

GOBIERNO DE PUERTO RICO

20^{ma.} Asamblea
Legislativa

3^{ra.} Sesión
Ordinaria

SENADO DE PUERTO RICO

P. del S. 1289

26 de mayo de 2026

Presentado por el señor *Ríos Santiago*

Referido a

LEY

Para enmendar el Artículo 285 de la Ley 146-2012, según enmendada, conocida como el “Código Penal de Puerto Rico”, a los fines de tipificar y penalizar la destrucción, alteración, ocultación y fabricación de evidencia digital; establecer penas agravadas por el uso de inteligencia artificial generativa en la comisión de tales delitos; incorporar las definiciones tecnológicas; y para otros fines relacionados.

EXPOSICIÓN DE MOTIVOS

La era digital ha transformado radicalmente no solo la forma en que nos relacionamos y comunicamos, sino también el modo en que se cometen, investigan y adjudican los delitos. En la actualidad, las estructuras criminales operan sin barreras físicas, utilizando redes encriptadas y plataformas tecnológicas sofisticadas que ponen en evidencia las limitaciones de un ordenamiento penal que no ha evolucionado al mismo ritmo que la amenaza que pretende combatir.

La necesidad urgente de atender este asunto queda confirmada en los hallazgos del Informe Anual 2025 del Centro de Querellas de Crímenes por Internet del Buró Federal de Investigaciones (FBI IC3, por sus siglas en inglés). Dicho informe constató que los delitos cibernéticos generaron daños económicos cercanos a los \$21 mil millones en los Estados Unidos durante ese año. Dentro de ese renglón, resulta alarmante el

registro de 22,364 querellas directamente asociadas al uso ilícito de la inteligencia artificial, las cuales produjeron, por sí solas, mermas superiores a los \$893 millones. En ese contexto, Puerto Rico ocupa el último lugar entre las 52 jurisdicciones reportantes, posición que no obedece a una menor incidencia delictiva, sino a la ausencia de tipos penales expresos y actualizados que permitan identificar, clasificar y perseguir estas conductas de manera efectiva.

La evidencia digital constituye en la actualidad uno de los principales elementos probatorios del proceso penal. Un archivo digital puede destruirse con un simple comando, un metadato alterarse en segundos y una plataforma de nube vaciarse remotamente antes de que llegue la orden judicial de preservación. A ello se suma que la inteligencia artificial generativa permite fabricar evidencia de apariencia auténtica que desafía los métodos forenses convencionales. La proliferación de contenido sintético no solo facilita la fabricación de prueba falsa, sino que erosiona la confianza en la evidencia auténtica, con el potencial de paralizar el sistema de justicia criminal.

Ante esta realidad, el texto vigente del Artículo 285 resulta insuficiente. Su alcance se limita a la “prueba documental” y al “objeto” físico, omite la alteración y fabricación como conductas punibles, y no contempla referencia alguna a datos electrónicos, metadatos ni al uso de inteligencia artificial. El principio de legalidad, consagrado en el Artículo 2 del propio Código Penal y reafirmado en doctrina reiterada del Tribunal Supremo, establece que no se instará acción penal por un hecho que no esté expresamente definido como delito, prohibiendo taxativamente crear o imponer delitos por analogía para suplir estos vacíos. Esta incertidumbre jurídica compromete tanto la validez del proceso penal como las garantías constitucionales del acusado.

La presente medida legislativa es fruto de un proceso de consulta pública en el que comparecieron el Departamento de Justicia, la Policía de Puerto Rico, el Instituto de Estadísticas de Puerto Rico, la Oficina del Comisionado de Instituciones Financieras (OCIF) y Puerto Rico Innovation & Technology Service (PRITS), quienes coincidieron en

la necesidad de enmendar el Artículo 285 de nuestro Código Penal. Siguiendo la recomendación expresa de las agencias, el texto enmendado opera mediante principios generales y definiciones tecnológicamente neutrales, sin prescribir estándares técnicos rígidos, garantizando su vigencia ante la evolución constante de la tecnología.

Por otro lado, la norma aquí establecida reconoce que, en determinadas circunstancias, las víctimas de delitos pueden incurrir en la eliminación de evidencia digital movidas por el temor, la vergüenza, el impacto emocional del hecho o el desconocimiento tecnológico, sin que medie propósito alguno de obstaculizar la justicia. Tratar esta conducta con la misma severidad que la destrucción deliberada y premeditada sería contrario a los principios de proporcionalidad y justicia que inspiran nuestro ordenamiento penal. Por ello, la presente medida incorpora expresamente el elemento de intencionalidad como requisito indispensable del tipo penal, de manera que solo incurrirá en responsabilidad criminal quien actúe con el propósito deliberado de impedir la presentación o el uso de la evidencia, correspondiendo al Ministerio Público establecer dicho elemento más allá de duda razonable.

