caso, queda en evidencia la falta de regulación específica sobre *deepfakes* en muchos países, la ineficacia de las autoridades para abordar este tipo de delitos y el impacto devastador de la violencia digital en la vida de las víctimas, no sólo a nivel social, sino también económico. Debido a esto, la legislación australiana ha comenzado a endurecerse en torno al uso de la IA en la creación y distribución de contenido sexual explícito (BBC, 2025).

Pero esto no es todo. La imagen de las mujeres también puede estar sujeta a manipulaciones con fines políticos. Así lo reporta la cadena de noticias CNN en su

¹⁵ Lo cual equivale a aproximadamente 12.500 dólares estadounidenses.

publicación “*My identity is stolen: photos of european influencers used to push pro-Trump propaganda on fake X accounts*”. Un caso de manipulación de imagen y suplantación de identidad de varias influencers y modelos europeas que se enteran de esta situación debido a que la cadena de reportaje se pone en contacto con una de ellas. En el escenario presentado, los cuerpos e identidades de casi 60 mujeres son empleados para realizar una campaña favorable al entonces candidato republicano Donald Trump, a la vez que se difama a Kamala Harris, quien se presentara como candidata por el Partido Demócrata. Si bien la mayor parte de estas cuentas se constituyen de imágenes robadas, CNN describe qué parte de las mismas parecen generadas por IA. Esto configura, sin lugar a dudas, una violación a los derechos de imagen e intimidad de estas mujeres, que nada tienen que ver con la reelección de Donald Trump en noviembre de 2024.

Respecto de esto último, parece relevante, sin embargo, atreverse a un análisis prospectivo. Y es que no puede ignorarse que el triunfo de Trump podría generar cambios significativos en el panorama internacional en relación con los ciberdelitos y los derechos de las mujeres, especialmente considerando las políticas adoptadas durante su primer mandato (2016-2020). En este período, Trump mostró escepticismo hacia acuerdos multilaterales, como el Acuerdo de París y diversas iniciativas de la ONU. De hecho, el 21 de enero de 2025 (es decir, un día después de su investidura), el 47° presidente de Estados Unidos firmó la salida de su país de dicho acuerdo (El Mundo, 2025). Este enfoque unilateralista podría traducirse en una menor participación de Estados Unidos en diversas iniciativas internacionales, como la Convención de la ONU sobre Ciberdelincuencia. Asimismo, el enfoque “América Primero” podría llevar a una interpretación más restrictiva de las obligaciones internacionales en casos de extradición o intercambio de datos, lo que afectaría la capacidad de resolver casos de ciberdelincuencia, perjudicando a las víctimas que dependen de la cooperación judicial para garantizar el acceso a la justicia.

Por otro lado, la reciente aparición pública de Melania Trump en respaldo de la *Take It Down Act*¹⁶ plantea una dimensión inesperada en este análisis (BBC News, 2025). Su apoyo, respaldado por empresas como Meta y TikTok, podría indicar un intento del gobierno estadounidense por fortalecer la legislación nacional en materia de ciberdelincuencia y protección de la intimidad, en contraste con su escepticismo hacia los marcos multilaterales.

¹⁶ Una legislación bipartidista destinada a criminalizar la difusión no consensuada de imágenes íntimas, incluyendo aquellas creadas mediante IA. Durante su intervención en el Capitolio, Melania Trump enfatizó la urgencia de proteger, especialmente, a mujeres y niñas de la explotación en línea.

Esta última tendencia, que sin embargo se mantiene, podría dificultar la armonización de estándares globales en la lucha contra la violencia digital.

Finalmente, no se puede obviar que el historial de Donald Trump en temas de género sugiere un posible retroceso en el avance de políticas enfocadas en la protección de los derechos de las mujeres. Por esto, el ODS 5 podría enfrentarse a obstáculos si Estados Unidos reduce su apoyo a programas internacionales de protección contra la violencia digital. Teniendo esto en cuenta, se pasará al análisis normativo.

5. De Budapest a Montevideo: puentes y fisuras en la regulación global de la ciberdelincuencia

El objetivo de esta sección es realizar un análisis comparativo de los acuerdos vigentes redactados y publicados a la fecha, a partir de los postulados presentados anteriormente, teniendo en especial consideración la brecha de datos de género. A razón de lo anterior, se buscará complementar este estudio con el enfoque aportado por la teoría constructivista de las Relaciones Internacionales.

Entre la normativa a analizar, además del Convenio de Budapest del año 2001, se encuentra la Convención sobre Ciberdelincuencia de Naciones Unidas, adoptada en diciembre de 2024. Asimismo, se incluirá el Proyecto de Ley para la Tipificación de Ciberdelitos que se está tratando en el Parlamento uruguayo, elaborado durante la pandemia de COVID-19.

5.1 El Convenio de Budapest sobre Ciberdelincuencia (2001)

El Convenio sobre Ciberdelincuencia fue firmado en Budapest en el año 2001. De acuerdo con el Consejo Europeo, esta es la norma internacional más relevante y completa en relación a la ciberseguridad, aportando una guía a los Estados para la legislación en esta materia y como marco para la cooperación internacional en materia penal (Calcaterra Dufour, 2022). Además, de acuerdo con Iermano (2024), el Convenio enfrenta de forma directa e indirecta algunos tipos de violencia de género, ya sea perpetrada en el ciberespacio o mediante la tecnología.

Uruguay fue invitado formalmente en 2023 a ser parte de este Convenio, luego de la decisión tomada por el Comité de Ministros del Consejo de Europa. La misma responde al interés manifestado por la República Oriental en setiembre de 2022, al concluir un proceso de consultas con instituciones del Poder Ejecutivo competentes en la materia, coordinado por la Cancillería desde el año 2021 (Ministerio de Relaciones Exteriores, 2023). Sin embargo, aún

no se ha concretado dicha adhesión, por requerir una previa adecuación de las normas penales nacionales a las del Convenio¹⁷.

Desde su entrada en vigor, se han redactado dos protocolos adicionales: el primero, que fuera aprobado en 2003, tiene como objetivo incriminar los actos racistas y xenófobos, mientras que el segundo, del año 2021, busca potenciar la cooperación internacional entre Estados, autoridades competentes y con el sector privado en la divulgación de pruebas electrónicas (Calcaterra Dufour, 2022).

El éxito de este instrumento europeo es que las medidas previstas en él, concilian una respuesta eficaz por parte de la justicia penal con la salvaguardia del Estado de derecho. Por una parte, impone a los Estados parte que tipifiquen en sus códigos penales los delitos perpetrados en contra o mediante datos y sistemas informáticos, o relativos a la distribución de pornografía infantil, entre otros delitos; y, por otra, la obligación de reforzar los poderes en materia de derecho procesal y penal nacionales, dotando, *inter alia*¹⁸, a los sistemas judiciales los medios necesarios para garantizar pruebas electrónicas en relación a cualquier delito (Iermano, 2024). Indica la citada autora

la Convención de Budapest ofrece un marco interesante para combatir la violencia en línea y facilitada por la tecnología contra las mujeres, aún sin mencionarla, tanto desde el punto de vista procesal como de la cooperación internacional, especialmente en el punto de las investigaciones y para la seguridad de las pruebas electrónicas (Iermano, 2024, p. 79)¹⁹

Sin embargo, en el contexto presentado por esta monografía, el Convenio enfrenta desafíos al no abordar explícitamente este tipo de delitos teniendo en cuenta la brecha de datos de género. Esta omisión es particularmente significativa dado el impacto desproporcionado que los mismos tienen sobre la vida de las mujeres, en contravención con los principios de igualdad y no discriminación consagrados en la Agenda 2030, de la cual los Estados signatarios también lo son de Budapest del 2001.

Uno de los mayores retos en la persecución de vulneraciones transfronterizas de derechos de imagen e intimidad es la dispersión jurisdiccional. Las tecnologías como los *deepfakes* permiten que los perpetradores operen desde cualquier lugar del mundo, aprovechando vacíos legales y diferencias normativas entre Estados. El Convenio de Budapest aporta herramientas claves, como el establecimiento de mecanismos de cooperación

¹⁷ Aunque dicha adecuación ya ha sido emprendida con la aprobación de la ley N° 20.327, que será analizada en próximos apartados.

¹⁸ Entre otras cosas.

