R3D
Red en Defensa de los Derechos Digitales

Análisis técnico y propuestas respecto del Dictamen de Ley Federal de Telecomunicaciones y Radiodifusión

Colaboración con la justicia - Conservación y acceso a datos de personas usuarias de telecomunicaciones

A. Conservación masiva e indiscriminada de metadatos de comunicaciones

a. Análisis

El artículo 190, fracción II de la LFTR vigente y el artículo 160, fracción II del Dictamen, establecen la obligación por parte de los concesionarios de telecomunicaciones y los autorizados que determine la autoridad reguladora de conservar de manera masiva, indiscriminada y prolongada los metadatos de comunicaciones. Es decir, a toda persona usuaria de telecomunicaciones —la casi totalidad de las cuáles no se encuentran vinculadas a ningún hecho delictivo— le es recolectada y almacenada por 24 meses, información sobre sus comunicaciones, incluyendo el tipo de comunicación, fecha, hora y duración de la misma, datos que identifican a los interlocutores y sus dispositivos, e incluso su localización aproximada.

Diversos tribunales constitucionales, internacionales y de derechos humanos han tenido la oportunidad de analizar la compatibilidad de disposiciones similares y han concluído que la conservación masiva, indiscriminada y prolongada de metadatos de comunicaciones resulta violatoria del derecho a la vida privada de las personas usuarias de telecomunicaciones.

Por ejemplo, el Tribunal de Justicia de la Unión Europea (en adelante "TJUE") ha establecido en el Caso *Digital Rights Ireland* que:

> *"Estos datos, considerados en su conjunto, pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los medios sociales que frecuentan".*[1]

Igualmente, el Relator Especial sobre la promoción y protección del derecho a la libertad de expresión de la Organización de las Naciones Unidas (en adelante "ONU"), ha señalado que:

---

[1] TJUE. Digital Rights Ireland vs. Minister of Communications, Marine and Natural Resources y otros. Casos Conjuntos, C-293/12 y C-594/12, 8 de abril de 2014, párr. 93.

> *"El carácter dinámico de la tecnología no solo ha cambiado la forma en que puede llevarse a cabo la vigilancia, sino también "qué" puede vigilarse. Al facilitar la creación de oportunidades de comunicación e intercambio de información, Internet también ha posibilitado la elaboración de un gran volumen de datos de transacciones de personas y acerca de estas. Esta información, conocida como datos de las comunicaciones o metadatos, incluye información personal sobre particulares, su ubicación y actividades en línea, así como registros e información conexa sobre los correos electrónicos y los mensajes que envían o reciben. Los datos de las comunicaciones pueden almacenarse, son accesibles y permiten la realización de búsquedas, y su revelación a las autoridades públicas y su utilización por estas están en gran medida no reguladas.* ***El análisis de estos datos puede ser sumamente revelador e invasivo, en particular cuando los datos se combinan y acumulan.*** *En tal sentido, los Estados se basan cada vez más en datos de las comunicaciones para prestar apoyo a las investigaciones de las fuerzas del orden o de seguridad nacional. Los Estados también están disponiendo la obligatoriedad de conservar y retener los datos de las comunicaciones para poder llevar a cabo una vigilancia histórica."*
>
> *(énfasis añadido)*

Inclusive, la propia SCJN ha reconocido que **"**del análisis de los datos de tráfico de comunicaciones se pueden extraer conclusiones muy precisas sobre la vida privada de las personas cuya información se ha conservado, como lo pueden ser los hábitos de la vida cotidiana, las actividades realizadas y las relaciones, entre otras"[2].

Por lo tanto, debe concluirse que la interferencia con el derecho a la vida privada producto del almacenamiento masivo e indiscriminado de los metadatos de comunicaciones no es, de ninguna manera, trivial, sino que la revelación ilícita o accidental de los mismos compromete seriamente los derechos humanos de las personas usuarias.

En apoyo de lo anterior, el Relator Especial sobre el derecho a la libertad de opinión y expresión de la ONU ha expresado que::

> *"Las leyes de retención de datos nacionales son invasivas y costosas, y amenazan los derechos a la privacidad y a la libertad de expresión. Al obligar a los proveedores de servicios de comunicación a crear grandes bases de datos con información acerca de quién se comunica con quien a través de un teléfono o de Internet, la duración de la comunicación, y la localización de las y los usuarios, y a conservar dicha información (en ocasiones por años), la leyes de retención obligatoria de datos incrementan el alcance de la vigilancia estatal de manera considerable, y por tanto el alcance de las violaciones a derechos humanos. Las bases de datos sobre datos de comunicaciones son, además, altamente vulnerables al robo, fraude y revelación accidental"[3].*

