GOBIERNO DE PUERTO RICO

18 va Asamblea Legislativa — 5ta Sesión Ordinaria

SENADO DE PUERTO RICO

P. del S. 1319

19 de junio de 2019

Presentado por el señor *Dalmau Ramírez*

Referido a la Comisión de Gobierno

LEY

Para establecer la "Ley de Privacidad de Información Electrónica" con el fin de proteger el derecho a la intimidad de las personas sobre información almacenada en un dispositivo electrónico o transmitida a un proveedor remoto de servicios de computadora.

EXPOSICIÓN DE MOTIVOS

El Gobierno de Puerto Rico tiene como política pública respetar y garantizar los derechos consagrados en la Declaración Universal de Derechos Humanos, adoptada por la Asamblea General de la Organización de las Naciones Unidas el 10 de diciembre de 1948. El Artículo 12 de dicho instrumento internacional, que es norma imperativa entre el cuerpo de normas del derecho internacional consuetudinario, establece que "[n]adie será objeto de injerencias arbitrarias en su vida privada, ni su familia, ni cualquier entidad, ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques". La Constitución de Puerto Rico recoge expresamente este derecho en la Sección 8 del Artículo II al disponer que "[t]oda persona tiene derecho a protección de ley contra ataques abusivos a su honra, a su reputación y a su vida privada o familiar".

Como corolario del derecho a la intimidad reconocido en la Constitución, la Sección 10 del Artículo II dispone que "[s]ólo se expedirán mandamientos autorizando registros, allanamientos o arrestos por autoridad judicial, y ello únicamente cuando exista causa probable apoyada en juramento o afirmación, describiendo particularmente el lugar a registrarse, y las personas a detenerse o las cosas a ocuparse". En vista de lo anterior, la Constitución requiere que el Estado obtenga una orden judicial basada en causa probable cada vez que pretenda realizar un registro o allanamiento que pueda incidir sobre la expectativa razonable de intimidad que posea la persona afectada sobre la cosa o el lugar a ser registrado, siempre que la sociedad esté dispuesta a reconocer que dicha expectativa merece ser protegida.

El derecho a la intimidad en Puerto Rico es de tal envergadura que el mismo opera *ex propio vigore* y puede hacerse valer entre personas privadas. "[E]ste derecho constitucional impone a toda persona el deber de no inmiscuirse en la vida privada o familiar de los demás seres humanos". *Figueroa Ferrer v. E.L.A.*, 107 D.P.R. 250 (1978). Es por ello que la protección opera tanto frente al Estado como ante personas particulares.

A pesar del sitial importante que ocupa el derecho a la intimidad en nuestro ordenamiento constitucional, el desarrollo de excepciones al requisito de orden judicial basada en causa probable por parte de los tribunales ha reducido el ámbito de aplicación de esta protección. La doctrina de información en manos de terceros constituye una de estas limitaciones importantes. En términos generales, esta doctrina plantea que una persona carece de expectativa razonable de intimidad sobre aquella información que divulgó voluntariamente a terceras personas. De cierta forma, se presupone que la persona "asume el riesgo" de que el Estado obtenga la información divulgada, independientemente de que el dueño de la información nunca haya pretendido entregarla al Gobierno.

Según plasmado recientemente en el Informe de la Comisión de Derechos Civiles sobre Vigilancia Gubernamental y Protesta Pública en Puerto Rico: Análisis de prácticas

de vigilancia por la Policía de Puerto Rico durante las manifestaciones del 1ro de mayo de 2017, mientras la Corte Suprema de Estados Unidos desarrollaba la doctrina de información en manos de terceros para eximir del requisito de orden judicial a nivel federal, desde hace más de dos décadas el Tribunal Supremo de Puerto Rico resolvió que el derecho a la intimidad incluido expresamente en nuestra Constitución es de factura más ancha que el que se desprende de la Constitución federal. Así, en *RDT Construction v. Contralor I*, 141 D.P.R. 424 (1996), el Máximo Foro se rehúso a aplicar automáticamente esta doctrina federal, reconociendo a una corporación una expectativa razonable de intimidad sobre sus cuentas bancarias. El Tribunal validó el reclamo de expectativa razonable de intimidad en ese caso, en parte, porque:

> Mediante dicha información, se puede determinar la ocupación de la persona investigada, los lugares que frecuenta, los bienes que adquiere, a qué partido o grupo político contribuye, los periódicos y las revistas que lee con frecuencia, la iglesia a la cual hace donativos, las asociaciones a las cuales pertenece, las tiendas o establecimientos donde compra, los médicos que visita y otra información de naturaleza íntima.