¹⁹ Traducción propia del italiano.

internacional para preservar evidencia digital transfronteriza (Art. 2) y facilitar el intercambio de información entre autoridades nacionales competentes (Art. 31). Además, si bien tipifica delitos como el acceso ilícito, la manipulación de datos y el fraude informático, el Convenio no incluye categorías específicas que se relacionen con la producción mediante IA de *deepfakes* de contenido sexual no consentido y su posterior distribución. Desde el punto de vista del DPI, esta omisión plantea interrogantes sobre la suficiencia de los marcos normativos para abordar las nuevas formas de ciberviolencia de género.

En este sentido, se entiende que la falta de normas materiales podría solucionarse mediante la adopción de protocolos adicionales como los ya existentes, que establezcan estándares específicos para el tratamiento de este tipos de casos. Algunas de sus disposiciones podrían establecer el reconocimiento de la manipulación y distribución no consentida de imágenes como una forma de violencia digital de género, así como incluir agravantes específicas en casos donde la víctima sea una mujer, en línea con los principios de protección diferencial establecidos, por ejemplo, por el Convenio de Estambul²⁰ y las recomendaciones de la CEDAW²¹.

Finalmente, la manipulación mediante IA y difusión de *deepfakes* íntimos de mujeres contraviene directamente el ODS 5 de la Agenda 2030. Estas vulneraciones perpetúan patrones de violencia de género y discriminación, exacerbando las desigualdades estructurales que enfrentan las mujeres en el ámbito digital. El Convenio de Budapest del año 2001, al no tener en cuenta explícitamente la mencionada brecha de datos de género, se queda corto frente a los compromisos internacionales de garantizar una vida libre de violencia y discriminación para las mujeres. Por ello sería necesario, entre otras cosas, que se incorporaran en su texto o en protocolos adicionales, disposiciones específicas que protejan a las mujeres contra la ciberviolencia de género, así como el fomento de la cooperación internacional para la eliminación de contenidos dañino mediante tecnologías de detección y eliminación proactivas de *deepfakes*.

²⁰ Aprobado en 2011, es un tratado del Consejo de Europa que busca prevenir y combatir la violencia contra las mujeres y la violencia doméstica, estableciendo medidas de protección, sanción y prevención. Este Convenio promueve la adopción de políticas integrales, el acceso a la justicia y la cooperación internacional para erradicar dichas violencias.

²¹ “Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer” por sus siglas en inglés; adoptada en 1979 por la Asamblea General de la ONU, es un tratado internacional que busca eliminar la discriminación de género en todos los aspectos de la vida. Establece una serie de medidas que los Estados deben tomar para garantizar la igualdad de derechos entre hombres y mujeres, promoviendo la eliminación de la discriminación en áreas como la política, la educación, el trabajo y la salud.

5.2 Convención sobre Ciberdelincuencia de Naciones Unidas (2024)

5.2.1 Contexto del inicio de las negociaciones y algunas controversias

La Convención fue propuesta por Rusia en el año 2017, con la intención de “combatir los problemas y amenazas que plantean los delitos en el ámbito de las tecnologías de la información y las comunicaciones” (Open Global Rights, 2024). En 2019, la Asamblea General de Naciones Unidas acordó, mediante la Resolución 74/247, el establecimiento de un comité *ad hoc* (CAH) encargado de dirigir las negociaciones. El mismo está abierto al ingreso de todos los Estados miembros de la ONU, así como otros actores en calidad de observadores, incluida la sociedad civil; éste órgano es presidido por la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) (Civics Lens, 2024).

Expertos y organizaciones de la sociedad civil advirtieron, durante el proceso de negociación, frente a posibles abusos que podrían perpetrar algunos Estados, sobretodo en lo referente a la restricción de derechos fundamentales como la libertad de expresión y la privacidad. Esto es particularmente preocupante para países con antecedentes de deficiencias en Derechos Humanos y autoritarismo, donde las leyes sobre ciberdelincuencia ya han sido utilizadas para perseguir a activistas, periodistas y defensores de Derechos Humanos.

Asimismo, el proceso de negociación ha sido criticado por su falta de transparencia y la limitada participación de actores de interés público. Pues, de esta manera podría facilitarse la adopción de normas globales que prioricen intereses estatales sobre la protección de derechos individuales, generando a la vez la legitimación de prácticas de vigilancia masiva o medidas desproporcionadas bajo el pretexto de combatir el cibercrimen.

El 9 de agosto de 2024, tras tres años de trabajo, los Estados miembros de la ONU alcanzaron finalmente el acuerdo respecto de esta nueva convención. El texto final fue aprobado por la Asamblea General para su adopción formal el 26 de diciembre de 2024, sin ser sometido a votación (UNODC, 2024); la firma del documento se abrirá en una ceremonia a ser celebrada en Vietnam en 2025, entrando en vigor 90 días después de la ratificación del 40° signatario. La UNODC seguirá funcionando como secretaria del Comité *ad hoc*, y se ocupará de negociar un protocolo adicional, complementario a la Convención, así como una Conferencia de Estados partes.

5.2.2 Análisis normativo: algunas comparaciones con el Convenio de Budapest (2001)

El Preámbulo de la Convención reconoce de forma explícita la importancia de incorporar una perspectiva de género en las medidas para combatir la ciberdelincuencia. Este enfoque es un avance significativo en comparación con el Convenio de Budapest del 2001, que no aborda de manera específica los impactos diferenciados de la ciberdelincuencia en hombres y mujeres. Además, se subraya la necesidad de proteger los Derechos Humanos, incluidos los relativos a la privacidad y la protección de datos personales. Este reconocimiento es clave para abordar el uso de tecnologías como la IA generativa para vulnerar los derechos de imagen e intimidad de las mujeres.

A razón de lo anterior, el artículo 16 de la Convención tipifica como delito la difusión no consentida de imágenes de carácter íntimo, un avance esencial para proteger los derechos de las mujeres en el ciberespacio. Este artículo establece lo siguiente:

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito en su derecho interno la venta, distribución, transmisión, publicación o facilitación de otra manera, de forma deliberada y sin derecho, de una imagen de carácter íntimo de una persona por medio de un sistema de tecnología de la información y las comunicaciones, sin el consentimiento de la persona mostrada en la imagen.

2. A los efectos del párrafo 1 del presente artículo, por “imagen de carácter íntimo” se entenderá un registro visual de una persona mayor de 18 años de edad captado por cualquier medio, con inclusión de un registro fotográfico o videográfico, que sea de carácter sexual, en el cual estén expuestas las partes íntimas de la persona o esta realice actividades sexuales, que fuera privado en el momento de captarse y respecto del cual la persona o personas mostradas tuvieran una expectativa razonable de privacidad en el momento de perpetrarse el delito.

3. Un Estado parte podrá ampliar la definición del término “imagen de carácter íntimo”, según proceda, a las representaciones de personas menores de 18 años de edad si han alcanzado la edad mínima legal para realizar actividades sexuales establecida en el derecho interno y la imagen no muestra abusos o explotación de niños.

4. A los efectos del presente artículo, una persona menor de 18 años de edad mostrada en una imagen de carácter íntimo no puede consentir la difusión de una

imagen de carácter íntimo que constituya material que muestre abusos sexuales de niños o explotación sexual de niños en virtud del artículo 14 de esta Convención.

5. Los Estados partes podrán exigir como requisito que exista el propósito de causar daños para que se considere que existe responsabilidad penal.

6. Los Estados partes podrán adoptar otras medidas en relación con los asuntos vinculados al presente artículo, de conformidad con su derecho interno y en consonancia con las obligaciones internacionales aplicables.

Como puede leerse, este artículo también proporciona una clara definición de lo que se considerará una “imagen de carácter íntimo”, no obstante a que los Estados la amplíen de acuerdo con su normativa nacional. En esto se diferencia del Convenio de Budapest, el cual proporciona un marco amplio para combatir la ciberdelincuencia, pero no incluye disposiciones específicas para este tipo de delitos. Asimismo, refuerza indirectamente la protección de las mujeres, recayendo en su ámbito de aplicación los delitos analizados por la presente monografía, en concordancia con el ODS 5 de la Agenda 2030 y el Pacto del Futuro.

