

8 de septiembre de 2026

Hon. Ángel Toledo López
Presidente
Comisión de lo Jurídico
Senado de Puerto Rico
atoledo@senado.pr.gov

Honorable Presidente:



PO Box 192333
San Juan, Puerto Rico 00919
787-753-8493
acluofpr@aclu.org

La Unión Americana de Libertades Civiles (ACLU, por sus siglas en inglés) defiende los derechos fundamentales descritos en la Constitución de los Estados Unidos y la Declaración de Derechos. Estos derechos incluyen el derecho a la libertad de expresión, el derecho a la privacidad, y el debido proceso legal. La ACLU también fundamenta su posición en las disposiciones constitucionales estatales y las leyes federales y estatales que fomentan estos derechos y otros derechos similares como el derecho a la protección frente a la sobrecriminalización.

En atención a lo anterior, la ACLU de Puerto Rico interesa exponer su posición en torno al Proyecto del Senado 974 presentado por el Hon. Carmelo Ríos Santiago para añadir un nuevo Título VI – Delitos Cibernéticos; reenumerar el actual Título VI como Título VII; reenumerar los actuales Artículos 301, 302, 303, 304, 305, 306, 307, 308, y 309, para ser reenumerados como los Artículos 377, 378, 379, 380, 381, 382, 383, 384 y 385, de la Ley Núm. 146-2012, según enmendada, conocida como el “Código Penal de Puerto Rico”, a los fines de tipificar delitos cibernéticos y otros conexos de los mismos; entre otros fines.

El Senado tiene ante su consideración un proyecto de ley dirigido a codificar conductas ilícitas en el mundo cibernético. Su objetivo es incorporar al Código Penal una sección que tipifique como delito cualquier tipo de conducta ilegal o delictiva en que se haya utilizado un equipo, una Red o un dispositivo de hardware.¹ A esos efectos, el P del S 974 busca tipificar como delito cibernético conductas como el acoso cibernético, fraude, crimen pornográfico, “sexting”, “grooming” entre otros, con miras a proteger a la

¹ Véase, Exposición de Motivos del PS974.



ciudadanía de determinadas acciones ilícitas. Sin embargo, su alcance podría tener implicaciones legales de gran trascendencia respecto a los derechos constitucionales de las personas en Puerto Rico como expondremos a continuación. Aunque el proyecto busca brindar mayor protección frente a conductas ilícitas mediante el uso de artefactos cibernéticos, surgen interrogantes puntuales sobre su alcance e interpretación, particularmente porque algunas de sus disposiciones podrían entrar en conflicto con derechos fundamentales como lo es la Primera y Cuarta Enmienda de la Constitución de los Estados Unidos, cuyos derechos también surgen plasmados en la Constitución de Puerto Rico, y el principio de legalidad.

Como es sabido, la Primera Enmienda de la Constitución de los Estados Unidos garantiza la libertad de expresión frente a las actuaciones del Estado. Asimismo, dicha disposición protege la libertad de prensa, un derecho medular en cualquier gobierno democrático. Por su lado, la Cuarta Enmienda de la Constitución de los Estados Unidos garantiza la protección de individuos contra registros irrazonables, lo cual incluye el derecho de la privacidad. Estas protecciones también son garantizadas por la Constitución de Puerto Rico, junto con diversas leyes federales y estatales que abordan derechos tan importantes. Por tanto, la privacidad no solo es un asunto de política pública, sino un derecho fundamental en los Estados Unidos y Puerto Rico. Es decir, en ambas jurisdicciones se reconoce el derecho a ser libre ante la intromisión indebida del gobierno. Inclusive, a diferencia de la Constitución de los Estados Unidos que adopta el derecho de privacidad jurisprudencialmente por interpretación, la Constitución de Puerto Rico lo reconoce expresamente.

Por otro lado, el principio de legalidad es medular en nuestro Estado de Derecho. El Código Penal de Puerto Rico establece “No se instará acción penal contra persona alguna por un hecho que no esté expresamente definido como delito en este Código o mediante ley especial [...]” 33 LPRA § 5002. El principio de legalidad exige que los delitos estén tipificados de forma clara y libre de toda vaguedad. *Pueblo v. García Colón*, 183 DPR 129 (2011).

