PROYECTO DE LEY

El Senado y la Cámara de Diputados sancionan con fuerza de ley…

Ley de Acceso y Preservación de Evidencia Digital en el Proceso Penal

Capítulo I- Disposiciones generales.

Artículo 1°. Objeto. Es objeto de la presente ley, el establecer reglas para la preservación de evidencia digital, la entrega de dispositivos y soportes, así como la asistencia para su acceso y sancionar su incumplimiento.

Artículo 2°. Definiciones. A los efectos de esta ley, se entiende por:

a) Dispositivo digital: Todo artefacto electrónico o medio virtual que permita el almacenamiento de datos o información.

b) Credenciales de acceso: Conjunto de indicadores únicos que permiten probar la identidad de una persona a los fines de acceder a un dispositivo digital.

c) Datos: contenido de la información y elementos alojados en los dispositivos digitales.

d) Medio de cifrado: procesos informáticos empleados para impedir la lectura o el acceso a la información contenida en un dispositivo digital.

Capítulo II - Preservación

Artículo 3°. Orden de Preservación Inmediata. El juez competente podrá ordenar por resolución debidamente fundada, sin sustanciación alguna, la preservación por hasta noventa (90) días de datos específicos en poder de personas humanas o

jurídicas, prohibiendo su supresión o alteración. Dicha orden podrá prorrogarse existiendo causas debidamente fundamentadas.

Artículo 4°. Deber de custodia. La persona que reciba la Orden de Preservación deberá generar registros de integridad de accesos a los fines de garantizar la integridad de la información.

Artículo 5°. Conservación de cadena de custodia. Igualmente, los organismos intervinientes en la ejecución de la Orden de Preservación documentarán toda acción sobre la información preservada, bajo estrictos estándares, garantizando así la inalterabilidad de la cadena de custodia.

Capítulo III - Entrega y acceso a dispositivos

Artículo 6°. Orden de Entrega o Acceso a Dispositivos. El juez competente podrá ordenar, por resolución debidamente fundada, la entrega inmediata de dispositivos digitales o la información para el acceso a los mismos.

Artículo 7°. Orden de Asistencia para Acceso a Datos. El juez competente podrá ordenar, por resolución debidamente fundada, que terceros con conocimiento técnico brinden información o asistencia razonable y necesaria para acceder a datos específicos alojados en dispositivos digitales.

El incumplimiento será pasible de la sanción prevista en el artículo 17 de la presente.

Artículo 8°. Asistencia del investigado o imputado. No podrá compelerse al investigado o imputado a revelar credenciales memorizadas cuando ello importare la violación del principio de no autoincriminación y/o el de inocencia.

Artículo 9°. Exigencia de datos biométricos. El juez competente podrá ordenar, por resolución debidamente fundada y bajo criterios de necesidad y proporcionalidad, la utilización de datos biométricos del investigado o imputado (huellas digitales, rasgos faciales u otros parámetros físicos) a los fines exclusivos de desbloquear el acceso a un dispositivo digital.

La medida deberá ejecutarse en condiciones que respeten la dignidad de la persona y con constancia escrita, videográfica y bajo control de la defensa técnica.

Queda prohibida, bajo pena de nulidad, la compulsión a revelar contraseñas, patrones, códigos memorizados u otros datos cuyo suministro importe autoincriminación de carácter intelectual.

Artículo 10.- Alcance de las Ordenes. Las órdenes establecidas en los artículos 6° y 7° de la presente, deberán:

a) limitar dispositivos, cuentas, intervalos temporales y tipos de datos;

b) requerir bitácora de acceso, filtros y exportación segregada;

c) Establecer con precisión la información que pretende recabarse.

Artículo 11. Medidas cautelares para impedir borrados. El juez competente podrá ordenar, mediante resolución fundada, disponer en modo cautelar el aislamiento de redes, bloqueo de sincronizaciones, clonado forense inmediato, así como cualquier medida tendiente a preservar la información debiendo, en todo caso observarse las previsiones de los artículos 4° y 5°

Artículo 12. Garantías de registro. Toda ejecución de orden deberá quedar debidamente registrada y resultar auditable, indicando hashes, logs, software usado y peritos intervinientes. Asimismo, deberá notificarse al afectado, salvo reserva fundada.