Asimismo, la Convención de la ONU, aborda los aspectos relacionados con la jurisdicción (Capítulo II) y la cooperación internacional (Capítulo V). Ambas dimensiones son esenciales para enfrentar las vulneraciones transfronterizas de los derechos de imagen y a la intimidad de las mujeres; en primer lugar, el artículo 22 establece las bases para que los Estados parte determinen su jurisdicción penal sobre los delitos tipificados en la misma. Este artículo conoce la naturaleza transnacional de los ciberdelitos y prevé que los Estados ejerzan jurisdicción en los siguientes supuestos: cuando el delito sea cometido en su territorio (principio de territorialidad); cuando el delito sea cometido contra uno de sus nacionales (principio de personalidad pasiva); y cuando el delito sea cometido por un nacional de ese Estado (principio de personalidad activa). Además, se incluye una cláusula que permite a los Estados establecer jurisdicción en otros casos, contemplando incluso la imposibilidad de extraditar a quien los cometa.

Esta disposición es fundamental para resolver los conflictos de leyes y jurisdicciones que surgen de delitos transfronterizos. Sin embargo, puede darse el fenómeno de las jurisdicciones concurrentes, donde múltiples Estados puedan reclamar competencia sobre un mismo acto. Esto puede dificultar un enjuiciamiento efectivo, especialmente en casos como la distribución global de imágenes íntimas manipuladas, donde las plataformas digitales y los perpetradores pueden ubicarse en jurisdicciones diferentes. A razón de lo anterior, sería ideal que la Convención incluyera directrices más claras sobre la priorización de jurisdicciones o

mecanismos específicos para resolver disputas entre Estados, ya que esto afecta particularmente a las víctimas.

En segundo lugar, el Capítulo V establece un marco exhaustivo para la cooperación internacional en materia de ciberdelincuencia, abarcando medidas como la asistencia judicial mutua (Artículo 35), la extradición (Artículo 44), la preservación de evidencia digital²² y la eliminación del contenido ilícito (Artículo 41). En el caso de este último artículo, parece pertinente señalar que el mismo no establece directrices específicas sobre cómo garantizar la colaboración de las plataformas digitales. Sin embargo, estas disposiciones son cruciales para garantizar una respuesta coordinada a los delitos transfronterizos perpetrados en el ciberespacio, donde la rapidez y la eficacia de las acciones conjuntas determina el éxito de las investigaciones y procesos judiciales.

Si se compara con el Convenio de Budapest (2001), puede apreciarse que ambos enfatizan la importancia de la cooperación internacional; sin embargo, la Convención de Naciones Unidas ofrece disposiciones más específicas y actualizadas para abordar el flujo global de información, lo que lo hace más adecuado frente a nuevas tecnologías como la IA generativa.

Continuando con el análisis de las disposiciones, en su artículo 34, el instrumento multilateral se centra en la asistencia y protección de las víctimas, incluyendo medidas específicas como: procedimientos para obtener indemnización y restitución, la incorporación de una perspectiva de género en la protección y asistencia, especialmente para víctimas de delitos tipificados en los artículos 14 a 16 (abusos sexuales, explotación y difusión no consentida de imágenes), así como la ya mencionada eliminación de contenido dañino en línea, lo que es particularmente relevante para combatir la difusión de *deepfakes* íntimos. Esto también lo diferencia del Convenio de Budapest (2001), que se centra exclusivamente en la persecución de delitos; la Convención pone un énfasis significativo en la protección integral de las víctimas, alineándose con los principios de la Agenda 2030 y el enfoque centrado en las personas. Por esto, es importante destacar que la Convención de Naciones Unidas reafirma la importancia de garantizar que los procedimientos judiciales y las medidas adoptadas no revictimicen a las mujeres, fomentando paralelamente la capacitación de las autoridades

²² Aunque el artículo 29 no pertenece al capítulo de cooperación, se entiende que el mismo es complementario y relevante para este análisis. Establece que los Estados deben garantizar la preservación rápida de los datos electrónicos relacionados con los delitos, incluso antes de que se presente una solicitud formal de asistencia judicial. Esto es especialmente útil en casos donde el contenido ilícito circula rápidamente en línea, lo que puede dificultar su rastreo si no se toman medidas inmediatas.

judiciales en temas de género y ciberviolencia, un componente igualmente ausente en el Convenio de Budapest (2001).

En definitiva, la Convención, aunque nunca menciona a la IA específicamente, representa un avance significativo en comparación con el Convenio de Budapest, al abordar de manera específica las vulneraciones transfronterizas de los derechos de imagen y a la intimidad, con un enfoque claro en la protección de las mujeres y teniendo en cuenta la brecha de datos de género. Este enfoque es crucial para enfrentar desafíos modernos como la proliferación de deepfakes íntimos, no consentidos por las víctimas. En aras de fortalecer aún más este marco jurídico internacional, sería prudente garantizar mecanismos efectivos para la cooperación internacional en tiempo real, sobre todo respecto del borrado del contenido en línea; a su vez, deberán integrarse estándares más claros respecto de la responsabilidad de las plataformas digitales como principales canales de difusión de los deepfakes. Ofrece una oportunidad óptima para establecer un marco jurídico verdaderamente inclusivo, centrado en la protección de los Derechos Humanos y la igualdad de género en el entorno digital, al ser el primer documento internacional contra el crimen en 20 años.

5.3 Uruguay frente a los desafíos tecnológicos: normativa, estrategias e inteligencia artificial

En esta sección, se analizarán las principales acciones adoptadas por Uruguay para responder a los desafíos del ciberespacio, con especial atención a la Ley N.º 20.327, recientemente promulgada, y a las estrategias nacionales orientadas a la regulación de la IA y la ciberseguridad. Por un lado, se describirá el posicionamiento del país en relación con la agenda tecnológica global y sus iniciativas específicas para promover un uso ético y responsable de la IA. Por otro, se examinará la Ley N.º 20.327 en comparación con instrumentos internacionales como la Convención de Budapest (2001) y la Convención sobre Ciberdelincuencia de la ONU (2024), destacando las similitudes, diferencias y áreas de oportunidad para fortalecer el marco normativo nacional en un contexto globalizado.

5.3.1 Posicionamiento y estrategias nacionales: hacia una agenda tecnológica inclusiva y ética

De acuerdo con la revisión literaria, Uruguay se perfilaba en 2020 como líder regional en la temática de ciberseguridad (BID y OEA, 2020). El inicio de la implementación de políticas digitales en el país se remonta a la segunda mitad de la década de 2000. Según Calcaterra Dufour (2022), se destacan cuatro hitos clave relacionados con la ciberseguridad en

Uruguay: en 2005, la creación de la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC) como unidad ejecutora del gobierno; en 2008, la fundación dentro de esta agencia del Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy); en 2015, el establecimiento del Equipo de Respuesta a Incidentes de Seguridad Cibernéticos (D-CSIRT) dentro del Ministerio de Defensa; y, finalmente, en agosto de 2021, la creación de la Unidad de Ciberdelitos en el Ministerio del Interior (p. 8). En este entramado institucional, corresponde a esta última unidad policial recibir y gestionar denuncias de víctimas privadas de ciberdelitos, como una mujer afectada por *deepfakes*.

En el marco de la cooperación internacional, Uruguay ha establecido vínculos con diversas organizaciones internacionales y nacionales para el intercambio de información, prácticas y coordinación de esfuerzos en la lucha contra el ciberdelito. Estos incluyen colaboraciones con fuerzas policiales, agencias de seguridad, empresas tecnológicas y organizaciones no gubernamentales (Ministerio del Interior, 2023).

La primera Agenda Digital de Uruguay fue lanzada en 2006 y, desde entonces, se han implementado cinco versiones. Su edición más reciente, la Agenda Digital 2025 - Sociedad Digital Resiliente (AGESIC, 2023), manifiesta el objetivo de lograr una “conectividad universal de calidad del Estado con la ciudadanía” (Calcaterra Dufour, 2022, p. 9). Este objetivo conlleva un aumento significativo del volumen de datos manejados por el Estado uruguayo, lo que subraya la necesidad de crear un espacio digital seguro. En este contexto, los objetivos de ciberdelincuencia de la Agenda incluyen la adopción del Marco de Ciberseguridad creado por AGESIC, centrado en áreas como “servicios, infraestructura y redes críticas; educación sobre ciberseguridad; e implementación de nuevas tecnologías de análisis predictivo y automatización de respuestas” (Calcaterra Dufour, 2022). Sin embargo, la Agenda 2025 carece de propuestas específicas sobre cooperación internacional y su única referencia a la seguridad jurídica menciona de forma genérica la “promoción de la adhesión a estándares y convenciones internacionales” (AGESIC, 2023), sin detallar mecanismos para concretar esta adhesión, lo que limita su alcance práctico a pesar de su alineación con postulados constructivistas.