[2] SCJN. 2a Sala. Sentencia en el Amparo en Revisión 964/2015. 4 de mayo de 2016. Página 53 de la sentencia.
[3] Informe del Relator Especial sobre el derecho a la libertad de opinión y expresión de la Organización de las Naciones Unidas. 17 de abril de 2013. A/HRC/23/40

A este efecto, es fundamental observar que la obligación de conservación de datos es prolongada (por 24 meses), mucho más allá de lo que, en todo caso, sería necesario para la prestación del servicio. Además, que la conservación es masiva e indiscriminada, es decir, la obligación contemplada en el artículo 190, fracción II de la LFTR vigente y 160, fracción II del Dictamen implican la obligación de conservar una lista amplia de metadatos de comunicaciones, muchos de los cuáles no resulta necesario almacenar para la prestación del servicio respecto de la absoluta totalidad de las personas usuarias de telecomunicaciones. En este sentido, se conservan y almacenan los datos de millones de personas usuarias de telecomunicaciones, sin que la inmensa mayoría de ellos esté (o vaya a estar) implicada en una investigación de un delito o una amenaza a la seguridad nacional.

Esta recolección y almacenamiento masivo e indiscriminado de metadatos de comunicaciones ha sido considerada una medida innecesaria y desproporcionada, por ejemplo, por el TJUE, el cual ha señalado que:

> *"[L]a Directiva 2006/24 abarca de manera generalizada a todas las personas, medios de comunicación electrónica y datos relativos al tráfico sin que se establezca ninguna diferenciación, limitación o excepción en función del objetivo de lucha contra los delitos graves.*
>
> *En efecto, por una parte, la Directiva 2006/24* ***afecta con carácter global a todas las personas que utilizan servicios de comunicaciones electrónicas, sin que las personas cuyos datos se conservan se encuentren, ni siquiera indirectamente, en una situación que pueda dar lugar a acciones penales****. Por lo tanto,* ***se aplica incluso a personas respecto de las que no existen indicios que sugieran que su comportamiento puede guardar relación, incluso indirecta o remota, con delitos graves****. Además,* ***no establece ninguna excepción, por lo que se aplica también a personas cuyas comunicaciones están sujetas al secreto profesional con arreglo a las normas de la legislación nacional****.*
>
> *Por otra parte, aun cuando la Directiva pretende contribuir a la lucha contra la delincuencia grave,* ***no exige ninguna relación entre los datos cuya conservación se establece y una amenaza para la seguridad pública*** *y, en particular,* ***la conservación no se limita a datos referentes a un período temporal o zona geográfica determinados o a un círculo de personas concretas que puedan estar implicadas de una manera u otra en un delito grave, ni a personas que por otros motivos podrían contribuir, mediante la conservación de sus datos, a la prevención, detección o enjuiciamiento de delitos graves****.*
>
> *En segundo lugar, a esta falta general de límites se añade que la Directiva 2006/24 no fija ningún criterio objetivo que permita delimitar el acceso de las autoridades nacionales competentes a los datos y su utilización posterior con fines de prevención, detección o enjuiciamiento de delitos que, debido a la magnitud y la gravedad de la injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta, puedan considerarse suficientemente graves*

para justificar tal injerencia. Por el contrario, la Directiva 2006/24 se limita a remitir de manera general, en su artículo 1, apartado 1, a los delitos graves tal como se definen en la legislación nacional de cada Estado miembro.

(...) En tercer lugar, en lo que atañe al período de conservación de los datos, la Directiva 2006/24 prescribe, en su artículo 6, la conservación de éstos durante un período mínimo de seis meses ***sin que se establezca ninguna distinción entre las categorías de datos*** *previstas en el artículo 5 de la Directiva en función de su posible utilidad para el objetivo perseguido o de las personas afectadas.*

(...) De lo anterior resulta que la Directiva 2006/24 no establece reglas claras y precisas que regulen el alcance de la injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta. Por lo tanto, ***debe considerarse que esta Directiva constituye una injerencia en los derechos fundamentales de gran magnitud y especial gravedad en el ordenamiento jurídico de la Unión****, sin que esta injerencia esté regulada de manera precisa por disposiciones que permitan garantizar que se limita efectivamente a lo estrictamente necesario."*[4]

(énfasis añadido)

Igualmente, en el *Caso Watson y otros*, resuelto por el TJUE, respecto a una disposición similar, resolvió que:

"[S]i bien es cierto que la eficacia de la lucha contra la delincuencia grave, especialmente contra la delincuencia organizada y el terrorismo, puede depender en gran medida del uso de técnicas modernas de investigación, este objetivo de interés general, por muy fundamental que sea, no puede por sí solo justificar que una normativa nacional que establezca la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización deba ser considerada necesaria a los efectos de dicha lucha (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 51).