Artículo 13. Información privilegiada. No podrá accederse por el procedimiento establecido en la presente a datos relacionados con comunicaciones o documentos que se encuentren amparados por el secreto profesional, salvo renuncia expresa del titular de dicho privilegio.

Artículo 14.- Remedios. Cualquier persona que fuera pasiva de alguno de los procedimientos establecidos en la presente podrá promover incidente de nulidad o exclusión probatoria por inobservancia de garantías constitucionales ante el mismo juez que intervino, quien deberá resolver la petición en el plazo máximo de cuarenta y ocho (48) horas.

Capítulo IV — Ilícitos y sanciones

Artículo 15. Alteración dolosa de evidencia digital. Será reprimido con prisión de seis (6) meses a cuatro (4) años quien, con intención, destruya, borre, altere u oculte datos relevantes para una investigación penal o proceso en curso con el fin de impedir u obstaculizar su descubrimiento.

Las penas previstas en este artículo serán de dos (2) a seis (6) años, si media Orden de Entrega o Acceso a Dispositivos notificada, si el autor es funcionario público, o si se trata de delitos contra la integridad sexual de niños/niñas.

Artículo 16. Incumplimiento de Orden de Entrega o Acceso a Dispositivos. El incumplimiento injustificado de una Orden de Entrega o Acceso a Dispositivos será penado con prisión de tres (3) meses a un (1) año o multa.

En caso que el incumplimiento provenga de un proveedor de servicios, además, se impondrá multa de entre cien (100) y mil (1000) Salarios Mínimos Vitales y Móviles y en casos graves o ante incumplimientos reiterados, condena accesoria de inhabilitación para continuar funcionando.

Artículo 17. Incumplimiento de Orden de Asistencia para Acceso a Datos por terceros. El incumplimiento injustificado de una Orden de Asistencia para Acceso a Datos será penado con prisión de seis (6) meses a dos (2) años y multa de entre cincuenta (50) y quinientos (500) Salarios Mínimos Vitales y Móviles.

Las penas previstas en este artículo serán de uno (1) a cuatro (4) años y la multa de cien (100) a mil (1000) Salarios Mínimos Vitales y Móviles, si el caso versare sobre seguridad nacional, crimen organizado o delitos contra la integridad sexual de niños y niñas.

No constituirá delito cuando la falta de cumplimiento obedeciera a limitaciones o imposibilidades técnicas acreditadas en el descifrado u obtención de la información.

Capítulo V- Reglamentación y Disposiciones Finales

Artículo 18. Autoridad de aplicación y protocolos. El Poder Ejecutivo designará la autoridad administrativa de aplicación de la presente.

El Ministerio Público Fiscal y el Máximo organismo Judicial de cada jurisdicción deberán aprobar protocolos técnicos y publicar estadísticas anuales de los procedimientos.

Artículo 19. Invítase a las Provincias y a la Ciudad Autónoma de Buenos Aires, a adherir a la presente ley.

Artículo 20. La presente Ley entrará en vigencia a los noventa (90) días de su promulgación.

Artículo 21. Comuníquese al Poder Ejecutivo.

OSCAR AGOST CARREÑO

Diputado Nacional

FUNDAMENTOS

Señor Presidente:

La evidencia digital se ha transformado en uno de los insumos probatorios más relevantes en el proceso penal contemporáneo. Su carácter efímero, fácilmente manipulable y replicable, exige una regulación específica que garantice su preservación, acceso controlado y resguardo de garantías constitucionales.

La presente iniciativa procura llenar un vacío normativo que hoy deja libradas a interpretaciones dispares cuestiones tan delicadas como la conservación de datos, la entrega de dispositivos o la asistencia técnica para el acceso a la información. Se trata, en definitiva, de asegurar que la investigación penal disponga de herramientas idóneas sin menoscabar derechos fundamentales.