Alineado con estas iniciativas, Uruguay ha avanzado significativamente en la formulación de un marco regulatorio para abordar los desafíos y oportunidades asociados con la inteligencia artificial (IA). El 28 de junio de 2024, AGESIC presentó al Poder Legislativo el Informe sobre recomendaciones para una regulación de la inteligencia artificial, estructurado en tres orientaciones principales: desarrollo ético, protección de derechos

humanos y promoción de la innovación tecnológica. Entre las recomendaciones, destaca la revisión y actualización de la normativa vigente para garantizar que las aplicaciones de IA respeten los derechos fundamentales, con especial atención a la protección de los derechos de imagen e intimidad, particularmente de grupos vulnerables como las mujeres (AGESIC, 2024).

Complementando estos esfuerzos, la Estrategia Nacional de Inteligencia Artificial 2024-2030 establece un marco integral para el desarrollo y uso ético, responsable y seguro de la IA en Uruguay. Esta estrategia se fundamenta en principios como el respeto a la dignidad humana, la equidad, la no discriminación y el fortalecimiento de la democracia. Además, pone un énfasis significativo en la protección de los derechos humanos y de los datos personales. Al promover una gobernanza basada en la transparencia, la rendición de cuentas y la protección de la privacidad, Uruguay busca mitigar los riesgos asociados al uso indebido de tecnologías emergentes como los *deepfakes*, fortaleciendo así su compromiso con la ciberseguridad y los derechos fundamentales.

Calcaterra Dufour (2022) cita al director ejecutivo de AGESIC, Heber Praguas, que en la Comisión de innovación, ciencia y tecnología celebrada el año 2021, expresó que “[Uruguay carece de] legislación específica en cuanto a ciberdelitos [...] salvo por algunas excepciones que la analogía permite, excepcionalmente, ya que en el derecho penal no es una herramienta de uso”. Asimismo, también se recupera la declaración de la especialista en seguridad de la informática y asesora de AGESIC, Dra. Jimena Hernández, quien hace hincapié en la desactualización del Código Penal uruguayo, el cual mantiene las figuras tradicionales a pesar de los pocos cambios que ha sufrido. De acuerdo con ella, los ciberdelitos “se amparan en lo que tiene que ver con los accesos indebidos a sistemas o los daños que se pueden generar a un sistema” (p. 9).

5.3.2 La Ley N.º 20.327 en perspectiva internacional: un análisis comparativo con el Convenio de Budapest (2001) y la Convención de Naciones Unidas sobre Ciberdelitos (2024)

La preocupación por la ciberseguridad ha entrado a las Cámaras del Poder Legislativo, concretamente, a través de la aprobación, en setiembre de 2024, de la ley N.º 20.327 para la Tipificación de Ciberdelitos. El proyecto que la precediera no es el primero de su calidad en ser introducido, sino el quinto; la diferencia con sus homólogos anteriores es que, actualmente, se conjugan una serie de fundamentos que lo hacen cobrar mayor fuerza: en primer lugar, diversos actores internacionales (BID, OEA, delegación de la UE en Uruguay y

la Embajada de EEUU) que, en conjunto con actores nacionales como la AGESIC, generan presión sobre el Estado uruguayo, entre otras cosas, debido al incremento en las cifras de los ciberataques. Además se debe tener presente que el proyecto de ley fue elaborado durante la pandemia de COVID-19, momento de extrema vulnerabilidad de los sistemas de las empresas, ahora trasladados a las computadoras personales de los empleados debido al teletrabajo.

Alineado con los principios y normativas establecidos en el Convenio de Budapest (2001), la ley tiene como objetivo brindar soluciones legales para combatir la ciberdelincuencia, actualizar el Código Penal y promover la educación en ciberseguridad (Cámara de Senadores, 2024). Para la actualización del Código, la propuesta introduce una serie de artículos orientados a tipificar diversos delitos cibernéticos: acoso telemático, fraude informático, daño informático, acceso ilícito a datos informáticos y suplantación de identidad. A continuación, se describirán los mismos, para luego proceder a compararlos con los artículos que componen la Sección 1 “Derecho penal sustantivo, Capítulo II del Convenio de Budapest, así como con los artículos correspondientes de la Convención de la ONU, anteriormente analizados.

El artículo 1 de la ley uruguaya sanciona el acoso telemático, definido como la persecución, vigilancia o intento de contacto no deseado con otra persona mediante el uso de medios electrónicos. Las penas previstas para el mismo se agravan si la víctima es un menor de edad, personas con quienes previamente el ejecutor haya tenido una relación afectiva o íntima, o una persona en situación de vulnerabilidad (Cámara de Senadores, 2024). Por su parte, el Convenio no incluye este delito explícitamente, pero su marco general permite que los Estados parte legislen internamente para abordar estos delitos emergentes, en función de sus contextos locales. En cambio, la Convención de la ONU tampoco aborda este delito de forma explícita, pero introduce disposiciones relacionadas con la protección de datos personales; por lo tanto, el acoso telemático podría entrar dentro de su ámbito de aplicación.

El fraude informático está tipificado en el artículo 3, penalizando el uso indebido de sistemas informáticos para realizar cualquier tipo de operación no consentida con el fin de obtener beneficios económicos. Budapest (2001) aborda este tema en su artículo 8, aunque el proyecto uruguayo es más específico en cuanto a las formas que puede adoptar este fraude. La ONU también tipifica este delito en su Convención, pero con disposiciones adicionales sobre la cooperación internacional para rastrear y congelar activos financieros relacionados con el mismo.

Se introduce por el artículo 5 el daño informático, el cual penaliza la destrucción, alteración o inutilización de sistemas informáticos o datos con la intención de causar daños. Este delito tiene como agravante la irreparabilidad del daño o la afectación de estructuras críticas del Estado. Por su parte, el Convenio europeo, tipifica este delito en sus artículos 4 y 5, destacando la importancia de proteger la integridad de los datos y los sistemas críticos. En la Convención de la ONU, este tipo de daño se relaciona con disposiciones más amplias sobre ciberseguridad estatal y protección de infraestructuras críticas, alineándose en términos generales con ambos instrumentos pero incluyendo mecanismos avanzados de cooperación para prevenir ataques transfronterizos.

El artículo 6 de la ley N° 20.327 sanciona el acceso ilícito a datos informáticos, penalizando el ingreso no autorizado a sistemas o datos digitales, buscando proteger igualmente la privacidad de las personas como la seguridad de las instituciones. El artículo 2 del Convenio de Budapest tiene en cuenta el mismo delito, destacando la importancia de proteger los datos y la privacidad de los usuarios. De manera complementaria, la Convención de la ONU amplía esta regulación al establecer que los Estados deben adoptar medidas específicas para la preservación de evidencia digital transfronteriza, fortaleciendo la persecución penal en un entorno global.

De igual manera, el mismo artículo sanciona la interceptación ilícita y la vulneración de datos. Respecto de la primera, se pena a quien intercepte, interrumpa o interfiera por medios técnicos aquellos datos informáticos no públicos. Este delito se encuentra alineado con lo dispuesto en el artículo 3 de Budapest 2001; sin embargo, la normativa uruguaya amplía el alcance al incluir también la interrupción o interferencia de datos, aspectos no desarrollados en el texto de Budapest. Por otro lado, la Convención de la ONU, en su artículo 10 introduce disposiciones más específicas que abarcan tanto la transmisión como el almacenamiento de datos, reflejando una evolución normativa que se aproxima más a las disposiciones de la norma nacional.

En cuanto a la vulneración de datos es definida como el acceso, apoderamiento, uso o modificación de datos confidenciales de terceros, sin la autorización del titular; asimismo, se sanciona a aquellos que difundan, revelen o cedan a terceras personas los datos, hechos o imágenes registradas en soportes digitales. Este concepto encuentra paralelismos con el artículo 2 del Convenio de Budapest (2001), que protege la confidencialidad de los sistemas informáticos mediante la penalización del acceso ilícito. Sin embargo, la descripción del delito en Budapest no abarca explícitamente la “difusión o cesión a terceros”, dejando una

brecha que sí está contemplada tanto en la ley uruguaya como en el artículo 13 de la Convención de Naciones Unidas. Este último, además, incluye la alteración o el uso indebido de datos, consolidando un enfoque más completo hacia estos delitos.