A este respecto, debe señalarse, por una parte, que una normativa de este tipo tiene como consecuencia, habida cuenta de sus características, descritas en el apartado 97 de la presente sentencia, que la conservación de los datos de tráfico y de localización se convierta en la regla, mientras que el sistema creado por la Directiva 2002/58 exige que esa conservación de datos sea excepcional.

Por otra parte, una normativa nacional, como la controvertida en el asunto principal, que cubre de manera generalizada a todos los abonados y usuarios registrados y que tiene por objeto todos los medios de comunicación electrónica así como todos los datos de tráfico, no establece ninguna diferenciación, limitación o excepción en función del objetivo que

[4] TJUE. Digital Rights Ireland vs. Minister of Communications, Marine and Natural Resources y otros. Casos Conjuntos, C-293/12 y C-594/12, 8 de abril de 2014.

se pretende lograr. Esta normativa afecta globalmente a todas las personas que hacen uso de servicios de comunicaciones electrónicas, aunque no se encuentren, ni siquiera indirectamente, en una situación que justifique una acción penal. Por tanto, esa normativa se aplica incluso a las personas de las que no existe ningún indicio para pensar que su comportamiento pueda tener una relación, incluso indirecta o remota, con la comisión de delitos graves. Además, no establece ninguna excepción, por lo que se aplica también a personas cuyas comunicaciones están sujetas a secreto profesional conforme al Derecho nacional (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartados 57 y 58).

Una normativa de este tipo no exige ninguna relación entre los datos cuya conservación se establece y una amenaza para la seguridad pública. En particular, no está limitada a una conservación de datos referentes a un período temporal, una zona geográfica o un círculo de personas que puedan estar implicadas de una manera u otra en un delito grave, ni a personas que por otros motivos podrían contribuir, mediante la conservación de sus datos, a la lucha contra la delincuencia (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 59).

Una normativa nacional como la controvertida en el asunto principal excede, por tanto, de los límites de lo estrictamente necesario y no puede considerarse justificada en una sociedad democrática, como exige el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta."[5]

De igual manera, en el presente caso la LFTR dispone la conservación masiva, obligatoria e indiscriminada de todos los metadatos de comunicaciones correspondientes a alrededor de 112.4 millones de líneas de telefonía móvil, lo cual representa aproximadamente al 89% de las personas habitantes en México[6]. Permaneciendo dicha obligación de conservación por 24 meses, tiempo durante el cual se encuentran en riesgo de vulneración o acceso no autorizado, sin que la inmensa mayoría de dichas personas y líneas telefónicas sean relevantes o se encuentren relacionadas con algún hecho delictivo y sin importar si las comunicaciones respecto de las cuales se conserva la información constituyen comunicaciones especialmente protegidas, por ejemplo, por virtud del derecho a la protección de las fuentes periodísticas o en atención al secreto profesional que existe entre una persona imputada de un delito y su abogada defensora.

De esta manera, se concluye que la recolección y almacenamiento prolongado, masivo e indiscriminado de metadatos de comunicaciones que establece el artículo 190, fracción II de la LFTR vigente y 160, fracción II del Dictamen violan el derecho a la privacidad de las personas usuarias de telecomunicaciones.

---

[5] TJUE. Watson y otros. Vs Secretary of State for the Home Department y otros. Casos Conjuntos, C-203/15 y C-698/15, 21 de diciembre de 2016.
[6] Instituto Federal de Telecomunicaciones (IFT). Nota Técnica de Datos Oportunos de los Indicadores de los sectores de Telecomunicaciones y Radiodifusión a septiembre de 2021. 20 de diciembre de 2021. Disponible en:
http://www.ift.org.mx/comunicacion-y-medios/comunicados-ift/es/89-de-cada-100-habitantes-en-el-pais-cuentan-con-servicio-movil-de-acceso-internet-comunicado

b. Propuesta

A partir del análisis anterior, se propone modificar el artículo 160, fracción II para sustituir la obligación de conservar metadatos de comunicaciones de manera indiscriminada y prolongada por un sistema en donde las autoridades facultadas pueden ordenar a los concesionarios y autorizados de telecomunicaciones la conservación temporal de información sobre líneas específicas que a su criterio resulten relevantes para una investigación, con la posibilidad de prorrogar dicha orden de conservación cuando sea necesario. Esto evitaría la conservación prolongada de la inmensa mayoría de la información que hoy es almacenada y puesta en riesgo de manera innecesaria, al no ser relevante para ninguna investigación.

Un estudio del Parlamento Europeo[7] ha demostrado que la ausencia de una obligación generalizada de retención masiva e indiscriminada de metadatos no ha tenido un impacto estadísticamente relevante en la investigación y persecución de hechos delictivos.