Por consiguiente, al tratarse de un proyecto que busca criminalizar ciertas conductas mediante el uso de artefactos cibernéticos, no



solo se levantan preocupaciones de índole constitucional, sino, es menester evaluar la claridad y especificidad de los artículos propuestos, ya que, de carecer de claridad, ser confuso para la ciudadanía, ser sobreabarcador o incluir penas excesivas, pudiese atentar con el principio de legalidad consagrado en el Artículo 2 del Código Penal de Puerto Rico.

La ACLU ha sido líder nacional en la lucha por salvaguardar los derechos constitucionales. Edificada sobre la base de un trabajo de casi un siglo, la ACLU emplea una estrategia integrada de litigios, educación pública y defensa, para proteger la privacidad y luchar en contra penas desproporcionadas. Esto pues, es parte primordial de la misión de la ACLU, su trabajo para preservar los derechos fundamentales cobijados por la Primera y Cuarta Enmienda, tanto como leyes federales y estatales.

Sin duda, adoptar medidas para hacer frente al aumento de los delitos cibernéticos constituye una necesidad imperante para proteger a las personas en una sociedad cada vez más dependiente de la tecnología. Ahora bien, la complejidad surge cuando, en el quehacer de proteger a la ciudadanía contra cierta conducta ilícita mediante el uso de artefactos tecnológicos, se sobrepasan las garantías constitucionales y las leyes especiales que protegen a las personas frente al Estado. En esa intersección, es fundamental establecer un balance de intereses entre proteger a la ciudadanía sobre crímenes cibernéticos y a su vez, salvaguardar igualmente la privacidad y el principio de legalidad. Nuestra Asamblea Legislativa tiene el deber de legislar para hacer cumplir los derechos constitucionales, y evitar crear disposiciones vagas que reconozcan nuevos derechos o amplíen excesivamente el alcance y contenido de los ya existentes, particularmente cuando ello pueda tener consecuencias jurídicas de alcance peligroso.

En el 1986, el Congreso de los Estados Unidos aprobó el *Consumer Fraud and Abuse Act* (“CFAA”) como medida de seguridad para crímenes cibernéticos debido a las preocupaciones crecientes que habían surgido sobre como atender delitos informáticos. El CFAA creó un marco federal para criminalizar el acceso no autorizado a computadoras, adaptándose a la rápida evolución de la tecnología y amenazas cibernéticas. En *Van Buren v. United States*, 593 U.S. 374 (2021), el Tribunal Supremo federal al interpretar dicha ley, concluyó que un individuo excede su autoridad únicamente



cuando accede a información que no está autorizada a obtener, **y no cuando hace un uso indebido del acceso para fines no autorizados**. En *Carpenter v. United States*, 585 U.S. 296 (2018), el Tribunal Supremo federal explicó que medidas de protección cibernéticas tienen que cumplir con la Cuarta Enmienda de la Constitución y enfatizó que la Cuarta Enmienda no solo protege un interés propietario sino también en aquellos casos que exista una expectativa razonable de privacidad.

La preocupación del choque entre el objetivo de seguridad sin trastocar derechos constitucionales y leyes federales y estatales continúa siendo un tema de alto interés para los tribunales. Recientemente, en *Chatrie v. United States*, 609 U.S. __ (2026), el Máximo Foro federal sostuvo que obtener los datos históricos de ubicación de Google de una persona mediante una orden judicial de geovalla (*geofence warrant*) constituye un registro en virtud de la Cuarta Enmienda, porque las personas tienen una expectativa razonable de privacidad respecto a dichos datos. En este sentido, cabe señalar que la judicatura federal ha demostrado cautela al adjudicar controversias relacionadas con el uso de artefactos tecnológicos y, a su vez, al realizar el balance de interés correspondiente. Ello responde a que estos asuntos requieren un análisis detenido, debido a las implicaciones trascendentales que pueden tener sobre los derechos fundamentales de la ciudadanía.