Son agravantes de este delito que el autor sea el encargado de custodiar los soportes, que el afectado sea un menor de edad o un adulto incapaz, que se cometa con finalidad lucrativa, que sea cometido en afectación de los datos personales tutelados por la ley N° 18.331²³ y, finalmente, que se trate de datos estatales o vinculados a estructuras críticas. Esto es un avance importante en contraposición con los instrumentos internacionales: mientras Budapest (2001) no establece agravantes específicos, la Convención de la ONU incluye disposiciones sobre datos sensibles y sectores vulnerables, reflejando una mayor atención a la protección de datos personales y derechos humanos.

Por último, uno de los delitos más relevantes tipificados en la ley nacional es la suplantación de identidad (artículo 7). Este delito sanciona la adopción o apropiación de la identidad de otra persona, a través de medios electrónicos, para cometer fraudes o causar daño a la víctima. El Convenio no aborda explícitamente la suplantación de identidad como delito separado, aunque muchos aspectos de este pueden entrar dentro del ámbito de aplicación del artículo 2 del instrumento europeo. Por su parte, la Convención de la ONU tampoco incluye este delito de forma explícita, lo que representa una debilidad en un contexto donde las identidades digitales son frecuentemente utilizadas para perpetrar ciberdelitos.

Martín Pecoy (2021) realiza también un análisis comparativo profundo entre ambos instrumentos y establece los antecedentes para futuros debates; en primer lugar, algunos delitos tipificados por el proyecto (artículos 1, 2 y 6) ya se encuentran comprendidos en el corpus normativo uruguayo, por lo que podría llevar a una derogación tácita de los mismos. Para Pecoy, sólo castigar no soluciona el problema en el caso del artículo 3, como tampoco lo hace elevar el castigo, en caso de ser ya existente, sin justificación (refiere a los artículos 4, 5 y 9 del proyecto).

Finalmente, el artículo 8 sanciona el abuso de los dispositivos, entendido como la producción, adquisición, importación, comercialización o facilitación de programas, sistemas informáticos o telemáticos, credenciales o contraseñas de acceso, destinados a cometer un delito. En comparación, mientras que la Convención de Budapest (2001) proporciona un

²³ La Ley N.º 18.331 de Protección de Datos Personales y Acción de Habeas Data (2008) regula el tratamiento de datos personales en Uruguay, incluyendo datos sensibles como origen racial, preferencias políticas y salud. La normativa establece principios como legalidad, veracidad y consentimiento informado, además de derechos como el acceso y la rectificación. Aunque aplica al ámbito público y privado, excluye datos vinculados a actividades personales y seguridad del Estado. (Ley N.º 18.331, 2008).

marco inicial para sancionar el abuso de dispositivos (artículo 6), la Convención de la ONU regula de forma explícita el uso indebido de credenciales y contraseñas en su artículo 15. Esto refleja un enfoque adaptado a los desafíos tecnológicos actuales, incorporando además agravantes relacionados con el uso de estas herramientas en redes críticas o en perjuicio de datos sensibles, lo que refuerza la protección de las víctimas y la seguridad de los sistemas (Naciones Unidas, 2024).

Uno de los pilares de este ajuste del Código, y de la ley en general, es la campaña educativa, promovida por el Poder Ejecutivo y orientada a formar a la población sobre ciberseguridad y finanzas personales. Siendo el primer aspecto de mayor relevancia, se destaca la intención de instruir sobre fraudes comunes, como el phishing, vishing y smishing, cada vez más sofisticados, representando gran riesgo para los usuarios digitales. El objetivo de implementar estas medidas educativas es concientizar a la población, en aras de prevenir y mitigar los efectos de la ciberdelincuencia.

En el marco de esta ley se promueve la creación de un registro de ciberdelincuentes, cuya finalidad sería facilitar la identificación y prevención de operaciones fraudulentas. Este registro permitiría mayor control y prevención de fraude financiero por parte de las emisoras de dinero e instituciones financieras.

A raíz de la información recopilada y gracias al análisis comparado realizado, puede decirse que la ley uruguaya representa un esfuerzo integral para actualizar el marco legal y proteger tanto a individuos como instituciones de los crecientes riesgos del entorno digital. Al alinearse con los principios del Convenio de Budapest (2001), Uruguay está avanzando hacia una regulación más robusta, aunque aún tiene espacio para incorporar ciertas áreas adicionales, como los delitos relacionados con el contenido. Con la tipificación de estos delitos, el país está construyendo una base sólida para enfrentar los desafíos de la ciberdelincuencia en un contexto global, aunque “llama la atención la ausencia de propuestas relativas a la aprobación de la cooperación internacional” (Calcaterra Dufour, 2022). Para esto, la Convención de la ONU complementa estas disposiciones al ofrecer un enfoque internacional más inclusivo y detallado, con énfasis en la cooperación transfronteriza y la contemplación explícita de la brecha de datos de género, lo que sugiere oportunidades para futuras reformas nacionales e internacionales.

Capítulo IV

6. Conclusiones: El papel de las normas internacionales en la protección de los derechos a la imagen y a la intimidad de las mujeres (y de todas las personas)

El análisis realizado a lo largo de este trabajo ha puesto en evidencia que la ausencia de una regulación explícita sobre los *deepfakes* pornográficos en el Derecho Penal Internacional no sólo deja a las víctimas en un estado de indefensión jurídica, sino que también refuerza una estructura de desigualdad en la que la brecha de datos de género y la industria pornográfica operan en mutua retroalimentación. La falta de normativas que atiendan de manera específica la manipulación audiovisual con inteligencia artificial permite que la pornografía digital evolucione hacia formas de consumo cada vez más accesibles, hiperpersonalizadas y carentes de control, favoreciendo la consolidación de un modelo en el que los cuerpos de las mujeres siguen siendo utilizados como mercancía visual.

Desde un enfoque constructivista de las Relaciones Internacionales, esta problemática no puede analizarse en términos puramente normativos, sino que debe comprenderse dentro de un marco más amplio de producción de significados, valores y normas en el sistema internacional. La falta de regulación de los *deepfakes* no es solo una omisión técnica o un vacío legal, sino la manifestación de un orden internacional construido en torno valores que históricamente han priorizado los grandes intereses económicos de la industria pornográfica sobre los de los individuos. La ausencia de normas que protejan de manera efectiva los derechos de imagen e intimidad de las mujeres no es accidental, sino que responde a una estructura de poder que ha minimizado el impacto de la violencia digital de género y ha relegado estas discusiones a un plano secundario en la agenda internacional, además de perpetrar la adicción de los consumidores a este tipo de contenido.

En relación con la última afirmación, la normalización del consumo de contenido pornográfico manipulado tiene implicaciones directas en la construcción de subjetividades y en la forma en que los individuos, especialmente los hombres, perciben la sexualidad y las relaciones interpersonales. Como han señalado estudios en neurociencia, el acceso ilimitado a la pornografía genera procesos de desensibilización, reconfigurando los circuitos de recompensa del cerebro y reforzando patrones de consumo compulsivo. En este contexto, la hiperrealidad que ofrecen los *deepfakes* no solo intensifica esta dependencia, sino que también reduce la capacidad de los consumidores para diferenciar entre contenido real y manipulado,

lo que en última instancia refuerza la percepción de la mujer como un objeto de consumo sin agencia ni consentimiento. Esto sin dejar de lado que la afectación de los sujetos es diferente; como se ha podido ver en la reseña de casos, mientras que los hombres se ven perjudicados en su esfera privada, las mujeres ven las consecuencias de la manipulación de su imagen en sus círculos sociales, tanto personales como laborales.

Si bien los Objetivos de Desarrollo Sostenible (ODS) y la Agenda 2030 han incorporado compromisos orientados a la igualdad de género (ODS 5) y a la promoción de la salud mental y el bienestar (ODS 3), su impacto real en el ámbito de la violencia digital y la regulación de la inteligencia artificial sigue siendo marginal, pues la misma no estaba tan difundida en el momento de la firma del compromiso en 2015. La realidad es que, aunque estos instrumentos han permitido generar un marco de referencia internacional para la protección de derechos, la implementación efectiva de políticas que regulen la producción y distribución de contenido *deepfake* ha sido insuficiente hasta la fecha.