Sin embargo, dado que bajo el sistema propuesto será crucial que las fiscalías y otras autoridades facultadas actúen de manera oportuna para realizar los requerimientos de conservación y evitar la pérdida de evidencia útil para las víctimas de hechos delictivo, aunado a la actual inoperancia de las fiscalías, entendemos que el cese abrupto del sistema de conservación de metadatos puede representar un obstáculo tanto para las víctimas de hechos delictivos, como para las personas imputadas, por lo que se estima razonable establecer un régimen transitorio que mantenga el sistema actual por dos años en lo que las fiscalías son fortalecidas para ser capaces de desempeñar sus funciones con celeridad y profesionalismo.

B. Acceso a datos conservados y geolocalización en tiempo real

a. Análisis

[7] European Parliamentary Research Service. General Data Retention / Effects on Crime. 27 de enero de 2020. Disponible en: https://www.patrick-breyer.de/wp-content/uploads/2020/10/EPRS_103906-_General_data_retention___effects_on_crime_FINAL.docx

Los artículos 159 y 160 del Dictamen replican prácticamente sin cambio alguno lo que establecen los artículos 189 y 190 de la LFTR vigente. Cuando dichas disposiciones fueron establecidas en 2014, múltiples legisladores[8] y organizaciones de la sociedad civil[9] advertimos de los riesgos que éstas implicarían para la privacidad y seguridad de la población.

En su oportunidad, se advirtió que la falta de claridad y precisión respecto de las autoridades facultadas para hacer requerimientos y la ausencia del requisito explícito de control judicial previo podría producir serios abusos. Igualmente, se advirtió que la obligación de conservar masiva e indiscriminadamente los metadatos de comunicaciones de la totalidad de las personas usuarias de telecomunicaciones, además de ser una medida que no cumple con los estándares de derechos humanos de necesidad y proporcionalidad, conllevaba un grave riesgo de vulneración de datos y acceso ilícito por parte de actores estatales o no estatales.

En este sentido, en los Informes "El Estado de la Vigilancia: Fuera de Control" (2016), ¿Quién No Defiende Tus Datos? (2018) y "El Estado de la Vigilancia" (2025), hemos documentado cómo los riesgos advertidos se han materializado, destacándose las siguientes irregularidades y abusos:

1. **El acceso a datos conservados y la geolocalización en tiempo real por parte de autoridades sin facultades**

La Corte Interamericana de Derechos Humanos ha señalado que las medidas de restricción al derecho a la privacidad, en especial las medidas de vigilancia encubierta, deben ser precisas e indicar reglas claras y detalladas sobre la materia[10], tales como las circunstancias en que dicha medida puede ser adoptada; las personas autorizadas a solicitarla, a ordenarla y a llevarla a cabo; el procedimiento a seguir entre otros elementos[11].

---

[8] Ver Votos Particulares, Reservas e Intervenciones de las y los Senadores Corral, Encinas, Padierna, Bartlett, Robledo, Barrales y otros. Disponible en: https://www.senado.gob.mx/66/diario_de_los_debates/documento/2640 y Reservas e Intervenciones las y los Diputados Monreal, Alcalde, Mejía, Zavala y otros. Disponible en: https://cronica.diputados.gob.mx/DDebates/62/2do/2P/3Extra/jul/01L62A2E301.html#LEY%20FEDERAL%20DE%20TELECOMUNICACIONES%20Y%20RADIODIFUSION;%20LEY%20DEL%20SISTEMA%20PUBLICO%20DE%20RADIODIFUSION%20DEL%20ESTADO%20MEXICANO;%20Y%20DIVERSAS%20DISPOSICIONES%20EN%20MATERIA%20DE%20TELECOMUNICACIONES%20Y%20RADIODIFUSION11

[9] Ver Red en Defensa de los Derechos Digitales (R3D) #NoMásPoderAlPoder: Las amenazas a la privacidad en la Ley de Telecom. Disponible en: https://web.archive.org/web/20141012105948/http://internetlibre.mx/post/91191001866/nomaspoderalpoder-las-amenazas-a-la-privacidad-en-la y Ley de Telecomunicaciones; Nexos. Luis Fernando García y Carlos Brito. Enrique Peña Nieto contra el Internet. Disponible en: https://web.archive.org/web/20140405145500/http://www.redaccion.nexos.com.mx/?p=6176

[10] Corte IDH.Caso Escher y otros vs. Brasil. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 6 de julio de 2009. Serie C No. 200, párr. 131.

[11] Ídem

De igual manera, en el contexto de medidas de vigilancia encubierta, como la geolocalización, en tiempo real, de equipos de comunicación móvil o el acceso a metadatos de comunicaciones, el Tribunal Europeo de Derechos Humanos (TEDH) ha señalado que la ley debe ser lo suficientemente clara en sus términos para otorgar a los ciudadanos una indicación adecuada respecto de las condiciones y circunstancias en que las autoridades están facultadas para recurrir a dichas medidas.[12] Además, ha establecido que en vista del riesgo de abuso que cualquier sistema de vigilancia secreta implica, las medidas deben basarse en una ley que sea particularmente precisa, en vista de que la tecnología disponible para realizar esas actividades continuamente se vuelve más sofisticada[13].