Id. en la pág. 441-42.

Más recientemente, en *Weber v. ELA*, 190 D.P.R. 688 (2014), el Tribunal Supremo extendió la visión expansiva sobre el derecho a la intimidad, reconociendo una expectativa razonable de intimidad sobre el registro de llamadas telefónicas de una persona, aun cuando se encuentre en manos de terceros, por lo cual el Estado no puede obtener esos registros sin obtener una orden judicial a esos efectos o, como mínimo, notificarle a la persona afectada. En palabras del Tribunal:

> A quién llamamos, cuándo lo llamamos, con qué frecuencia lo llamamos o por cuánto tiempo hablamos equivale, sin duda, a contenido. No cabe duda que hay una expectativa subjetiva de intimidad sobre el registro de llamadas que hace una persona y que la sociedad entiende que tal expectativa es razonable.

Id. en la pág. 712-13.

Si la doctrina de información en manos de terceros era cuestionable desde sus inicios, el desarrollo de nuevas tecnologías y el advenimiento del internet complican aún más su aplicación adentrado ya el siglo XXI. En momentos en que gran parte de nuestra sociedad utiliza tanto, o hasta depende de, dispositivos electrónicos desde los cuales envía y almacena información sensitiva, la aplicación desmedida de esta doctrina borraría de la Constitución la protección al derecho a la intimidad en el mundo digital siempre que un tribunal concluyese que ninguna información almacenada en un servidor de un proveedor de servicios de computadora goza de protección constitucional por haber sido divulgada voluntariamente a dicho proveedor.

Con el fin de proteger el derecho constitucional a la intimidad de las personas en el ámbito digital, esta Asamblea Legislativa establece el deber de las agencias de seguridad pública del Gobierno de Puerto Rico de obtener una orden judicial basada en causa probable como requisito previo para acceder a cierta información almacenada en un dispositivo electrónico o transmitida por su dueño a un proveedor remoto de servicios de computadora.

DECRÉTASE POR LA ASAMBLEA LEGISLATIVA DE PUERTO RICO:

Artículo 1. – Título

Esta Ley se conocerá como la "Ley de Privacidad de Información Electrónica".

Artículo 2. - Declaración de Política Pública

El Gobierno de Puerto Rico tiene como política pública respetar y garantizar los derechos consagrados en la Declaración Universal de Derechos Humanos. El Artículo 12 de dicho instrumento internacional establece que "[n]adie será objeto de injerencias arbitrarias en su vida privada, ni su familia, ni cualquier entidad, ni de ataques a su honra o su reputación". La Constitución de Puerto Rico recoge expresamente este

derecho en la Sección 8 del Artículo II al disponer que "[t]oda persona tiene derecho a protección de ley contra ataques abusivos a su honra, a su reputación y a su vida privada o familiar".

Como corolario del derecho a la intimidad reconocido en la Constitución, la Sección 10 del Artículo II dispone que "[s]ólo se expedirán mandamientos autorizando registros, allanamientos o arrestos por autoridad judicial, y ello únicamente cuando exista causa probable apoyada en juramento o afirmación, describiendo particularmente el lugar a registrarse, y las personas a detenerse o las cosas a ocuparse". En consecuencia, la Constitución requiere que el Estado obtenga una orden judicial basada en causa probable cada vez que pretenda realizar un registro o allanamiento que pueda incidir sobre la expectativa razonable de intimidad que posea la persona afectada sobre la cosa o el lugar a ser registrado, siempre que la sociedad esté dispuesta a reconocer que dicha expectativa merece ser protegida.

A raíz del vertiginoso avance tecnológico de estos tiempos, no es razonable concluir que una persona renuncia automáticamente a cualquier expectativa de intimidad sobre sus comunicaciones electrónicas por el mero hecho de que dicha información se encuentra almacenada realmente en los servidores de un proveedor de servicios de computadora. Con el propósito de hacer cumplir la política pública referida, establecemos claramente el deber de las agencias de seguridad pública del Gobierno de Puerto Rico de obtener una orden judicial basada en causa probable como requisito previo para acceder a cierta información almacenada en un dispositivo

electrónico o transmitida por su dueño a un proveedor remoto de servicios de computadora.