En este sentido, el Informe Global de la Brecha de Género 2024 del Foro Económico Mundial ha señalado que, al ritmo actual de los avances, tomará 134 años alcanzar la paridad de género a nivel global (Whitting, 2025). Esta proyección no sólo pone de manifiesto la persistencia de desigualdades estructurales, sino que también subraya la necesidad de que las iniciativas regulatorias sobre IA incorporen la existencia de la brecha de datos de género. La inexistencia de censos que reflejen con precisión el impacto de la pornografía en las dinámicas sociales y en la configuración de la subjetividad masculina es un claro ejemplo de cómo la brecha de datos de género sigue afectando la toma de decisiones en este ámbito. Desde la perspectiva constructivista de las Relaciones Internacionales, el problema radica en que los marcos normativos actuales no solo reflejan las estructuras de poder existentes, sino que también contribuyen activamente a su reproducción, consolidando un *statu quo* en el que la seguridad digital y la protección de la intimidad siguen siendo percibidas como problemas individuales en lugar de desafíos estructurales del sistema internacional.

El Pacto para el Futuro (2024), por otro lado, ha sido presentado como una herramienta para fortalecer la cooperación internacional y garantizar que las tecnologías emergentes sean utilizadas de manera ética y equitativa. Sin embargo, su efectividad dependerá de la capacidad y voluntad de los Estados soberanos para establecer mecanismos concretos que no solo contemplen la protección de las víctimas, sino que también aborden el impacto de la pornografía digital en la construcción de la desigualdad, teniendo en cuenta la manera en la que afecta al cerebro del adicto. El hecho de que la paridad de género aún esté a

más de un siglo de distancia refuerza la idea de que el sistema internacional no ha priorizado políticas estructurales que transformen la raíz de estas desigualdades, dejando a la conjugación de la regulación digital la violencia de género en un segundo plano. Regular los *deepfakes* es más que una cuestión de seguridad cibernética: es un imperativo para detener la escalada de un modelo de consumo que perpetúa dinámicas de violencia simbólica y estructural contra las mujeres.

Desde la perspectiva de las Relaciones Internacionales, la gobernanza global sobre estos temas requiere una mayor representación de voces diversas en los espacios de decisión. Para que la brecha de datos de género se reduzca de manera efectiva, es fundamental que la regulación de la inteligencia artificial y de los *deepfakes* pornográficos no sea elaborada únicamente desde una visión tecnocrática o reduccionista, sino que incorpore un enfoque interdisciplinario que escuche tanto a las mujeres afectadas como a la comunidad científica. Es imprescindible que los espacios de negociación internacional incluyan la participación de mujeres expertas en derecho, tecnología y derechos humanos, pero también que se tomen en cuenta los hallazgos de la neurociencia sobre cómo la pornografía moldea la percepción de la sexualidad y la afectividad, especialmente en los hombres, quienes, si bien no son los únicos que consumen, por su biología, son más propensos a desarrollar adicción.

Este enfoque transversal y basado en la evidencia es clave, porque la brecha de datos de género no puede reducirse únicamente a partir de la voz de las mujeres; es un problema estructural que afecta a toda la sociedad y que debe abordarse de manera racional y colectiva. La regulación efectiva de los *deepfakes* pornográficos solo será posible si se fomenta un debate informado en el que las distintas disciplinas y actores sociales puedan aportar soluciones integrales. No se trata solo de criminalizar a quienes producen y consumen este contenido, sino de transformar las condiciones que permiten su proliferación descontrolada y su consumo compulsivo.

Finalmente, aunque las normativas existentes en el Derecho Penal Internacional –como la Convención de Budapest (2001) y la Convención de la ONU sobre Ciberdelincuencia (2024)–, así como en el derecho nacional uruguayo –es decir, la Ley N° 20.327–, constituyen avances importantes en la regulación de la ciberdelincuencia, este trabajo ha demostrado que no son suficientes para abordar los *deepfakes* pornográficos de manera integral. La existencia de estos marcos jurídicos es, sin duda, preferible a un vacío normativo absoluto; sin embargo, su eficacia se ve limitada por la falta de una tipificación específica que atienda las vulneraciones transfronterizas de los derechos de imagen e

intimidad de las mujeres. Desde un enfoque constructivista de las Relaciones Internacionales, es fundamental reconocer que las normas no solo regulan la realidad, sino que también la construyen. Por ello, la inclusión de estos delitos en la agenda internacional no solo debe traducirse en sanciones penales, sino en la transformación del propio sistema normativo para que refleje una nueva concepción de seguridad digital contemplando la brecha de datos de género.

Como futura licenciada, considero que la intersección entre violencia de género, adicción a la pornografía y falta de regulación de los *deepfakes* configura un círculo vicioso que no solo perpetúa la desigualdad, sino que también obstaculiza la construcción de un entorno digital seguro y equitativo para todos los usuarios que se encuentran navegando en el ciberespacio. Esto se ve alimentado por la desconexión creciente entre el mundo digital y el real, distorsionando la percepción del entorno que tienen los usuarios, y agravando, en consecuencia, la vulnerabilidad frente a las agresiones digitales.

La regulación debe enmarcarse en estrategias más amplias de promoción de la educación digital efectiva, con énfasis en el trato de los datos personales, la transparencia en el desarrollo tecnológico y la rendición de cuentas de las plataformas que facilitan la circulación de este contenido. La misma no es solo una cuestión técnica o legal, sino una necesidad urgente para garantizar que los derechos fundamentales de los individuos sean protegidos, en un mundo donde la tecnología avanza a un ritmo mucho más acelerado que la capacidad del Derecho para responder a sus implicaciones y consecuencias en el plano real.

La IA ha llegado para quedarse, sobre todo debido a las grandes perspectivas de crecimiento productivo y económico, pero esto no implica que deba desatenderse su impacto en nuestras vidas cotidianas. El reto no es únicamente normativo, sino profundamente político y social: no se puede permitir que la estructura jurídica internacional siga operando bajo lógicas obsoletas, dominadas por grandes intereses económicos. En este contexto de fragilidad de los usuarios digitales, es fundamental tener presente la idea planteada por Martha Finnemore: “El contexto normativo también cambia con el tiempo y, a medida que cambian las normas y los valores internacionales, crean cambios coordinados en los intereses y el comportamiento de los Estados en todo el sistema.” (p. 2). Queda un largo camino por recorrer y, en última instancia, la verdadera transformación dependerá de la capacidad de la comunidad internacional para reconocer que la lucha contra la violencia digital no es solo una cuestión de ciberseguridad, sino un imperativo de derechos humanos.

Bibliografía

- Acale Sánchez, M. (2013). DERECHO PENAL, IMAGEN E INTIMIDAD: ESPECIAL REFERENCIA A LOS PROCESOS DE VICTIMIZACIÓN DE LAS MUJERES. *Revista de Derecho Penal y Criminología*, 10.
- AGESIC. (18 de diciembre 2023). *Agenda Uruguay Digital 2025 - Sociedad digital resiliente*. IMPO.
file:///C:/Users/Martina%20Lamaita/Downloads/Agenda%20Uruguay%20Digital%202025%20-%20Sociedad%20digital%20resiliente.pdf
- AGESIC (2024). *Informe sobre recomendaciones para una regulación de la inteligencia artificial*.
<https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/informe-sobre-recomendaciones-para-regulacion-inteligencia-artificial>
- AGESIC (2024). *Estrategia Nacional de Inteligencia Artificial Uruguay 2024–2030*.
<https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-nacional-inteligencia-artificial-uruguay-2024-2030-8>
- Aguado, Á. L. (2022). Neutralidad del derecho internacional privado en cuanto al género, una forma de violencia de género institucional. In *Anales de la Cátedra Francisco Suárez* (No. 2, pp. 293-326).
- Antony García, C. (2001). Perspectivas de la criminología feminista en el siglo XXI. *Revista de derecho y ciencias penales: Ciencias Sociales y Políticas*, (3), 249-259
- Ambos, K. (2004). Derechos Humanos y derecho penal internacional. *Diálogo Político*, 21(3), 85-115.
- Ambos, K. (2013). ¿Castigo sin soberano? La cuestión del ius puniendi en derecho penal internacional Una primera contribución para una teoría del derecho penal internacional consistente.
- Arvanitidis, B., Baron, M., Featherstone, O., Munsí, P., Platt, A., Polglase, K. (28 de agosto de 2024). *My identity is stolen: Photos of European influencers used to push pro-Trump propaganda on fake X accounts*. CNN.
<https://edition.cnn.com/2024/08/28/europe/fake-maga-accounts-x-european-influencers-intl-cmd/index.html>