El articulado se encuentra diseñado bajo estricta observancia de la Constitución Nacional y de la Convención Americana sobre Derechos Humanos, en especial en lo atinente a los principios de legalidad, necesidad y proporcionalidad.

A su vez, en relación a otras garantías, destacamos lo siguiente:

Derecho a la intimidad y privacidad: toda medida requiere orden judicial debidamente fundada, con delimitación de dispositivos, intervalos temporales y categorías de datos.

Garantía contra la autoincriminación: se excluye expresamente la obligación del imputado de revelar credenciales memorizadas.

Debido proceso y defensa en juicio: se habilita la promoción de incidentes de nulidad o exclusión probatoria por inobservancia de garantías, asegurando tutela judicial efectiva.

Protección de privilegios profesionales: se establece la intangibilidad de comunicaciones y/o documentos amparados por secreto profesional, garantizando el libre ejercicio de la defensa técnica y la libertad de prensa.

En cuanto a diversos antecedentes jurisprudenciales relevantes, destacamos que la Corte Suprema de Justicia de la Nación ha sentado en "Halabi" la exigencia de control judicial estricto frente a medidas que puedan afectar la intimidad. El proyecto replica este estándar al requerir resoluciones fundadas y limitadas en su alcance.

A su vez, la Corte Suprema de Estados Unidos fijó precedentes de referencia en Riley v. California y Carpenter v. United States, donde se exige orden judicial previa y criterios de minimización en el acceso a dispositivos y datos sensibles. Estas pautas han sido recogidas expresamente.

En torno al derecho comparado, el cual ha sido especialmente considerado, dejamos de relieve que el Convenio de Budapest sobre Ciberdelincuencia recomienda la preservación expedita de datos y la asistencia obligatoria de quienes posean conocimiento técnico de los sistemas. La propuesta se alinea con tales estándares, promoviendo cooperación judicial efectiva y resguardando la validez probatoria.

En el derecho comparado, países como Reino Unido, Francia, Australia y Nueva Zelanda contemplan sanciones para quienes se rehúsan a descifrar, entregar claves o brindar asistencia. El presente proyecto incorpora esas figuras, pero con garantías específicas acordes a nuestro sistema constitucional.

En cuanto a los aspectos salientes del proyecto, destacamos los siguientes:

Orden y alcance: delimitación precisa de dispositivos, cuentas, períodos de tiempo y categorías de datos.

Minimización: filtrado por palabras, fechas o revisión escalonada, evitando intromisiones excesivas.

Cadena de custodia digital: registro de integridad, logs y hashes, asegurando la trazabilidad y auditabilidad de la prueba.

Consentimiento informado en biometría: solo bajo resolución judicial fundada y con constancia escrita y fílmica, y debido patrocinio letrado, en resguardo del imputado.

En orden a las sanciones propuestas, la tipificación penal de la alteración dolosa de evidencia digital y el incumplimiento de órdenes judiciales responde a la necesidad de evitar la impunidad derivada de la destrucción o reticencia en la entrega de pruebas.

Las escalas penales y agravantes se encuentran diseñadas bajo un criterio de proporcionalidad y lesividad, reservándose los mayores márgenes punitivos para casos de especial gravedad, como delitos contra la integridad sexual de niños y niñas, seguridad nacional o incumplimientos por funcionarios públicos.

La iniciativa conjuga la necesidad de dotar al proceso penal de herramientas modernas y eficaces con el mandato de proteger los derechos y garantías constitucionales de las personas. El proyecto, inspirado en el derecho comparado y en compromisos internacionales, pretende lograr un equilibrio entre eficacia investigativa y tutela de derechos fundamentales, anticipándose así a cuestionamientos de inconstitucionalidad.

Por todo lo expuesto, solicito a mis pares el acompañamiento al presente proyecto.

OSCAR AGOST CARREÑO

Diputado Nacional