

GOBIERNO DE PUERTO RICO

20^{ma.} Asamblea
Legislativa

3^{ra.} Sesión
Ordinaria

SENADO DE PUERTO RICO

P. del S. 1099

19 de febrero de 2026

Presentado por el señor *Ríos Santiago*

Referido a

LEY

Para establecer la “Ley para la Conservación, Preservación y Manejo de Evidencia Digital en Investigaciones Criminales en Puerto Rico”; establecer obligaciones a proveedores de servicios de comunicaciones electrónicas y servicios remotos; disponer sobre la retención de datos, órdenes de preservación de evidencia digital, cadena de custodia digital y salvaguardas de confidencialidad, particularmente en casos que involucren menores de edad; y para otros fines relacionados.

EXPOSICIÓN DE MOTIVOS

La evolución tecnológica y la creciente digitalización de las comunicaciones han transformado de manera sustancial la dinámica social, económica y gubernamental en la era contemporánea. En este nuevo entorno, la evidencia de naturaleza digital se ha convertido en un componente esencial para la investigación, procesamiento y adjudicación de delitos. Sin embargo, la facilidad con que los datos electrónicos pueden ser alterados o eliminados, junto con la ausencia de un marco legal local uniforme, representa un desafío significativo para las autoridades encargadas de hacer cumplir la ley.

En Puerto Rico no existe, al presente, un estatuto integral que regule de forma coherente la conservación, preservación y manejo de evidencia digital en el contexto de investigaciones criminales. Esta laguna normativa genera incertidumbre jurídica,

dificulta la obtención y preservación adecuada de la prueba tecnológica y puede conllevar la pérdida irremediable de información esencial para el esclarecimiento de delitos. En particular, la falta de parámetros claros impacta adversamente aquellas investigaciones en las que se ven involucrados menores de edad, quienes constituyen una población especialmente vulnerable en el ámbito cibernético.

A nivel federal, el *Stored Communications Act* (18 U.S.C. §§ 2701-2713) establece un marco regulatorio sobre el acceso, divulgación y preservación de comunicaciones electrónicas y datos almacenados por proveedores de servicios. No obstante, la aplicación efectiva de dicho marco requiere legislación estatal complementaria que defina mecanismos procesales ágiles y establezca obligaciones razonables de cooperación para los proveedores de servicios de comunicaciones electrónicas y remotas, conforme a las particularidades jurídicas y operacionales de cada jurisdicción.

En el caso de Puerto Rico, resulta imperativo adoptar una política pública clara en relación con la conservación y manejo de evidencia digital. La ausencia de normas específicas sobre cadena de custodia digital, retención de datos, órdenes de preservación y confidencialidad en el manejo de información tecnológica compromete tanto la efectividad de las investigaciones como la protección de los derechos fundamentales de las personas involucradas. Un marco normativo debidamente estructurado permitirá equilibrar el interés del Estado en la persecución efectiva del delito con las garantías constitucionales contra registros, allanamientos y confiscaciones irrazonables.

Esta medida tiene como propósito establecer las bases jurídicas para la solicitud, conservación y manejo seguro de datos digitales vinculados a la comisión de delitos. A tales fines, se definen los deberes y responsabilidades de los proveedores de servicios de comunicaciones electrónicas y servicios remotos, se crean mecanismos uniformes de preservación y cadena de custodia digital, y se incorporan salvaguardas de confidencialidad orientadas a proteger especialmente la información relativa a menores de edad.

Las disposiciones aquí propuestas se desarrollan en armonía con el ordenamiento jurídico federal, incluyendo las normas interpretadas por el Tribunal Supremo de los

Estados Unidos en *Carpenter v. United States*, 138 S. Ct. 2206 (2018), y con los estándares de debido proceso reconocidos en el derecho comparado. De esta manera, se dota al Gobierno de Puerto Rico de un instrumento legislativo moderno, coherente y compatible con las exigencias tecnológicas contemporáneas, que fortalece las capacidades investigativas del Estado y salvaguarda los valores fundamentales de la justicia y la protección de la dignidad humana.

Por tanto, esta Asamblea Legislativa considera necesario establecer como política pública del Gobierno de Puerto Rico el fortalecimiento de un sistema de investigación criminal que incorpore de manera eficaz la evidencia digital, asegurando su integridad, autenticidad y admisibilidad, sin menoscabo de los derechos constitucionales de las partes, a fin de garantizar la corrección de los procesos penales y mantener la confianza de la ciudadanía en la administración de justicia en el entorno digital.