-
- Asamblea General de las Naciones Unidas (2024). *Pacto para el Futuro*.
<https://docs.un.org/es/A/RES/79/1>
- AS. (2024). *Una árbitra suspendida de por vida por aparecer supuestamente en un video sexual*.
<https://as.com/tikitakas/famosos/una-arbitra-suspendida-de-por-vida-por-aparecer-supuestamente-en-un-video-sexual-n/>
- Banco Interamericano de Desarrollo, Organización de los Estados Americanos (2020). *Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y el Caribe*. Reporte Ciberseguridad 2020. www.observatoriociberseguridad.com
- Barrera Arrestegui, L., (2012). FUNDAMENTOS HISTÓRICOS Y FILOSÓFICOS DE LA INTELIGENCIA ARTIFICIAL. *UCV-HACER. Revista de Investigación y Cultura*, 1(1), 87-92.
- Bates, B. (2020). *Deepfake pornography and the end of consent*. *Journal of Media Ethics*, 35(2), 86-98.
- BBC News Mundo. (2025). *"Cada momento publicado en Instagram y Facebook lo convirtió en porno": cómo un hombre traicionó a su amiga usando su imagen con inteligencia artificial*. BBC News Mundo. <https://www.bbc.com/mundo/articles/cjdegvm50g4o>
- BBC News. (2025). *Melania Trump backs 'Take It Down Act' targeting non-consensual intimate images*. BBC News. <https://www.bbc.com/news/articles/c8d41zv4ng2o>
- Cabrera, C. T. (2024). El derecho a la propia imagen (ya la voz) frente a la inteligencia artificial. *InDret*, (1), 74-113.
- Cáceres Nieto, E. (2023). La inteligencia artificial aplicada al Derecho como una nueva rama de la teoría jurídica. *Anales de la Cátedra Francisco Suárez* 57, pp. 63-89.
- Cairolí Martínez, M. H. (2003). El Derecho Penal uruguayo y las nuevas tendencias dogmático penales. *Tomo II: Concursos, iter criminis, pena*. Fundación de Cultura Universitaria.
- Calcaterra Dufour, V. (2022). *Ciberseguridad en Uruguay: hacia la adhesión al Convenio de Budapest*.
- Cárdenas Aravena, C. (2021). La mujer y las consideraciones de género en el derecho penal internacional y en la justicia penal internacional. *Criminología feminista* (pp. 131-152). LOM Ediciones.
- Cerdán Martínez, V. M., Padilla Castillo, G. (2019). *Historia del fake audiovisual: deepfake y la mujer en un imaginario falsificado y perverso*.

-
- Cherif Bassiouni, M. (1982). El Derecho penal internacional: Historia, objetivo y contenido. *Anuario de derecho penal y ciencias penales*, 5-42.
- Chesney, R., Citron, D. (2019). *Deepfakes and the new disinformation war: The coming age of post-truth geopolitics*. *Foreign Affairs*, 98(1), 147-155.
- CIVICUS LENS (27 de setiembre de 2024). *La Convención de la ONU sobre ciberdelincuencia, un nuevo tratado inquietante*. CIVICUS LENS. <https://lens.civicus.org/la-convencion-de-la-onu-sobre-ciberdelincuencia-un-nuevo-tratado-inquietante/>
- Criado Pérez, C. (2020). *La mujer invisible. Descubre cómo los datos configuran un mundo hecho por y para los hombres/The invisible woman. Discover how data shapes a world made by and for men*. Editorial Seix Barral.
- Código Penal, Ley No. 9.155, Diario Oficial No. 17.327, (1933).
- Colmenares-Guillén, L. E., Hernández, J. L., De Jesús, J. (2020). Análisis del Iter Criminis de la pornografía infantil en Facebook. *Revista Visión Criminológica-Criminalística*, 8(31), 9-15.
- Constitución de la República Oriental del Uruguay, (1967)
- Convención de Budapest sobre la ciberdelincuencia (1 de julio de 2004)
- Convenio de Estambul sobre prevención y lucha contra la violencia contra las mujeres y la violencia doméstica (2011)
- Declaración Universal de Derechos Humanos, G.A. Res. 217A, Asamblea General de la ONU, 3ª Sesión, (1948).
- Del Arenal Moyúa, C., Sanahuja Perales, J. A. (2015). *Teorías de las relaciones internacionales*. Tecnos.
- Donnelly, J. (2011). La construcción social de los Derechos Humanos internacionales. *Relaciones Internacionales*, (17), 153-184.
- El Mundo. (11 de octubre 2024). *Suspenden de por vida a una árbitra tras la aparición de un supuesto vídeo sexual*. <https://www.elmundo.es/deportes/futbol/2024/10/11/6708f8af21efa0747d8b4577.html>
- El Mundo. (21 de enero de 2025). *El Ártico registra su temperatura más alta en la historia*. Recuperado de <https://www.elmundo.es/ciencia-y-salud/medio-ambiente/2025/01/21/678f6c89fdddf3d6f8b45a2.html>
- Fagan, P. (2009). *Los efectos de la pornografía*. Plataforma para la Política Cristiana.

-
- Fagioli, M., Sanguinetti, L. (2019). El derecho a la imagen en derecho uruguayo. *Revista de Derecho*, 18(35), 193-204.
- Finnemore, M. (1996). *National interests in international society*. Cornell University Press.
- Foro Económico Mundial. (2024). *Navigating Cyber Resilience in the Age of Emerging Technologies*. Foro Económico Mundial. <https://www.weforum.org/>
- Franganillo, J. (2022). Contenido generado por inteligencia artificial: oportunidades y amenazas. *Anuario ThinkEPI*, 16.
- Fresnedo de Aguirre, C. (2022). Derecho Internacional Privado, Tomo I, Parte General. *FCU, Montevideo*, 160-167
- Fresnedo de Aguirre, C. (2022). Derecho Internacional Privado, Tomo III, Parte Especial. *FCU, Montevideo*, 602-625.
- Fresnedo de Aguirre, C. (2022). Los estereotipos de género y cómo deconstruirlos. Una visión desde el Derecho Internacional Privado. *Revista de la Facultad de Derecho*, 10.22187/rfd2022nesp1a14
- Frosini, T. E. (2022). La privacy nell'era dell'intelligenza artificiale. *DPCE online*, 51(1).
- Gaeti Márquez, S. (2021). *Iter criminis*.
- Gaimari, G. (2021). *Inteligencia artificial e impacto en el cibercrimen* (Doctoral dissertation, Universidad de Belgrano-Facultad de Derecho y Ciencias Sociales-Abogacía).
- Garg, P., Raza, A., Kumar, R. (2021). *Deepfake pornography: A new challenge for cybersecurity and legal frameworks*. *International Journal of Cybersecurity Intelligence and Cybercrime*, 4(1), 23-40.
- Goldschmidt, W. (1951). Normativismo y normologismo en el Derecho penal y en el Derecho internacional privado. *Anuario de Derecho Penal y Ciencias Penales*, (3), 513-518.
- González Pulido, I. (2023). El uso de la inteligencia artificial generativa en la investigación de la ciberdelincuencia de género: ante el auge de los deepfakes. *IUS ET SCIENTIA*, 9(2), 157-180.
- Iermano, A. (2024). Violenza digitale e Convenzione di Istanbul: una dimensione distinta ma non separata dalla violenza contro le donne. *Freedom, security & justice: european legal studies: 1*, 2024, 64-95.
- IMPO. (2008). *Ley N.º 18.331: Protección de datos personales y acción de habeas data*. Recuperado de <https://www.impo.com.uy/bases/leyes/18331-2008>
- IMPO. (2024). *Ley N.º 20.327: Prevención y represión de la ciberdelincuencia*. Recuperado de <https://www.impo.com.uy/bases/leyes-originales/20327-2024>

