Ciudad de México
9 de diciembre de 2020

FICHA TÉCNICA SOBRE EL PADRÓN NACIONAL DE USUARIOS DE TELEFONÍA MÓVIL

La Red en Defensa de los Derechos Digitales (R3D) condena la aprobación del *Dictamen por el que se reforma la Ley Federal de Telecomunicaciones y Radiodifusión para crear un "Padrón Nacional de Usuarios de Telefonía Móvil"*, por parte de la Comisión de Comunicaciones y Transportes de la Cámara de Diputados, y exige al Pleno que sea rechazado en atención a las siguientes consideraciones:

1. No existe evidencia de que los registros de tarjetas SIM contribuyan a la reducción de delitos como la extorsión

El Padrón Nacional de Usuarios de Telefonía Móvil es, en términos generales, una reedición del fallido Registro Nacional de Usuarios de Telecomunicaciones (RENAUT), promovido por el gobierno de Felipe Calderón y el entonces Secretario de Seguridad Pública, Genaro García Luna. Durante la operación del RENAUT, el delito de extorsión aumentó 40% y el de secuestro 8%.

Igualmente, estudios como el informe de la Asociación Mundial de Operadores de Telefonía GSMA sobre registro obligatorio de tarjetas SIM (2016) indican que "no existe evidencia de que el registro obligatorio de tarjetas SIM reduzca el crimen"[1].

Es por ello que países como el Reino Unido, Estados Unidos, Canadá y muchos otros han rechazado implementar este tipo de medidas.

2. El padrón sería fácil de evadir por la delincuencia

Es falso que el Padrón propuesto impida la comisión del delito de extorsión o que contribuya a su investigación y sanción. Asumir que las redes criminales usarán teléfonos asociados a su identidad para cometer sus delitos es inverosímil y falto de sentido común.

Actualmente existen múltiples técnicas y mecanismos que son utilizadas para la suplantación de números telefónicos, tales como: la clonación y duplicación de tarjetas SIM, el uso de tarjetas SIM de otras jurisdicciones en las que no existe un registro, (como Estados Unidos), la utilización de servicios de voz sobre IP (VOIP), el robo de teléfonos móviles, entre otros.

3. El padrón atenta contra la presunción de inocencia

Dada la facilidad con que es posible realizar llamadas telefónicas suplantando el número de teléfono de otra persona, es previsible que, de aprobarse el Dictamen, las autoridades investigadoras acusen a personas inocentes de la comisión de delitos.

1 https://www.gsma.com/publicpolicy/wp-content/uploads/2016/04/GSMA2016_Report_MandatoryRegistrationOfPrepaidSIMCards.pdf

Esto es aún más preocupante dada la redacción del artículo 180 Bis, el cual señala que "se presume [...] salvo prueba en contrario" que los actos jurídicos realizados desde una línea telefónica corresponden a la persona que se encuentra asociada al mismo en el Padrón.

Lo anterior no solo revierte la carga de la prueba, atentando así contra el principio de presunción de inocencia, sino que también implicaría el desperdicio de tiempo y recursos en el agotamiento de líneas de investigación que no conducen a la persona autora del delito.

4. La autoridad ya cuenta con múltiples herramientas para investigar delitos como la extorsión

Los promoventes del Dictamen ignoran que la autoridad investigadora ya cuenta con múltiples herramientas para combatir delitos como el de extorsión.

Por ejemplo, los artículos 303 del Código Nacional de Procedimientos Penales (CNPP) y 189 de la Ley Federal de Telecomunicaciones y Radiodifusión establecen la posibilidad de realizar la localización geográfica en tiempo real de equipos de comunicación móvil, así como el acceso a datos conservados por los concesionarios de telecomunicaciones respecto de toda línea de telefonía móvil —incluyendo las de prepago—, los cuales incluyen datos de ubicación geográfica respecto de cada comunicación. El CNPP inclusive permite a los ministerios públicos utilizar dichas técnicas de investigación sin autorización judicial previa, sujeto a ratificación posterior por parte de jueces de control en ciertos casos de emergencia, en los que se incluye el delito de extorsión.