En igual sentido, la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos señaló recientemente que:

> *"Las normas legales vagas o ambiguas que otorgan facultades discrecionales muy amplias son incompatibles con la Convención Americana, porque pueden sustentar potenciales actos de arbitrariedad que se traduzcan en la violación del derecho a la privacidad o del derecho a la libertad de pensamiento y expresión garantizados por la Convención.*
>
> *(...) Las leyes que habiliten la intercepción de las comunicaciones deben establecer con claridad y precisión las causas que el Estado puede invocar para solicitar esa intercepción, que sólo puede ser autorizada por un juez. Asimismo, se deben establecer por ley garantías vinculadas a la naturaleza, alcance y duración de las medidas de vigilancia; los hechos que podrían justificar esas medidas y las autoridades competentes para autorizarlas, llevarlas a cabo y supervisarlas. La ley debe ser clara en cuanto a posibles remedios para los abusos cometidos en el ejercicio de esas facultades."* [14]

No obstante lo anterior, los artículos 189 y 190, fracción I, II y III de la LFTR, los artículos 159 y 160, fracción I, II y III del Dictamen y los Lineamientos de colaboración en materia de seguridad y justicia vigentes, no señalan con precisión las autoridades facultadas para solicitar la colaboración de empresas para llevar a cabo las medidas de vigilancia, sino que únicamente se señala que las "autoridades competentes", no definidas por dicha ley, pueden solicitar dicha colaboración.

---

[12] TEDH. Caso de Uzun vs. Alemania. Aplicación No. 35623/05. Sentencia de 2 de Septiembre de 2010, párr. 61; Caso de Valenzuela Contreras vs. España. Aplicación No. 58/1997/842/1048. Sentencia de 30 de Julio de 1998, párr. 46.

[13] TEDH. Caso de Uzun vs. Alemania. Aplicación No. 35623/05. Sentencia de 2 de Septiembre de 2010, párr. 61; Weber y Sarabia vs. Alemania. Aplicación No. 54934/00. Decisión de 29 de Junio de 2006. párr. 93.

[14] CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. 31 de diciembre de 2013. OEA/Ser.L/V/II.

Si bien, al resolver el juicio de Amparo en Revisión 964/2015[15], interpuesto por R3D, la SCJN realizó una interpretación de los preceptos que pretendió dar más claridad a algunos de estos aspectos, como la definición de las autoridades competentes y la definición de algunas circunstancias específicas en las que puede ser solicitado el acceso a los datos conservados o la entrega de datos de localización en tiempo real, la ausencia de esta claridad en la ley formal y material, ha generado una grave incertidumbre jurídica que ha impactado en los derechos de las personas usuarias de servicios de telecomunicaciones, puesto que ha hecho imprevisibles las circunstancias y las autoridades que pueden llevar a cabo las interferencias secretas en la vida privada de la población.

Como muestra de lo anterior se puede apuntar, por ejemplo, que la Secretaría de Seguridad Pública del Estado de Baja California[16] y el Titular de Prevención y Readaptación Social de la Secretaría de Seguridad y Protección Ciudadana[17] se asumieron como "autoridades competentes" sin que las mismas posean una autorización explícita en una ley, o incluso sin que sea posible constitucionalmente que la tengan, como en el caso de las autoridades estatales, las cuales, según señala el artículo 16 constitucional, no se encuentran autorizadas a interferir con el derecho a la inviolabilidad de las comunicaciones privadas, a excepción del titular del ministerio público de la entidad federativa correspondiente.

Igualmente, se encuentra documentado, a partir de datos reportados por empresas de telecomunicaciones al IFT, que múltiples autoridades sin facultad expresa en la ley y sin encontrarse dentro de aquéllas identificadas por la SCJN, al resolver el Amparo en Revisión 964/2015, como autoridades facultadas para acceder a datos conservados por empresas de telecomunicaciones o a llevar a cabo la geolocalización en tiempo real, han accedido en la práctica a datos de personas usuarias de telefonía móvil. Por ejemplo, el Gobierno de Colima, el Gobierno del Estado de México, el Instituto Electoral de la Ciudad de México, la Secretaría de Comunicaciones y Transportes, la Secretaría de Hacienda y Crédito Público, la Secretaría de Seguridad Pública del Estado de Yucatán, la Secretaría de Seguridad Pública del Estado de Chiapas, el Sistema Estatal de Seguridad Pública del Estado de Baja California, el Instituto Electoral y de Participación Ciudadana del Estado de Oaxaca, Juzgados locales, la Policía Cibernética de Querétaro, la Procuraduría Federal de Protección al Consumidor, la Secretaría de Marina, así como decenas de miles de solicitudes