Establecido este marco general, procede entonces evaluar el proyecto presentado. El Proyecto del Senado 974 desequilibra el referido balance, pues utiliza un lenguaje confuso e intenta tipificar conductas delictivas de manera excesivamente abarcadoras, mediante disposiciones vagas y penas desproporcionadas. Por ejemplo, el P del S 974 establece en su Artículo 303:

Toda persona que, sin autorización o **excediendo una autorización**, destruya o **inutilice** en todo o en parte un sistema informático o sistema telemático o de telecomunicaciones o a sus componentes, impida, **altere**, entorpezca, **obstaculice** o **modifique** su funcionamiento o uso regular de acceso, **protegido o no con una medida de seguridad**, será sancionada con pena de reclusión por un término de **tres (3) años**. (Énfasis suplido).



Como está redactado, este artículo podría prestarse a penalizar de forma desproporcionada a una persona que—por ejemplo—, por iniciativa propia procure mejorar el funcionamiento de un sistema o modificarlo, ya que accede al mismo en el curso ordinario de sus actividades, aun cuando no exista una medida de seguridad que pretenda eludir ni ánimos de cometer un delito. También, surgen interrogantes de qué consiste “una medida de seguridad” y a qué se refiere con “excediendo una autorización”. No nos parece que disposiciones de esta naturaleza sean sabias, ni medidas efectivas de seguridad alineadas a garantizar la protección de los derechos constitucionales. El referido artículo, cuyo lenguaje similar se reproduce en disposiciones subsiguientes del proyecto, tiene un alcance excesivo que va más allá de penalizar conductas ilícitas. Por el contrario, podría crear un ambiente de miedo e incertidumbre y terminar criminalizando conductas realizadas de buena fe.

Igualmente, el proyecto criminaliza conductas que puedan surgir por error, equivocación o mal uso, aun cuando no medien propósitos o motivaciones ilícitas. De esta manera, establece penas que resultan desproporcionadas en relación con las conductas que pretende sancionar. Específicamente, en su Artículo 325. – Intercambio, Comercialización o Compra de Información de Equipos o Terminales Móviles, establece que: “Toda persona que, **intercambie**, comercialice, o **adquiera** bases de datos que contengan información de identificación de equipos terminales móviles, será sancionada con pena de reclusión por un término fijo de tres **(3) años**”. (Énfasis suplido).

La amplitud de esta disposición resulta preocupante, pues no establece con claridad bajo qué circunstancias la conducta descrita constituiría un delito. En particular, cabe preguntarse si la mera adquisición de cualquier base de datos que contenga información de identificación de equipos terminales móviles estaría prohibida y sujeta a una pena de tres (3) años de reclusión, independientemente del propósito, contexto o conocimiento de la persona. El artículo tampoco contempla circunstancias en las que la conducta pueda ocurrir de manera legítima, por error o de buena fe. Véanse, entre otras disposiciones que nos levantan similar

preocupación: los Artículos 302, 305, 307, 308, 310, 315, 316, 318, 321, 323, 326, 342, 343(a), 345, 350, 368, 371.²



² Artículo 302.- Acceso Indebido a Sistema Informático:

El que, sin autorización o excediendo una autorización en todo o en parte utilice, instale o acceda a un sistema informático o sistema telemático o de telecomunicaciones, o a sus componentes, protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a exigirlo, incurrirá en delito menos grave.

Artículo 305. – Ataque a la Integridad de Sistemas Informáticos del Sistema Público:

Toda persona que, sin autorización o excediendo una autorización, destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónicos, a sistemas del servicio público del Gobierno de Puerto Rico, cuyo contenido sea esencial para su funcionamiento o desarrollo de programas, de tratamiento de información, telemático o de telecomunicaciones a todo o en parte de sus componentes, protegido o no con una medida de seguridad, será sancionada con pena de reclusión por un término fijo de ocho (8) años.

Artículo 307. – Explotación Informática:

Será sancionada con pena de reclusión por término fijo de ocho (8) años toda persona que, sin autorización o excediendo una autorización en todo o en parte, utilice, instale o acceda a un sistema informático, telemático o de telecomunicaciones, esté o no protegido con medidas de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien ostente el legítimo derecho a exigirlo, con el propósito de explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar el tráfico de datos o voz, u ofrecer a terceros los servicios que estos sistemas proveen, sin que medie pago a los proveedores legítimos de tales servicios.