No se omite señalar que la ausencia de controles democráticos estrictos para el uso de dichas técnicas de investigación ha provocado serios abusos por parte de la autoridad. Por ejemplo —según datos obtenidos por R3D vía solicitudes de acceso a la información— entre 2016 y 2017, 85% de las técnicas de investigación mencionadas se hicieron sin autorización judicial previa, aduciendo una situación de emergencia; sin embargo, los jueces de control no ratificaron más del 45% de los accesos a datos conservados ni 85% de las localizaciones geográficas en tiempo real. Igualmente, existen múltiples reportes de acceso no autorizado a las bases de datos conservadas por empresas de telecomunicaciones, producto de la corrupción.

En suma, ha existido un abuso sistemático y generalizado de las facultades de investigación que invaden la privacidad de personas usuarias de telefonía móvil, lo cual debería tener mayor prioridad para el Congreso de la Unión que otorgar todavía más facultades invasivas, con menos controles contra el abuso.

Por lo tanto, la ausencia del Padrón que pretende aprobarse no impide a las autoridades combatir delitos como el de extorsión, sino que constituye un pretexto inaceptable para maquillar la incompetencia de las instituciones de seguridad o intenciones autoritarias.

5. El padrón viola derechos humanos y pone en riesgo la seguridad de las personas usuarias de telefonía móvil

Como la propia experiencia del país demuestra, la creación de bases de datos personales centralizadas constituyen un serio riesgo para la privacidad y seguridad de la ciudadanía. La filtración o acceso no autorizado a dicha información puede ser utilizada precisamente para

cometer delitos en contra de la ciudadanía, por parte de la delincuencia que opera fuera y dentro de las instituciones del Estado y de las propias empresas concesionarias.

La base de datos del fallido RENAUT, que se pretende emular en el Dictamen, fue rápidamente vulnerada y puesta a la venta por $500 pesos[2], con lo cual se potenció el riesgo para la ciudadanía de ser víctima de delitos que dicho registro pretendía evitar.

De igual manera, organismos internacionales de derechos humanos —como la Relatoría para la Libertad de Expresión de la ONU— han advertido[3] que la vinculación obligatoria de una tarjeta SIM a la identidad de una persona compromete gravemente el derecho a comunicarse de manera anónima y facilita el monitoreo de la población, lo cual vulnera el derecho a la libertad de expresión, a la privacidad y hasta a la vida de las personas; especialmente si se toma en cuenta la abundante evidencia de abuso de herramientas de vigilancia por parte de autoridades en México y la innegable y frecuente colusión de funcionarios públicos con la delincuencia organizada.

Es por ello que resulta particularmente preocupante que el Dictamen no establezca mecanismo de control alguno para el acceso a la base de datos por parte de autoridades que, como se ha mencionado anteriormente, han abusado ampliamente de las facultades de acceso a datos personales de personas usuarias de telecomunicaciones[4].

6. La recolección y almacenamiento de datos biométricos como parte del Padrón puede violar el derecho a la privacidad de manera irreversible

De último momento, fue agregada al Dictamen la obligación de recolectar y almacenar datos biométricos como parte del Padrón Nacional de Usuarios de Telefonía Móvil. Esto no solo duplica el proceso de emisión de la Cédula de Identidad Digital —recientemente aprobada por la Cámara de Diputados— sino que, de igual manera que con la Cédula, pone en grave riesgo de que se generen violaciones irreversibles al derecho a la privacidad.

En caso de filtración, los datos biométricos, al constituir rasgos físicos ligados a una persona —como huella digital, rostro, iris o ADN— no son posibles de modificar o restituir, a diferencia de otros datos personales que pueden ser cambiados, como el número de teléfono, el número de documento de identidad, contraseña o nombre de usuario.

Lo anterior se agrava debido a que el Dictamen pretende la construcción de una base de datos biométricos masiva y centralizada, que crea un punto único de falla altamente atractivo a ataques informáticos.