---

[15] R3D. La SCJN y la #LeyTelecom: Lo malo, lo bueno, lo absurdo y lo que sigue. Disponible en: https://r3d.mx/2016/05/05/la-scjn-y-la-leytelecom-lo-malo-lo-bueno-lo-absurdo-y-lo-que-sigue/

[16] Gobierno de Baja California. Acuerdo por el que el titular de la Secretaría de Seguridad Pública del Estado de Baja California, designa a los servidores públicos que se mencionan en el presente, para los efectos de lo dispuesto en el artículo 189 de la Ley Federal de Telecomunicaciones y Radiodifusión. Publicado en el Diario Oficial de la Federación el 9 de octubre de 2015. Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5411175&fecha=09/10/2015

[17] Secretaría de Seguridad y Protección Ciudadana (SSPC). Acuero por el que designa al Titular de Prevención y Readaptación Social como encargado de gestionar los requerimientos que se realicen en materia de telecomunicaciones y recibir la información correspondiente conforme a los artículos 189 y 190 de la Ley Federal de Telecomunicaciones y Radiodifusión; así como se le delegan las facultades que a continuación se indican. Publicado en el Diario Oficial de la Federación el 17 de marzo de 2020. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5589481&fecha=17/03/2020

de acceso a datos de usuarios y de geolocalización que han sido llevadas a cabo por autoridades no identificadas por las empresas de telecomunicaciones[18].

De esta manera, es claro que la incertidumbre jurídica alegada no resulta hipotética, sino que se ha materializado en perjuicio de los derechos de millones de personas usuarias de telefonía móvil en México, con lo cual se ha hecho evidente la incompatibilidad de los artículos 189 y 190, fracciones I, II y III vigentes (159 y 160 fracciones I, II y III del Dictamen) con el requisito de claridad, precisión y detalle que exigen el derecho a la privacidad y a la inviolabilidad de las comunicaciones privadas reconocidos en la Constitución y en los tratados internacionales de derechos humanos.

2. El acceso a datos conservados y la geolocalización en tiempo real sin control judicial efectivo

Una de las salvaguardas fundamentales para inhibir los riesgos de abuso de las medidas de vigilancia encubierta es el control judicial. La relevancia fundamental del control judicial previo o inmediato de medidas de vigilancia encubierta que invaden la privacidad de las personas ha sido resaltada por la Relatoría Especial para la Libertad de Expresión de la CIDH, la cual ha señalado que (énfasis añadido):

> *Las decisiones de realizar tareas de vigilancia que invadan la privacidad de las personas* ***deben ser autorizadas por autoridades judiciales independientes, que deben dar cuenta de las razones por las cuales la medida es idónea*** *para alcanzar los fines que persigue en el caso concreto; de si es lo suficientemente restringida para no afectar el derecho involucrado más de lo necesario; y de si resulta proporcional respecto del interés que se quiere promover.*[19]

En el mismo sentido, la Corte IDH ha establecido que "*se hace imprescindible que sean autoridades judiciales las encargadas de autorizar "medidas invasivas de recopilación de información""*, entendiéndose como los siguientes métodos de obtención de información (énfasis añadido):[20]

> *En todo caso, la efectiva protección de los derechos a la vida privada y a la libertad de pensamiento y de expresión, sumado al extremo riesgo de arbitrariedad que supone la utilización de las técnicas de vigilancia, selectiva o a gran escala, de las comunicaciones, máxime ante las nuevas tecnologías existentes, determinan para esta Corte que* ***cualquier medida en tal sentido (lo que incluye la interceptación, vigilancia y seguimiento de todo tipo de comunicación, sea telefónica, telemática o por***

---

[18] R3D. ¿Quién no defiende tus datos?. 2018. Páginas 13, 15. Disponible en: https://r3d.mx/wp-content/uploads/QNDTD-2018.pdf

[19] CIDH, Relatoría Especial para la Libertad de Expresión, Libertad de Expresión e Internet, 31 de diciembre de 2013, OEA/Ser.L/V/II, párr. 165.

[20] Corte IDH, Caso M*iembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia*, Sentencia de 18 de octubre de 2023, Excepciones Preliminares, Fondo, Reparaciones y Costas, párrs. 542, 547, 551 y 553.