Artículo 308. – Daño Informático:

Toda persona que, sin autorización o excediendo una autorización a propósito, con conocimiento o temerariamente, destruya, dañe o vandalice en todo o en parte los datos contenidos en un sistema de información, telemático o de telecomunicaciones o de sus componentes, protegido o no con una medida de seguridad, o en perjuicio de un tercero, suprima, modifique o destruya la información contenida, será sancionada con pena de reclusión por un término fijo de cinco (5) años.

Artículo 310. – Revelación De Secretos:

Toda persona que, sin autorización o excediendo una autorización a propósito, con conocimiento o temerariamente modifique, destruya, obtenga, copie o utilice información de seguridad pública en todo o en parte de los datos contenidos en un sistema de información, telemático o de telecomunicaciones o

de sus componentes, protegido o no con una medida de seguridad, será sancionada con pena de reclusión por un término fijo de cinco (5) años.

Artículo 315. –Dispositivos Fraudulentos:

Será sancionada con pena de reclusión por término fijo de ocho (8) años toda persona que, sin autoridad o causa legítima, produzca, use, posea, trafique o distribuya programas informáticos, equipos, materiales o dispositivos cuyo uso exclusivo o fundamental sea emplearse como herramienta para la comisión de crímenes y delitos de alta tecnología.

Artículo 316. – Suplantación de Páginas Electrónicas:

Será sancionada con pena de reclusión por un término fijo de tres (3) años toda persona que, sin estar facultada para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o suplante páginas electrónicas, enlaces o ventanas emergentes.

Artículo 318. – Facilitación del Delito:

Será sancionada con pena de reclusión por un término fijo de cinco (5) años toda persona que facilite los medios para la perpetración de un delito ejecutado mediante un sistema o red informática o telemática, o contenedores electrónicos, ópticos o magnéticos.

Artículo 321. –Manipulación de Equipos o Terminales Móviles:

Será sancionada con pena de reclusión por un término fijo de cuatro (4) años toda persona que, manipule, re programe, remarque o modifique terminales móviles de los servicios de comunicaciones en cualquiera de sus componentes, con el propósito de alterar las bases de datos positivas y negativas que se establecerán para tal efecto y que serán administradas por la entidad regulatoria correspondiente.

Artículo 323. –Manipulación de Equipos de Localización y Vigilancia:

Toda persona que, retire, modifique o inutilice, sin la debida autorización, dispositivos de localización y vigilancia, será sancionada con pena de reclusión por un término fijo de cinco (5) años.

Artículo 342. – Uso de Equipos para Invasión de Privacidad:

Será sancionada con pena de reclusión por un término fijo de dos (2) años toda persona que, sin causa legítima o autorización de la entidad legalmente competente, use sistemas electrónicos, informáticos, telemáticos, de telecomunicaciones, o dispositivos susceptibles de realizar operaciones que atenten contra la privacidad en cualquiera de sus manifestaciones.

Artículo 343(a). –Acceso Indebido a Correspondencia o Comunicaciones del Sistema Público y del Gobierno de Puerto Rico:

Será sancionada con pena de reclusión por un término fijo de cinco (5) años, toda persona que:

- a) opere o abuse de los servicios o instalaciones de telecomunicaciones de libre recepción o de



En esa dirección, cabe resaltar otros artículos que, por su redacción, suscitan serias preocupaciones para la ACLU, ya que podrían entrar en conflicto con derechos constitucionales fundamentales. En particular, el Artículo 337, titulado “Exhibición Pornográfica”, dispone: “Toda persona que, ofrezca o publique **espectáculos teatrales o cinematográficos obscenos**, transmita audiciones o **efectúe publicaciones** de idéntico carácter, será sancionado con pena de reclusión por **un término fijo de diez (10) años**”. La ACLU reitera su postura a nivel nacional de que no favorece legislación que pretenda regular de manera amplia material obsceno, particularmente cuando las restricciones pueden alcanzar expresión protegida por la Primera Enmienda. Este tipo de legislación puede entrar en conflicto con la libertad de expresión cuando emplea categorías ambiguas o más amplias que

radiodifusión sin autorización de la autoridad correspondiente, y el que permita que, en su domicilio, residencia, morada o medio de transporte, operen tales servicios o instalaciones [...].