2 https://hipertextual.com/2010/06/a-la-venta-los-datos-de-celulares-del-renaut-en-mexico

3 Informe del Relator Especial de la ONU para la promoción y protección del derecho a la libertad de expresión y opinión, David Kaye. 22 de Mayo de 2005. A/HRC/23/32.

4 Para más información sobre el abuso de las facultades de vigilancia contempladas en los artículos 189 y 190 de la LFTR ver: R3D. *El Estado de la Vigilancia: Fuera de Control. Noviembre de 2016.* https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016.pdf

Solo 17 países en el mundo exigen algún tipo de identificación biométrica para la compra de una tarjeta SIM. Dicha lista está predominantemente compuesta de países autoritarios como China, Arabia Saudita, Afganistán, Venezuela, Emiratos Árabes Unidos, Tayikistán, entre otros y que no incluye a ningún país plenamente libre y democrático.

El Padrón que establece el Dictamen constituye una política autoritaria, orientada al control y la vigilancia de la población, que es incompatible con la Constitución y los tratados internacionales de los que México es parte y pone en grave riesgo de daño irreversible a la población.

7. El Padrón desperdicia recursos indispensables para combatir la brecha digital

Finalmente, la creación y mantenimiento del Padrón tendría un enorme costo económico, tanto para el Instituto Federal de Telecomunicaciones como para los concesionarios y autorizados de telecomunicaciones —entre los cuales se encuentran proveedores de uso social sin fines de lucro—, el cual se ha estimado podría ascender a más de 21 mil millones de pesos.

Es una grave irresponsabilidad gastar miles de millones de pesos en medio de una crisis económica y una pandemia que ha desnudado las desigualdades y brechas digitales; sobre todo, para la construcción de un Padrón que no reducirá la incidencia delictiva y generará serios riesgos para la privacidad y seguridad de la ciudadanía.

El Padrón representa un gasto injustificado que distrae la urgente inversión en infraestructura para abatir la brecha digital, más cuando las autoridades de seguridad cuentan ya con múltiples herramientas alternativas para combatir delitos cometidos a través de la telefonía móvil.

En resumen, el “Padrón Nacional de Usuarios de Telefonía” propuesto:

- No contribuirá a la reducción del delito.
- No impedirá a extorsionadores continuar haciendo llamadas desde números no asociados a su identidad.
- Provocará que autoridades persigan líneas de investigación inútiles o que conducirán a la acusación de inocentes.
- Es innecesario, dado que ya existen múltiples herramientas para investigar y combatir delitos como la extorsión, como la localización geográfica en tiempo real y el acceso a datos conservados, además de la inhibición de las señales de telefonía en reclusorios y el combate a la corrupción en los mismos.
- Pone en riesgo la privacidad y seguridad de la población, dada la alta probabilidad de que la base de datos sea vulnerada, como ya sucedió en México con el fallido RENAUT.
- Al ser una base de datos masiva y centralizada constituye un punto único de falla, ampliamente atractivo para ataques informáticos y altamente vulnerable al acceso no autorizado de parte de autoridades y empleados de las empresas, vía corrupción o colusión con la delincuencia organizada.

- Genera un riesgo de daño irreversible a la privacidad al incluir la recolección y almacenamiento masivo y centralizado de datos biométricos.
- Constituye una medida propia de regímenes autoritarios que obstaculiza el derecho a la expresión anónima y facilita el monitoreo y control de la población en violación de los derechos humanos y las libertades fundamentales.
- Implica un desperdicio de recursos escasos en tiempos de crisis económica y sumamente necesarios para abatir la brecha digital en medio de una pandemia.
- No es una medida necesaria ni proporcional para el fin perseguido y, por ende, resulta inconstitucional y violatoria de los derechos humanos.

Por todo lo anterior, desde R3D: Red en Defensa de los Derechos Digitales hacemos un llamado urgente al Pleno de la Cámara de Diputados a desechar el Dictamen en su totalidad y abrir espacios de diálogo multiactor que informen al Congreso y a las autoridades de seguridad respecto de las múltiples alternativas para el combate al delito que tienen a su disposición y que no requieren la vulneración flagrante de los derechos humanos.