Al atemperar nuestro Código Penal, la presente medida también toma en consideración la realidad operativa de los sistemas de información contemporáneos. A tales fines, se establece una disposición de salvedad aplicable al sector corporativo e institucional, con el propósito de proteger la eliminación de datos que resulte de la ejecución rutinaria y automatizada de sus políticas de retención. Para acogerse a esta protección, es indispensable que la entidad actúe de buena fe, carezca de intención obstructiva y proceda con anterioridad a la notificación de una orden de preservación o requerimiento judicial.

A la luz de lo anterior, se declara como política pública que la integridad de la evidencia digital constituye un bien jurídico de la más alta importancia; que su destrucción, alteración, ocultación o fabricación representa una modalidad de obstrucción de la justicia de igual o mayor gravedad que sus manifestaciones en el

ámbito físico; y que el uso de inteligencia artificial generativa para llevar a cabo tales conductas intensifica el perjuicio ocasionado al sistema de justicia. Por tanto, considerando lo anterior, resulta procedente reconocer el uso de inteligencia artificial generativa en la comisión de estos delitos como una circunstancia agravante estatutaria que permita al tribunal, conforme a nuestro ordenamiento, imponer una pena proporcional al daño causado al proceso judicial.

Por todo lo cual, esta Asamblea Legislativa considera pertinente y meritorio enmendar el Artículo 285 del Código Penal de Puerto Rico. De esta manera, atemperamos la norma a nuestra realidad tecnológica, garantizando un balance justo que protege las operaciones institucionales legítimas mientras evita la impunidad de quienes se benefician del actual vacío normativo.

DECRÉTASE POR LA ASAMBLEA LEGISLATIVA DE PUERTO RICO:

1 Sección 1. — Se enmienda el Artículo 285 de la Ley Núm. 146 de 30 de julio de
2 2012, según enmendada, conocida como el "Código Penal de Puerto Rico", para que lea
3 como sigue:

4 “Artículo 285. — Destrucción de pruebas, *alteración, ocultación y fabricación de*
5 *evidencia.*

6 Toda persona que sabiendo que alguna prueba documental, *evidencia digital* o
7 cualquier objeto pudiera presentarse en cualquier investigación, procedimiento, vista o
8 asunto judicial, legislativo o administrativo, o cualesquiera otros trámites autorizados
9 por ley, la destruya, [o] esconda, *altere, oculte, o en el caso de evidencia digital, la fabrique,*
10 con el propósito de impedir su presentación, *uso o descubrimiento*, será sancionada con
11 pena de reclusión por un término fijo de tres (3) años.

1 *La destrucción, alteración, ocultación o fabricación de evidencia digital incluye, sin*
2 *limitarse a, las siguientes conductas:*

3 (1) *Destruir, borrar, sobrescribir o eliminar datos, archivos, registros electrónicos, metadatos*
4 *o cualquier información almacenada en formato digital, ya sea en dispositivos físicos,*
5 *sistemas remotos, plataformas de computación en la nube o servidores de terceros;*

6 (2) *Alterar, modificar, manipular o falsificar datos, archivos, metadatos, registros de*
7 *auditoría, marcas de tiempo o cualquier otra información digital, de forma tal que*
8 *comprometa su autenticidad o integridad como evidencia;*

9 (3) *Ocultar, transferir, cifrar con propósito obstructivo, o de cualquier otra manera hacer*
10 *inaccesible información o evidencia en formato digital a las autoridades o a las partes con*
11 *derecho a obtenerla conforme a derecho;*

12 (4) *Interferir, interrumpir o impedir la ejecución de una orden de preservación de datos*
13 *emitida conforme a derecho por una autoridad competente, incluyendo la instrucción a*
14 *un proveedor de servicios electrónicos para que elimine, destruya o no preserve la*
15 *información objeto de dicha orden;*

16 (5) *Crear, construir, generar o introducir en cualquier procedimiento información digital*
17 *falsa, alterada o fabricada que pretenda hacerse pasar como evidencia auténtica, con el*
18 *propósito de inducir a error a una autoridad investigativa, judicial, legislativa o*
19 *administrativa, o de inculpar falsamente a otra persona. Esta conducta será sancionada*
20 *con pena de reclusión por un término fijo de ocho (8) años.*

21 *Constituirá una circunstancia agravante estatutaria, por lo que el Tribunal podrá aumentar*
22 *la pena de conformidad con las disposiciones del Artículo 67 de este Código, cuando la conducta*