> ***otras redes exige que sea una autoridad judicial la que decida sobre su procedencia, definiendo a su vez los límites que se imponen, incluidos el modo, tiempo y alcances de la medida autorizada.***
>
> *Asimismo, dado su carácter invasivo en la vida privada de las personas y ante la exigencia de establecer controles especialmente rigurosos,* ***métodos de obtención de información como la escucha y grabación electrónica, incluida la audiovisual, así como la pretensión de los organismos de inteligencia de requerir información referida a datos personales a empresas privadas*** *que, por distintos motivos, lícitamente la administren o gestionen, requieren también de autorización judicial.*
>
> *Así las cosas, el Tribunal Interamericano es consciente de que el derecho a la privacidad demanda medidas de protección en torno al uso de las nuevas tecnologías, incluido el internet, en el marco de las actividades de inteligencia. En consecuencia,* ***se requiere igualmente autorización judicial previa para el empleo de técnicas de vigilancia y seguimiento con relación a personas determinadas que impliquen el acceso a bases de datos y sistemas de información no públicos que almacenen y procesen datos personales, el rastreo de usuarios en la red informática o la localización de dispositivos electrónicos****.*[21]

De igual forma, refuerza la noción de protección especial que requiere la información obtenida y clasificada como "datos sensibles", en el sentido siguiente (énfasis añadido):

> ***La exigencia de autorización judicial previa en estos ámbitos se sustenta, además, en la necesidad de brindar una protección reforzada a los datos sensibles de las personas****, entendidos como una categoría "más estrecha" de datos personales [...] que abarca aquellos que afectan "a los aspectos más íntimos de las personas", y que, según el contexto cultural, social o político, podría incluir, entre otros, "datos relacionados con la salud personal, las preferencias sexuales o vida sexual, las creencias religiosas, filosóficas o morales, la afiliación sindical, los datos genéticos, los datos biométricos dirigidos a identificar de manera unívoca a una persona física, las opiniones políticas o el origen racial o étnico, información sobre cuentas bancarias,documentos oficiales, información recopilada de niños y niñas o geolocalización personal"*[22]*. En definitiva, se trata de datos que* ***merecen una protección especial porque permiten calificar al individuo y ofrecen sustento para la elaboración de perfiles personales****.*
>
> *El Tribunal destaca que la necesaria intervención de una autoridad judicial en todos estos ámbitos es coherente con el rol de garantes de los derechos humanos que corresponde a las juezas y los jueces en un sistema democrático, cuya necesaria*

---

[21] ONU, Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, A/HRC/23/40, párr. 86; Informe de OACNUDH, "El derecho a la privacidad en la era digital", A/HRC/27/37, párr. 45; Comité de Derechos Humanos, Observaciones finales sobre el cuarto informe periódico de la República de Corea, U.N. Doc. CCPR/C/COR/CO/4, 3 de diciembre de 2015, párr. 43; y Consejo de Derechos Humanos, Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, U.N. Doc. A/HRC/35/22, 30 de marzo de 2017, párrs. 19 y 78.

Véase también, Tribunal de Justicia de la Unión Europea, Casos *Tele2 Sverige AB Vs. Post-och telestyrelsen*, y *Secretary of State for the Home Department Vs. Tom Watson y otros*, No. C-203/15 y C-698/15, Sentencia de 21 de diciembre de 2016, párr. 120.

[22] Principios Actualizados del Comité Jurídico Interamericano sobre la Privacidad y la Protección de Datos Personales, con Anotaciones, Principio 9 y pág. 24. *También véase*, Identidad de género, e igualdad y no discriminacióna parejas del mismo sexo. Obligaciones estatales en relación con el cambio de nombre, la identidad de género, y los derechos derivados de un vínculo entre parejas del mismo sexo (interpretación y alcance de los artículos 1.1, 3, 7, 11.2, 13, 17, 18 y 24, en relación con el artículo 1 de la Convención Americana sobre DerechosHumanos). Opinión Consultiva OC-24/17 de 24 de noviembre de 2017. Serie A No. 24, párr. 136, y Consejo de Europa, Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, 28 de enero de 1981, artículo 6.

> *independencia posibilita el ejercicio de un control objetivo, conforme a Derecho, respecto del actuar de los otros órganos del poder público, en este caso, de los servicios de inteligencia del Estado.* ***Para el efecto, la autoridad judicial será la encargada de evaluar, en las circunstancias del caso concreto, el cumplimiento de las exigencias previamente descritas y de llevar a cabo el juicio de proporcionalidad con relación a la medida solicitada.***
>
> *Así, en congruencia con la jurisprudencia interamericana, la resolución que dicte la autoridad judicial habrá de estar debidamente motivada, pues, de lo contrario, sería una decisión arbitraria.* ***Por consiguiente, la resolución judicial deberá demostrar, mediante una argumentación racional, que han sido ponderados todos los requisitos constitucionales, legales y convencionales, así como los otros elementos que justifiquen, según corresponda, la concesión o la negativa de la medida****.*

Sin embargo, como en su momento fue advertido, los artículos 189 y 190 fracción I, II y III —que se reproducen en los artículos 159 y 160 fracción I, II y III del Dictamen— no otorgan certidumbre jurídica respecto de si el acceso a datos conservados o la geolocalización en tiempo real requerían autorización judicial federal previa. Esto provocó que en los primeros años de su implementación, el 99% de los accesos a datos conservados por empresas de telecomunicaciones y la geolocalización en tiempo real fueran llevadas a cabo sin control judicial[23].