DECRÉTASE POR LA ASAMBLEA LEGISLATIVA DE PUERTO RICO:

1 Artículo 1.- Título.

2 Esta Ley se conocerá como la “Ley para la Conservación, Preservación y Manejo
3 de Evidencia Digital en Investigaciones Criminales en Puerto Rico”.

4 Artículo 2.- Política Pública.

5 Será política pública del Gobierno de Puerto Rico establecer un marco normativo
6 claro, uniforme y efectivo para la conservación, preservación, manejo y utilización de
7 evidencia digital en investigaciones criminales, particularmente aquellas que involucren
8 menores de edad, garantizando la integridad de la evidencia, la efectividad investigativa
9 del Estado y la protección de los derechos fundamentales.

10 Esta política pública se implementará en armonía con el derecho federal aplicable,
11 incluyendo el *Stored Communications Act* (18 U.S.C §§ 2701-2713), y con las Reglas de
12 Evidencia y de Procedimiento Criminal en Puerto Rico. Asimismo, será política pública

del Gobierno de Puerto Rico garantizar que toda medida de conservación y preservación de datos digitales se realice de manera razonable, proporcional y vinculada a fines legítimos de investigación criminal, evitando cargas indebidas a los proveedores de servicio y protegiendo los derechos constitucionales a la intimidad y a la protección contra registros y allanamientos irrazonables.

Nada de lo dispuesto en esta Ley se interpretará como una autorización para requerir la divulgación de contenido de comunicaciones electrónicas sin el cumplimiento de los requisitos establecidos en derecho federal aplicable, incluyendo el *Stored Communications Act* (18 U.S.C §§ 2701-2713).

Artículo 3.- Definiciones.

Para propósitos de esta ley, los siguientes términos o frases tendrán los significados que a continuación se expresan:

(a) “Proveedor de Servicio” significa toda persona natural o jurídica que, de manera intencional u organizada, ofrezca servicios de transmisión de comunicaciones electrónicas o acceso a internet a usuarios asentados en Puerto Rico, independientemente de su ubicación física o del lugar donde se encuentren sus servidores.

(b) “Proveedor de Hospedaje o Servicio Remoto” significa toda entidad que provea almacenamiento, procesamiento o manejo de datos digitales en nombre de usuarios.

(c) “Datos de Tráfico o Metadatos” significa información generada por sistemas electrónicos asociada a una comunicación que describe su origen, destino, ruta, fecha, hora, duración o tipo de servicio, sin incluir el contenido de la comunicación.

(d) “Evidencia Digital” significa cualquier información almacenada o transmitida en formato electrónico que pueda ser utilizada como prueba en un procedimiento judicial.

(e) “Preservación de Datos” significa la acción de mantener y proteger datos existentes contra su modificación o eliminación por un término determinado.

(f) “Orden de Preservación” significa mandato emitido por autoridad competente requiriendo la conservación de datos específicos.

(g) “Cadena de Custodia Digital” significa conjunto de procedimientos que garantizan la integridad, autenticidad y trazabilidad de la evidencia digital.

Artículo 4.- Obligación de Preservar Datos.

Todo proveedor de servicio o proveedor de hospedaje que opere o preste servicios en Puerto Rico vendrá obligado a conservar los datos de tráfico y registros de comunicaciones electrónicas por un período mínimo de doce (12) meses y no mayor de veinticuatro (24) meses, conforme se disponga mediante reglamentación.

Dicha obligación se limitará a los datos de tráfico o metadatos y no incluirá el contenido de las comunicaciones, salvo disposición expresa de ley o mandato judicial conforme a derecho.

Las disposiciones de este Artículo se interpretarán en armonía con el *Stored Communications Act* (18 U.S.C §§ 2701-2713). La obligación aquí dispuesta se limitará a

1 datos razonables necesarios para fines de investigación criminal y no podrá interpretarse
2 como una autorización para la recopilación masiva o indiscriminada de información. Su
3 implementación deberá cumplir con los principios de razonabilidad y proporcionalidad
4 conforme a la Constitución de Puerto Rico y la Constitución de los Estados Unidos.

5 Nada de lo aquí dispuesto se interpretará como una obligación incompatible con
6 las limitaciones establecidas en el *Stored Communications Act* (18 U.S.C §§ 2701-2713) ni
7 como autorización para la retención o divulgación de contenido de comunicaciones
8 electrónicas sin orden judicial válida conforme a derecho.