Artículo 3. – Definiciones

Para los fines de esta Ley, las siguientes palabras y frases tendrán el significado señalado a continuación:

1. Agencia de seguridad pública – cualquier entidad o subdivisión del Estado Libre Asociado de Puerto rico que se dedique primordialmente a prevenir, detectar o procesar actividad criminal, así como a poner en vigor leyes de naturaleza penal

2. Datos transmitidos – información electrónica o datos que son transmitidos inalámbricamente:

a. Desde un dispositivo electrónico a otro dispositivo electrónico sin utilizar una conexión intermedia; o

b. Desde un dispositivo electrónico a una antena cercana

3. Dispositivo electrónico – dispositivo que permite acceso a, o uso de, un servicio de comunicación electrónica, servicio remoto de computadoras o servicio de información de localización

4. Información de localización – información sobre la ubicación de un dispositivo electrónico, obtenida a través de un dispositivo de rastreo, que es generada, derivada u obtenida, parcial o totalmente, por la operación de un dispositivo electrónico

5. Información electrónica o datos – información o datos, incluyendo signos, señales, escritos, imágenes, sonidos o inteligencia de cualquier naturaleza, transmitida o almacenada parcial o totalmente mediante un sistema telegráfico, radial, electromagnético, fotoelectrónico o fotoóptico. Incluye la información de localización, datos almacenados o datos transmitidos de un dispositivo electrónico.

6. Récord de suscriptor – récord o información de un proveedor de un servicio de comunicaciones electrónicas o servicio remoto de computadoras que revela la siguiente información de un suscriptor o consumidor:

a. Nombre;

b. Dirección;

c. Récord de conexión telefónica a corta o larga distancia, o el récord del tiempo de la sesión o su duración;

d. La duración del servicio, incluido el día en que inició;

e. Tipo de servicio utilizado;

f. Número de teléfono, número de instrumento o cualquier otro número o identificación de suscriptor o consumidor, incluida una dirección de red asignada temporalmente

g. Medios y fuentes de pago por el servicio, incluyendo el número de una tarjeta de crédito o una cuenta bancaria.

7. Servicio de comunicación electrónica – servicio que provee a sus usuarios la habilidad de enviar o recibir comunicaciones electrónicas o telegráficas

8. Servicio de información de localización – proveedor de servicio de posicionamiento global (GPS, por sus siglas en inglés) o cualquier otro servicio basado en mapas, localización o información direccional

9. Servicio remoto de computadoras – proveedor de almacenamiento o procesamiento por computadora, mediante el uso de un sistema de comunicaciones electrónicas, dirigido al público

Artículo 4. —Requisito de orden judicial

(1) (a)Ninguna agencia de seguridad pública podrá obtener, como parte de una investigación o procesamiento criminal, sin una orden judicial basada en causa probable, la siguiente información:

i. Localización, información almacenada o datos transmitidos de un dispositivo electrónico; ni

ii. Información electrónica o datos transmitidos a un proveedor remoto de servicios de computador, incluyendo, pero sin limitarse a, el récord de suscriptor de la persona;

(b) Ninguna agencia de seguridad pública podrá usar, copiar o divulgar, para ningún propósito, la localización, la información almacenada, los datos transmitidos de un dispositivo electrónico, ni la información electrónica o los datos provistos por un proveedor remoto de servicios de computadora, que:

i. No formen parte de la orden judicial; y

ii. Hayan sido obtenidos como parte de un esfuerzo para obtener la localización, la información almacenada, los datos transmitidos de un dispositivo electrónico, o la información electrónica o los datos provistos por un proveedor remoto de servicios de computadora que sí forman parte de la orden judicial obtenida conforme a esta Ley.

(c) Una agencia de seguridad pública podrá usar, copiar o divulgar datos transmitidos de un dispositivo electrónico utilizado para comunicarse con el dispositivo electrónico que es objeto de la orden si la agencia de seguridad pública entiende razonablemente que los datos transmitidos son necesarios para cumplir el propósito de la orden.

(d) La información electrónica o los datos obtenidos en virtud de esta Ley serán destruidos de manera irrecuperable por la agencia de seguridad pública a la mayor brevedad posible luego de haber sido recolectada.