Artículo 345. – Acceso Indebido o Ilícito de Información Médica:

Toda persona que, sin autorización, violando o no los sistemas de seguridad, obtuviere para sí o para terceros, el acceso a datos médicos de otra persona, no destinados a él y especialmente protegidos contra el acceso no autorizado, será sancionada con pena de reclusión por un término fijo de cinco (5) años [...].

Artículo 350. – Apertura o Intercepción Ilegal de Comunicaciones:

Será sancionada con pena de reclusión por un término fijo de un (1) año toda persona que ilegítimamente abra, intercepte, o por cualquier otro medio tome conocimiento del contenido de un documento, pliego cerrado o despacho telegráfico, telemático, electrónico o de otra naturaleza que no le esté dirigido.

Artículo 368. – Difusión de Información Falsa:

Será sancionada con pena de reclusión por un término fijo de seis (6) años toda persona que, a través de medios electrónicos, informáticos, o mediante un sistema de telecomunicaciones, propague o difunda noticias o hechos falsos capaces de distorsionar o causar perjuicio a la seguridad y estabilidad del sistema financiero o de sus usuarios.

Artículo 371. –Divulgación de Información Financiera Reservada:

Será sancionada con pena de reclusión por un término fijo de cinco (5) años toda persona que, en beneficio propio o de terceros, divulgue información financiera clasificada como reservada por la autoridad competente en materia de finanzas públicas, cuando tal divulgación genere condiciones económicas desfavorables para el Estado.



la definición constitucional de obscenidad y, por consiguiente, puede tener un efecto inhibitor sobre expresión protegida. A su vez, el proyecto intenta definir de manera excesiva lo que se considera material obsceno, lo que podría generar una aplicación de alcance expansivo y poco definido de la disposición y, en consecuencia, criminalizar expresiones protegidas constitucionalmente, incluso cuando se trate de espectáculos o manifestaciones de carácter artístico. Más preocupante aún, la disposición establece **una pena de diez (10) años** de reclusión, que resulta excesiva y desproporcionada frente a la conducta que pretende sancionar.

Igualmente, el Artículo 351, titulado “Violación a la Intimidad”, también limita de forma excesiva la libertad de expresión, al criminalizar, con una pena de tres (3) años de reclusión, la publicación de audios, fotografías, videos o comunicaciones de otra persona sin su consentimiento o sin la debida autoridad legal.³ La disposición no solo plantea serias implicaciones constitucionales, sino ignora la realidad de que el uso de los medios tecnológicos se ha convertido en un importante mercado de ideas. Además, el lenguaje limitante de la libertad de expresión podría dar lugar a un sinnúmero de denuncias inmeritorias, motivadas por meras molestias o utilizadas como subterfugio para atender controversias de otra naturaleza.

Cabe destacar también que los artefactos cibernéticos han sido herramientas clave para documentar y divulgar injusticias, particularmente aquellas que de otro modo podrían permanecer ocultas o sin consecuencias. Sin embargo, el Artículo 351, según está actualmente redactado, perjudicaría más a la ciudadanía y menoscabaría sus derechos en lugar de garantizar su protección.

En esa dirección, a la ACLU le preocupan particularmente otros dos artículos que igualmente entran en conflicto con la Primera

³ Específicamente, el Artículo 351 – Violación a la Intimidad, dispone:
Será sancionada con pena de reclusión por un término fijo de tres (3) años toda persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y video, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona, por cualquier medio.