9 La conservación de datos conforme a este Artículo no constituirá por sí sola base
10 para la admisibilidad de evidencia, la cual estará sujeta a los procedimientos de
11 impugnación, incluyendo mociones de supresión de evidencia, conforme a las Reglas de
12 Procedimiento Criminal.

13 Artículo 5.- Órdenes de Preservación de Evidencia Digital.

14 El Tribunal de Primera Instancia podrá emitir órdenes de preservación de evidencia
15 digital a solicitud del Ministerio Público o de un agente del orden público autorizado,
16 previa determinación de causa probable o, en los casos previstos por ley, de motivo
17 fundado conforme a derecho.

18 Asimismo, el Ministerio Público podrá emitir solicitudes de preservación de carácter
19 expedito cuando existan circunstancias urgentes que justifiquen la conservación
20 inmediata de datos, basadas en motivo fundado. Dichas solicitudes no constituirán en sí
21 mismas autorización para acceder o divulgar información y tendrán una vigencia inicial
22 de noventa (90) días, debiendo ser presentadas ante el Tribunal para su validación dentro

1 de un término de setenta y dos (72) horas. La falta de validación judicial dentro de dicho
2 término conllevará la nulidad de la solicitud.

3 Las órdenes o solicitudes deberán especificar:

4 (a) Identificación del proveedor;

5 (b) Tipo de datos a preservarse;

6 (c) Periodo de tiempo aplicable;

7 (d) Fundamento de la solicitud;

8 (e) Base fáctica que sustente la pertinencia de los datos solicitados.

9 Lo anterior se entenderá sin perjuicio de los requisitos de orden judicial, citación o
10 autorización previa exigidos por el derecho federal aplicable para el acceso o divulgación
11 de datos.

12 Nada de lo dispuesto en este Artículo se interpretará como un sustituto de los
13 requisitos para la expedición de órdenes de allanamiento o registro conforme a las Reglas
14 de Procedimiento Criminal de Puerto Rico.

15 Artículo 6.- Salvaguardas de Confidencialidad.

16 En toda investigación que involucre menores de edad:

17 (a) Se garantizará la confidencialidad de la información recopilada;

18 (b) Se limitará el acceso a la evidencia digital a personal autorizado, sin menoscabar
19 el derecho del acusado a obtener y examinar la evidencia conforme a las Reglas de
20 Procedimiento Criminal;

21 (c) Se prohibirá la divulgación innecesaria de información identificable;

(d) Se adoptarán medidas para proteger la dignidad y privacidad de las víctimas, incluyendo las disposiciones aplicables sobre privilegios y protección de víctimas conforme a las Reglas de Evidencia de Puerto Rico.

Artículo 7.- Cadena de Custodia Digital.

La evidencia digital deberá ser recolectada, preservada, analizada y presentada mediante procedimientos que garanticen su integridad, autenticidad y trazabilidad.

A tales efectos, deberán adoptarse, como mínimo, los siguientes mecanismos:

(a) La creación de copias forenses de los dispositivos o datos originales;

(b) La utilización de funciones de verificación digital, incluyendo algoritmos de hash, para validar la integridad de la evidencia;

(c) El mantenimiento de registros detallados de acceso, transferencia, análisis y almacenamiento de la evidencia digital;

(d) La identificación de toda persona que haya tenido acceso a la evidencia;

(e) La documentación continua de la cadena de custodia desde su obtención hasta su presentación en el Tribunal.

El incumplimiento sustancial de estos procedimientos podrá afectar el peso o la admisibilidad de la evidencia conforme a las Reglas de Evidencia de Puerto Rico, incluyendo las disposiciones sobre autenticación e identificación de evidencia.

La admisibilidad de la evidencia digital se regirá además por disposiciones aplicables sobre prueba de referencia, autenticación, duplicados y evidencia electrónica contenidas en las Reglas de Evidencia.

Los procedimientos aquí establecidos estarán sujetos a los mecanismos de descubrimiento de prueba y a la impugnación por las partes conforme a las Reglas de Procedimiento Criminal de Puerto Rico.

Artículo 8.- Protección de la Identidad y Privacidad de Menores de Edad.