Artículo 5. — Excepciones

Una agencia de seguridad pública podrá obtener la localización, la información almacenada, los datos transmitidos de un dispositivo electrónico, la información electrónica o los datos provistos por un proveedor remoto de servicios de computadora, sin orden judicial, en las siguientes circunstancias:

1. Si el dispositivo es reportado perdido por su dueño;

2. Mediante el consentimiento informado y afirmativo del dueño o usuario del dispositivo electrónico;

3. Si el dueño ha divulgado pública y voluntariamente la información de localización; o

4. De un proveedor de servicios de computadora si dicho proveedor divulga voluntariamente la información de localización:

a. Bajo la creencia de que existe una emergencia que involucra un riesgo inminente de muerte, lesión física seria, abuso sexual, explotación sexual, secuestro o trata humana, de un individuo; o

b. Que es descubierta inadvertidamente por un proveedor de servicios de computadora y aparente estar relacionada con la comisión de un delito grave o de un delito menos grave que involucre violencia física, abuso sexual o deshonestidad.

Artículo 6. — Relevo de responsabilidad

Ningún proveedor de servicios de comunicación electrónica ni ningún proveedor de servicios remotos de computadora, sus oficiales, empleados o agentes responderá por haber provisto información o asistencia a una agencia de seguridad pública siempre que haya descansado de buena fe en los términos de una orden judicial basada en causa probable o en las excepciones provistas en el Artículo 5 de esta Ley.

Artículo 7. — Notificación

Toda agencia de seguridad pública que desee ejecutar una orden judicial al amparo de esta Ley deberá cumplir con los requisitos de notificación establecidos en las Reglas de Procedimiento Criminal a esos efectos.

Cuando la orden judicial tenga el propósito de obtener información en manos de un tercero, la agencia de seguridad pública deberá notificar la siguiente información al dueño del dispositivo electrónico, la información o los datos electrónicos especificados en la orden, dentro de los 5 días siguientes a la fecha en que la información o los datos electrónicos objeto de la orden hayan sido obtenidos:

1. Copia de la orden judicial solicitada y concedida;
2. El tipo de orden expedida;
3. El periodo de tiempo para el cual la recolección de información o datos fue autorizada;
4. El delito especificado en la solicitud para la orden; y
5. La identidad del juez que expidió la orden.

La obligación de notificar de este Artículo no se activa hasta tanto la identidad del dueño del dispositivo electrónico, la información o los datos especificados en la orden es conocida, o debía razonablemente ser conocida, por la agencia de seguridad pública.

Una agencia de seguridad pública que solicite una orden judicial al amparo de esta Ley podrá solicitar, y el tribunal podrá conceder, una posposición de la notificación requerida en este Artículo por un periodo no mayor de treinta (30) día, si el tribunal determina que existe causa probable para creer que la notificación podría:

1. Poner en peligro la vida o la seguridad física de un individuo;

2. Provocar la huida de una persona de la jurisdicción;

3. Conducir a la destrucción o alteración de evidencia;

4. Intimidar a un posible testigo; o

5. De alguna otra manera perjudicar seriamente una investigación o retrasar indebidamente un juicio.

A petición de la agencia de seguridad pública, un tribunal podrá conceder prórrogas adicionales al requisito de notificación, de no más de treinta (30) días cada una, siempre que se satisfagan todavía los mismos criterios que cuando se concedió la orden inicial.

Una vez vencida la prórroga concedida por el tribunal, la agencia de seguridad pública deberá enviar por correo al dueño del dispositivo electrónico, la información o los datos una copia de la orden judicial, acompañada de una notificación que:

1. Detalle con especificidad razonable la naturaleza de la investigación de la agencia de seguridad pública; y

2. Contenga la siguiente información:

a. Toda la información requerida en el primer párrafo de este Artículo.

b. Una declaración en torno a que la notificación fue pospuesta;

c. El nombre del tribunal que autorizó la posposición; y

d. Una referencia a la disposición de ley que autoriza dicha posposición.

Artículo 8. —Regla de exclusión

Evidencia obtenida en violación de esta sección será inadmisible en los tribunales.

Artículo 9. — Cláusula de Separabilidad

Si alguna de las disposiciones de la presente Ley fuere declarada inconstitucional, las restantes se mantendrán en vigor.

Artículo 10. — Esta Ley comenzará a regir inmediatamente luego de su aprobación.