Enmienda: el Artículo 361, titulado “Calumnia o Injuria”, y el Artículo 362, titulado “Difamación”.⁴ Ambas disposiciones restringen de manera excesiva la libertad de expresión y la libertad de prensa al criminalizar expresiones o afirmaciones de hechos que resulten falsos, incluso cuando hayan sido realizadas de buena fe o como consecuencia de negligencia. Esta amplitud podría tener un efecto inhibitorio sobre la libertad de expresión como la libertad de prensa y desalentar la participación ciudadana, particularmente cuando las personas expresan opiniones o comparten información sobre asuntos de interés público.

Como es sabido, cuando se trata de acciones por difamación en el derecho de daños, existen salvaguardias diferenciadas dependiendo de si se trata de una persona pública o privada. La jurisprudencia, tanto local como federal, se inclina a proteger la libertad de expresión, incluso cuando la información resulta ser falsa, salvo que se demuestre la existencia de malicia real. El Tribunal Supremo federal ha manifestado que esta garantía constitucional propicia un intercambio de información libre, robusto y abierto al debate público. *New York Times Co. v. Sullivan*, 376 U.S. 254, 270 (1964).

En el referido caso, el Tribunal concluyó que la publicación de información falsa respecto a conducta oficial de un funcionario público no genera responsabilidad automática, pues es necesario demostrar que las publicaciones se hicieron con malicia real. En ese sentido, la persona debe demostrar que la información publicada se hizo “a sabiendas que era falsa o con un grave menosprecio de si era falsa o no”. *Torres Silva v. El Mundo, Inc.*, 106 DPR 415, 421 (1977).

⁴ Artículo 361. Calumnia o Injuria:

Será sancionada con pena de reclusión por un término fijo de dos (2) años toda persona que, impute falsamente a otra la comisión o participación en un delito concreto. Si la calumnia se propagara con publicidad, será sancionada con pena de reclusión por un término fijo de tres (3) años.

Artículo 362. Difamación:

Será sancionada con pena de reclusión por un término fijo de cinco (5) años toda persona que difame a través de medios electrónicos, informáticos, telemáticos, de telecomunicaciones o audiovisuales.



Respecto a la persona privada, el Máximo Foro federal ha expresado que las personas privadas gozan de un mayor grado de protección ya que no gozan de la misma exposición a los medios. Sin embargo, el Tribunal Supremo federal ha concluido que los estados no estarían permitidos a imponer daños punitivos o establecer presunciones de daño sin establecer malicia real. *Gertz v. Robert Welch, Inc.*, 418 U.S. 323, 343 (1974). Por lo tanto, en la medida que los Artículos 361 y 362 nada dicen sobre la necesidad de probar malicia o completo menosprecio por la verdad como elemento del delito, levantan grandes preocupaciones constitucionales y entran en conflicto con la jurisprudencia federal y estatal. Por otro lado, es importante destacar que la calumnia y la difamación debe manejarse por la vía civil, y no codificarse como delito. Al momento, ni la calumnia ni la difamación están contempladas en nuestro Código Penal.

De igual manera, resulta preocupante lo dispuesto en la sección sobre Delitos Sexuales, en su Artículo 326, pues omite considerar situaciones fácticas que pueden surgir entre adolescentes con edades próximas y, como consecuencia, no establece medidas para atenderlas adecuadamente. A manera de ejemplo, el Código Penal de Puerto Rico, en su Artículo 130 – Agresión Sexual, dispone que no se configura el delito cuando, aunque la víctima no haya cumplido los dieciséis (16) años, esta sea mayor de catorce (14) años y la diferencia de edad entre la víctima y la persona acusada sea de cuatro (4) años o menos. 33 L.P.R.A. § 5191.

De esta manera, la Asamblea Legislativa evitó imponer responsabilidad penal en situaciones entre adolescentes de edades próximas en las que no hubiese mediado violencia o coerción. Sin embargo, el P del S 974 no contiene una excepción de naturaleza similar, a pesar de que sabido que los adolescentes utilizan con frecuencia los medios electrónicos para comunicarse e interactuar.⁵ En otras palabras, en su intento de criminalizar el “sexting”, entre adultos y menores de edad, el proyecto también criminaliza conductas entre adolescentes de edades próximas, aun cuando no exista manipulación o agresión, sino que se trate de

⁵ UNICEF, Redes sociales y adolescentes: lo que tenés que saber, <https://www.unicef.org/uruguay/redes-sociales-y-adolescentes-lo-que-tenes-que-saber> (última visita 20 de agosto de 2026).



formas en que estos suelen interactuar mediante el uso de la tecnología.