- Kühn, S., Gallinat, J. (2014). *Brain structure and functional connectivity associated with pornography consumption: The brain on porn*. JAMA Psychiatry, 71(7), 827-834.
- Lara Aguado, A. (2022). Neutralidad del Derecho internacional privado en cuanto al género, una forma de violencia de género institucional. *Anales de la Cátedra Francisco Suárez. Protocolo II*, pp. 293-326.
- Martin, W. T., Kim, S. (28 de agosto de 2024). ‘Anyone Can Be a Victim’: Sprawling AI Fake Nudes Crisis Hits South Korea. *The Wall Street Journal*.
<https://www.wsj.com/world/asia/anyone-can-be-a-victim-sprawling-ai-fake-nudes-crisis-hits-south-korea-eec02232>
- McDonald, E. (11 de marzo de 2024). *La Convención de las Naciones Unidas sobre la Ciberdelincuencia, en pausa por ahora, pero su amenaza para los Derechos Humanos persiste*. Open Global Rights.
<https://www.openglobalrights.org/un-cybercrime-convention-pause-threat-human-rights-remains/?lang=Spanish>
- McKeil, A. (Anfitrión). (2024, agosto 5). *The importance of norms in international affairs: A conversation with Martha Finnemore* [Episodio de podcast]. En Good Authority. Spotify.
<https://open.spotify.com/episode/4z3aDSOFL5ZrUASmT9PGrW?si=3Z7ouwdOSVmSEA2Y2K8bRw>
- Méndez Hernández, M. (2021). Criminología feminista. Una revisión bibliográfica. *Asparkia. Investigació Feminista*, (39), 233-253
- Mendoza Enríquez, O. A (2021). El derecho de protección de datos personales en los sistemas de inteligencia artificial. *Revista Ius*, 15(48), 179-207.
- Michaels, R., Ruiz Abou-Nigm, V., van Loon, H. (2021). *The private side of transforming our world*. Intersentia.
- Ministerio del Interior (7 de junio de 2023). *¿Qué es la Unidad de Ciberdelincuencia?*
<https://www.gub.uy/ministerio-interior/politicas-y-gestion/es-unidad-ciberdelincuencia>
- Ministerio de Relaciones Exteriores. (14 de febrero de 2023). *Uruguay es invitado por el Consejo de Europa a adherir al Convenio de Budapest sobre Ciberdelincuencia*. GUB.UY. Recuperado de
<https://www.gub.uy/ministerio-relaciones-exteriores/comunicacion/comunicados/uruguay-es-invitado-consejo-europa-adherir-convenio-budapest-sobre>

-
- Morales Montilla, C. (2020). Estudio de los derechos de imagen ya la intimidad en internet desde el Derecho Internacional Privado. Evolución de la jurisprudencia del Tribunal de Justicia de la Unión Europea.
- Mosca, J. B. (2019). Protección patrimonial del derecho de imagen en América Latina. *Latin American Legal Studies*, 5, 37-68.
- Moscoso Restovic, P. M. (2010). *Competencia judicial civil internacional por daño ambiental: determinación del hecho dañoso y su extensión. El caso europeo*. Foro: Nueva época, 11-12, 193-229. Recuperado de <https://revistas.ucm.es/index.php/FORO/article/download/37216/36017/40190>
- Naciones Unidas. (2015). *Transformar nuestro mundo: La Agenda 2030 para el Desarrollo Sostenible*. <https://www.un.org/sustainabledevelopment/es/agenda-2030>
- Naciones Unidas. (2024). Proyecto de convención de las Naciones Unidas sobre ciberdelincuencia. Asamblea General de las Naciones Unidas, A/AC.291/L.15.
- Naciones Unidas. (s.f.). *Igualdad de género y empoderamiento de la mujer*. <https://www.un.org/es/global-issues/gender-equality>
- Neira, M. L. M. (2020). Uso y divulgación de la imagen personal: enfoques en el derecho romano, en el derecho colombiano y su actual interacción con la Inteligencia Artificial. *Revista La Propiedad Inmaterial*, 30, 169.
- ONU Mujeres. (2020). Objetivo 5: Lograr la igualdad entre los géneros y empoderar a todas las mujeres y las niñas. <https://www.unwomen.org/es/news/in-focus/women-and-the-sdgs/sdg-5-gender-equality>
- Ortega Giménez, A. (2013). Imagen y circulación internacional de datos. *Iuris Tantum Revista Boliviana de Derecho*, (15), 130-147.
- Pecoy Taque, M. (16 de agosto de 2021). *El proyecto de ley uruguayo del año 2021 que pretende la tipificación de los ciberdelitos en Uruguay*. Thomson Reuters. <https://laleyuruguay.com/blogs/novedades/el-proyecto-de-ley-uruguayo-del-ano-2021-que-pretende-la-tipificacion-de-los-ciberdelitos-en-uruguay>
- Pérez-Ugena, M. (2024). La inteligencia artificial: definición, regulación y riesgos para los derechos fundamentales. *Estudios de Deusto: revista de derecho Público*, 72(1), 207-337.
- Programa de las Naciones Unidas para el Desarrollo (PNUD). (2021). Informe sobre el Desarrollo Humano 2021.

- Rainews. (2024, octubre). *Condannato a 18 anni per creare immagini di abusi su minori con l'intelligenza artificiale*.
https://www.rainews.it/video/2024/10/usava-lintelligenza-artificiale-per-creare-immagini-di-abusi-su-minori-condannato-a-18-anni-d3a709cd-b9a2-4340-a2d8-212f9a9c1a65.html?nxtep?wt_mc=2.social.wzp.rainews.wt
- Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo de 13 de junio de 2024 relativo a la Inteligencia Artificial. Diario Oficial de la Unión Europea.
<http://data.europa.eu/eli/reg/2024/1689/oj>
- Sáez Tapia, C. (2017). Derecho a la Imagen Propia y su Manifestación en Internet.
- Sagñay, F. G. S., Noboa, W. P. R., Freire, N. F. (2024). Deepfakes Pornográficos: Impacto jurídico-probatorio y social en el Ecuador. *Reincisol.*, 3(6), 2912-2934.
- Security Hero. (2024). 2023: State of deepfakes.
<https://www.securityhero.io/state-of-deepfakes/#key-findings>
- Schouten, P. (2007). Teoría social de la política internacional. *Alexander Wendt y el constructivismo en las Relaciones Internacionales (Primera ed.)*.(C. del Arenal, Ed.) Madrid, España: Publicaciones Universidad Complutense de Madrid.
- Soler, E. S. (2023). Retos jurídicos derivados de la inteligencia artificial generativa. *InDret*.
- Solove, D. J. (2020). *Understanding Privacy in a Digital World*. Harvard University Press.
- Sortino, E. (11 de agosto de 2024). *Ciberseguridad: La ONU aprueba un tratado internacional sobre delitos digitales*. Vatican News.
<https://www.vaticannews.va/es/mundo/news/2024-08/ciberseguridad-onu-aprueba-tratado-internacional.html>
- UNODC. (26 de diciembre de 2024). *La Asamblea General de las Naciones Unidas adopta una convención histórica contra la ciberdelincuencia*. Oficina de las Naciones Unidas contra la Droga y el Delito.
<https://www.unodc.org/lpomex/es/noticias/diciembre-2024/la-asamblea-general-de-las-naciones-unidas-adopta-una-convencion-historica-contra-la-ciberdelincuencia.html>
- Van der Laan, J., Velthuis, O. (2021). *The social dynamics of pornography platforms: From commodification to parasocial interaction*. Digital Culture & Society, 7(1), 45-62.
- Varnet Pérez, T., & Cartes-Velásquez, R. (2021). *Impacto biopsicosocial de la pornografía en internet: una revisión narrativa de la literatura*. Revista Argentina de Ciencias del Comportamiento, 13(3), 34-48.

Wendt, A. (1999). *Social theory of international politics* (Vol. 67). Cambridge University Press.

Whiting, K. (2025, 28 de febrero). *International Women's Day: What is it and why do we need it?* Foro Económico Mundial.
<https://www.weforum.org/stories/2025/02/international-women-day-why-do-we-need-it/>

Wikipedia. (20 de enero 2025). *Investidura presidencial de Donald Trump en 2025*. Recuperado de https://es.wikipedia.org/wiki/Investidura_presidencial_de_Donald_Trump_en_2025

Wilson, G. (2014). *Your brain on porn: Internet pornography and the emerging science of addiction*. Commonwealth Publishing.