El Gobierno de Puerto Rico garantizará la protección de la identidad y privacidad de los menores de edad en todas las etapas del proceso investigativo y judicial, adoptando medidas razonables para evitar la divulgación innecesaria de información que permita su identificación, en armonía con las Reglas de Evidencia de Puerto Rico y demás legislación aplicable.

Artículo 9.- Inmunidad.

Ningún proveedor de servicios de comunicaciones electrónicas o servicios remotos incurrirá en responsabilidad civil o penal por cumplir de buena fe con una orden judicial o solicitud de preservación emitida conforme a esta Ley.

Esta disposición no aplicará en caso de negligencia crasa o conducta intencional indebida.

Para efectos de este Artículo, se entenderá que existe buena fe cuando el proveedor actúa en cumplimiento razonable de una orden judicial o solicitud válida conforme a esta Ley. Esta inmunidad no limitará la facultad del Tribunal para evaluar la legalidad de la obtención de la evidencia ni su admisibilidad conforme a las Reglas de Procedimiento Criminal.

Artículo 10.- Reglamentación.

El Departamento de Justicia, en coordinación con el Negociado de la Policía de Puerto Rico y otras agencias pertinentes, adoptará la reglamentación necesaria para la implementación de esta Ley dentro de un término de ciento ochenta (180) días.

Dicha reglamentación incluirá, entre otros aspectos, la adopción de protocolos técnicos para la recolección, preservación, análisis y manejo de evidencia digital, en coordinación con el *Puerto Rico Innovation and Technology Service* (PRITS) y las agencias de orden público competentes, incluyendo estándares sobre formatos de hash, copias forenses, registros de auditoría y medidas de seguridad informática, consistentes con las mejores prácticas forenses aceptadas y con el ordenamiento jurídico aplicable.

Asimismo, la reglamentación dispondrá los mecanismos de coordinación operativa con las autoridades federales, incluyendo el Buró Federal de Investigaciones (FBI, por sus siglas en inglés), *Homeland Security Investigations* (HSI) y otras entidades competentes, de forma tal que la ejecución de esta Ley se lleve a cabo en armonía con la legislación federal vigente, incluyendo el *Stored Communications Act* (18 U.S.C. §§ 2701–2713), y demás normas aplicables, sin que ello implique limitación alguna a las facultades de dichas autoridades federales ni al uso de órdenes, citaciones u otros mecanismos procesales emitidos al amparo del derecho federal.

Artículo 11.- Limitación de Alcance.

Nada de lo dispuesto en esta Ley se interpretará como autorización para la recopilación masiva o indiscriminada de datos, debiendo toda actuación limitarse a lo estrictamente necesario para fines legítimos de investigación criminal, conforme a los

1 principios de razonabilidad y proporcionalidad. Asimismo, nada de lo anterior se
2 interpretará como una limitación a los derechos del acusado reconocidos en las Reglas de
3 Procedimiento Criminal de Puerto Rico.

4 Artículo 12.- Armonización con otras Leyes Aplicables.

5 Nada de lo dispuesto en esta Ley se interpretará en menoscabo de las obligaciones
6 y protecciones establecidas en la Ley 111-2005, según enmendada, conocida como “Ley
7 de Información al Ciudadano sobre la Seguridad de Bancos de Información”, relativas
8 a la protección de datos personales y la notificación de brechas de seguridad de
9 información. De igual modo, las disposiciones de esta Ley se aplicarán en armonía con
10 la Ley 148-2006, según enmendada, conocida como “Ley de Transacciones
11 Electrónicas”, en lo concerniente a la conservación, validez y eficacia probatoria de
12 documentos y registros electrónicos.

13 Artículo 13.- Separabilidad.

14 Si cualquier cláusula, párrafo, subpárrafo, oración, palabra, letra, artículo,
15 disposición, sección, subsección, título, capítulo, subcapítulo, acápite o parte de esta ley
16 fuera anulada o declara inconstitucional, la resolución, el dictamen o la sentencia dictada
17 a tal efecto no afectará, perjudicará, ni invalidará el remanente de esta ley. El efecto de tal
18 sentencia quedará limitado a la cláusula, párrafo, subpárrafo, oración, palabra, letra,
19 artículo, disposición, sección, subsección, título, capítulo, subcapítulo, acápite o parte de
20 ésta que así hubiera sido anulada o declarada inconstitucional.

21 Artículo 14.- Vigencia.

22 Esta ley entrará en vigor inmediatamente después de su aprobación.