1 *tipificada se ejecute mediante el uso de herramientas de inteligencia artificial generativa,*
2 *incluyendo, sin limitarse a, la creación de contenido sintético, imágenes falsificadas, videos*
3 *manipulados, audios alterados, documentos fabricados o cualquier otro tipo de “deepfake” o*
4 *material sintético generado mediante algoritmos de aprendizaje automático o tecnologías*
5 *similares, presentes o futuras.*

6 *La pena aplicable bajo este Artículo podrá aumentarse hasta un máximo de doce (12) años*
7 *cuando la conducta resultare en la condena de una persona inocente, en la absolución de una*
8 *persona culpable, en la paralización de una investigación criminal activa, o en la afectación de los*
9 *derechos procesales de una víctima de delito.*

10 *La responsabilidad penal bajo este Artículo requiere que la conducta se realice con*
11 *conocimiento de que la información afectada podía ser relevante en un procedimiento y con el*
12 *propósito deliberado de impedir su uso o de engañar mediante contenido fabricado.*

13 *La eliminación de evidencia digital motivada exclusivamente por razones emocionales,*
14 *cognitivas o de desorientación tecnológica, sin la concurrencia del elemento de propósito*
15 *obstructivo deliberado, no configurará los delitos aquí tipificados. Corresponde al Ministerio*
16 *Público establecer el elemento de intencionalidad más allá de duda razonable.*

17 *De igual forma, no incurrirá en responsabilidad penal bajo este Artículo aquella persona*
18 *natural o jurídica que, de buena fe, elimine información digital como resultado de la ejecución*
19 *rutinaria y automatizada de políticas institucionales de retención y disposición de documentos.*
20 *Esta protección legal aplicará exclusivamente cuando la destrucción ocurra con anterioridad a la*
21 *recepción de una orden de preservación de datos, citación o requerimiento oficial. Además,*

1 *requerirá la ausencia de un propósito deliberado de obstruir una investigación o procedimiento*
2 *en curso.*

3 Si la persona convicta es una persona jurídica será sancionada con pena de multa
4 hasta diez mil dólares (\$10,000) cuando la conducta constituyó la modalidad física prevista en
5 el primer párrafo de este Artículo. Si la persona jurídica convicta incurrió en alguna de las
6 conductas sobre evidencia digital tipificadas en los incisos (1) al (4) de este Artículo, la multa
7 será de hasta cincuenta mil dólares (\$50,000) por cada violación. Si la conducta constituyó la
8 fabricación de evidencia digital tipificada en el inciso (5), la multa será de hasta cien mil dólares
9 (\$100,000). Cuando aplique además la agravante por uso de inteligencia artificial generativa, la
10 multa podrá ascender hasta ciento cincuenta mil dólares (\$150,000) por cada violación.

11 Para fines de este Artículo, los siguientes términos tienen el significado que a continuación se
12 expresa:

13 (a) “Deepfake” significa todo contenido audiovisual, de audio, de imagen o de texto generado
14 o manipulado mediante técnicas de inteligencia artificial con el propósito de hacer que
15 parezca auténtico o que represente a una persona real diciendo, haciendo o transmitiendo
16 algo que no ocurrió en la realidad.

17 (b) “Evidencia digital” significa toda información o dato almacenado o transmitido en
18 formato digital que tenga valor probatorio potencial en una investigación, procedimiento,
19 vista o asunto judicial, legislativo o administrativo. Incluye, sin limitarse a, archivos de
20 texto, audio, video e imagen; mensajes de texto, correos electrónicos y comunicaciones en
21 plataformas de mensajería; registros de transacciones; metadatos; registros de auditoría

(audit logs); datos de geolocalización; e información almacenada en dispositivos electrónicos, servidores remotos o plataformas de computación en la nube.

(c) “Inteligencia artificial generativa” significa cualquier sistema computacional basado en modelos de aprendizaje automático o profundo capaz de generar, sintetizar, alterar o reproducir contenido en formatos de texto, imagen, audio, video u otros medios, ya sea mediante tecnologías actualmente existentes o aquellas que se desarrollen en el futuro.

(d) “Metadatos” significa la información estructural asociada a un archivo o dato digital que describe sus características, incluyendo su fecha de creación, fecha de modificación, autor, dispositivo de origen, coordenadas de ubicación, y demás atributos técnicos vinculados al archivo o dato.

(e) “Orden de preservación de datos” significa toda orden emitida por autoridad competente, fiscal o judicial, que requiera a una persona natural o jurídica, incluyendo proveedores de servicios electrónicos, la conservación de evidencia digital específica en el estado en que se encuentre al momento de la orden, sin alteración ni eliminación, por el tiempo que dicha orden establezca.

Sección 2. — Vigencia

Esta Ley entrará en vigor inmediatamente después de su aprobación.