En esa dirección, cabe resaltar, además, el Artículo 373. – Sabotaje al Sistema Financiero. El artículo dispone:

Será sancionada con pena de reclusión por un término fijo de **tres (3) años** toda persona que, **sin autorización modifique, destruya o provoque pérdida de información** contenida en sistemas o equipos de informática de instituciones integrantes del sistema financiero, siempre que tales sistemas se encuentren protegidos por **algún mecanismo de seguridad**. (Énfasis suplido).

Nuevamente, observamos cómo el proyecto intenta imponer una pena excesiva por una conducta que pudiera catalogarse como un error de buena fe. Inclusive, tampoco clarifica qué debe considerarse un “mecanismo de seguridad” ni si se requiere que la persona tenga o no acceso a este. Además, el uso de la palabra “algún” resulta sumamente ambiguo cuando se pretende imponer una pena de tres (3) años.

La amplitud del lenguaje del proyecto actual podría propiciar el uso indebido de sus disposiciones para instar denuncias innecesarias y sin fundamento, ya sea como medio de represalia o como herramienta para hostigar y silenciar. Tal como está redactado, el proyecto infringe con la jurisprudencia federal y con derechos fundamentales protegidos por la Constitución de los Estados Unidos y de Puerto Rico, particularmente con la Primera Enmienda y el principio de legalidad.

Las iniciativas para tipificar delitos cibernéticos, desde una perspectiva de derechos civiles y libertades constitucionales, conllevan profundas implicaciones sobre la privacidad ciudadana y el marco de vigilancia estatal. Ello porque cuando se redactan tipos penales sobre el acceso no autorizado a sistemas informáticos, interceptación de datos o cibercoso, el lenguaje amplio suele ser el principal riesgo por el efecto inhibitorio que causa la ambigüedad. Además, si hay falta de intención específica, esto es, si la ley no exige explícitamente una intención maliciosa, acciones legítimas de investigadores de seguridad, periodistas o activistas que exponen vulnerabilidades en el gobierno podrían ser



tipificadas como delito. Ello tiene un impacto en la libertad de expresión, pues definiciones imprecisas pueden ser instrumentalizadas para fiscalizar o criminalizar el discurso público, la protesta en línea o la crítica hacia funcionarios públicos en redes sociales, por ejemplo.

Por otro lado, la creación de nuevos delitos cibernéticos viene acompañada de mecanismos para facilitar su investigación. En la convergencia de la recopilación de prueba y el procedimiento criminal se hace patente los riesgos de la vigilancia

La ACLU reconoce la importancia de atender el problema de los delitos cibernéticos y comprende la complejidad de esta tarea. Sin embargo, en la medida en que el P. del S. 974 pretende aprobar un proyecto de ley sin considerar adecuadamente las serias implicaciones que sus disposiciones podrían tener sobre los derechos fundamentales de la ciudadanía, como aquí resaltados, además de imponer penas desproporcionadas, nos oponemos al proyecto. Somos de la opinión que este proyecto debe ser revisado y evaluado con detenimiento con personas expertas en la materia debido a las implicaciones trascendentales que puede tener sobre nuestros derechos.

En definitiva, proteger a la ciudadanía de crímenes cibernéticos no puede significar criminalizar indiscriminadamente las formas en que las personas se relacionan en el entorno digital. Por consiguiente, cualquier legislación que busque atender este asunto debe ser precisa, reflejar un adecuado entendimiento de los distintos contextos y guardar proporción con las conductas que pretende regular. De esta manera, la Asamblea Legislativa puede asegurarse de erradicar efectivamente las conductas abusivas sin extender innecesariamente el alcance del derecho penal.

Atentamente,

A handwritten signature in blue ink, appearing to read "Lolimar Escudero Rodríguez".

Lolimar Escudero Rodríguez
Abogada de Política Pública

Lcda. Claudia Fontanet Rodríguez
Harvard Fellow de Interés Público