Si bien, el artículo 303 del Código Nacional de Procedimientos Penales (en adelante "CNPP") y la Ley de la Guardia Nacional ya exigen, como regla general, la autorización judicial previa para llevar a cabo el acceso a datos conservados, el artículo 303 del Código Nacional de Procedimientos Penales establece excepciones a la regla del control judicial previo, estableciendo que "cuando esté en peligro la integridad física o la vida de una persona o se encuentre en riesgo el objeto del delito, así como en hechos relacionados con la privación ilegal de la libertad, secuestro, extorsión o delincuencia organizada", las fiscalías pueden ordenar directamente la geolocalización en tiempo real o la entrega de datos conservados por parte de los concesionarios y proveedores.

Cuando este mecanismo excepcional es utilizado por las fiscalías, el CNPP establece la obligación de informar al juez de control dentro de las 48 horas siguientes a que se haya cumplimentado el requerimiento, para efectos de que la autoridad judicial ratifique total o parcialmente la medida o revoque la misma. El Poder Judicial Federal también ha establecido mediante jurisprudencia que es competencia exclusiva de los jueces de control federales el conocer de las solicitudes de acceso a datos conservados[24].

---

[23] R3D. "*El Estado de la Vigilancia: Fuera de Control*" Noviembre 2016. Págs. 56 y 65 Consulta en: https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016.pdf

[24] Plenos Regionales. Tesis PR.P.CN. J/23 P (11a.) Gaceta del Semanario Judicial de la Federación. Libro 33, Enero de 2024, Tomo IV, página 3989. Registro digital: 2028011; y SCJN. Primera Sala. Tesis 1a. VI/2024 (11a.) Gaceta del Semanario Judicial de la Federación. Libro 37, Mayo de 2024, Tomo II, página 2250. Registro digital: 2028870.

No obstante lo anterior, las autoridades han eludido frecuentemente el control judicial federal. A partir de los datos obtenidos mediante solicitudes de acceso a la información entre 2016 y 2019, las autoridades admiten que al menos el 57.3% de las solicitudes reportadas fueron realizadas sin control judicial previo, de las cuales el 76.7% fueron realizadas invocando las causales de excepción a las que se refiere el artículo 303 del CNPP y de ellas, el 39.5% no fueron ratificadas total o parcialmente.

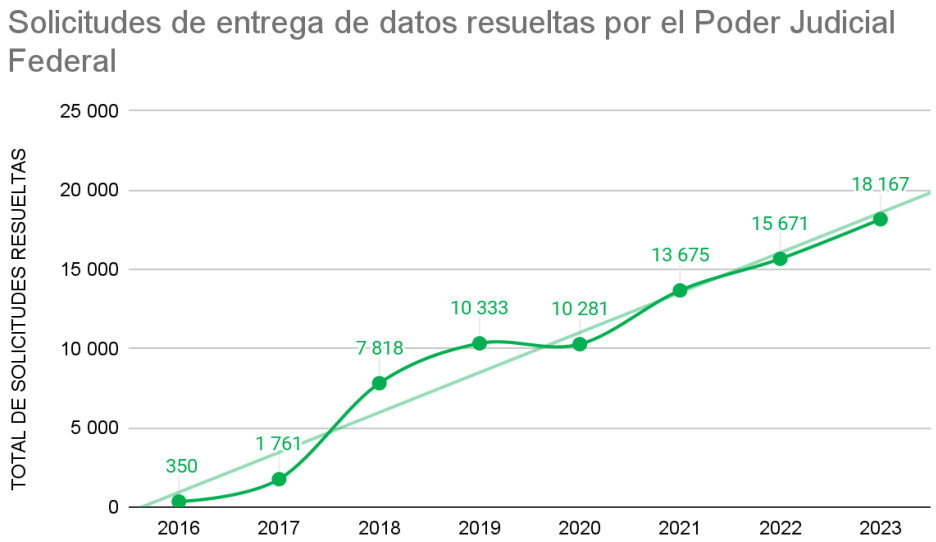
3. Irregularidades y abusos documentados

Al consultar los datos publicados por autoridades federales en la Plataforma Nacional de Transparencia (PNT), el Centro Nacional de Inteligencia (CNI) ha reportado en 0 el número de solicitudes de intervención de comunicaciones privadas desde el año 2016. La Fiscalía General de la República (FGR) únicamente reporta datos desde 2020, al igual que la Guardia Nacional, creada en 2019.

	Guardia Nacional	Fiscalía General de la República
2020	32	1967
2021	55	2017
2022	84	2299
2023	6	1891

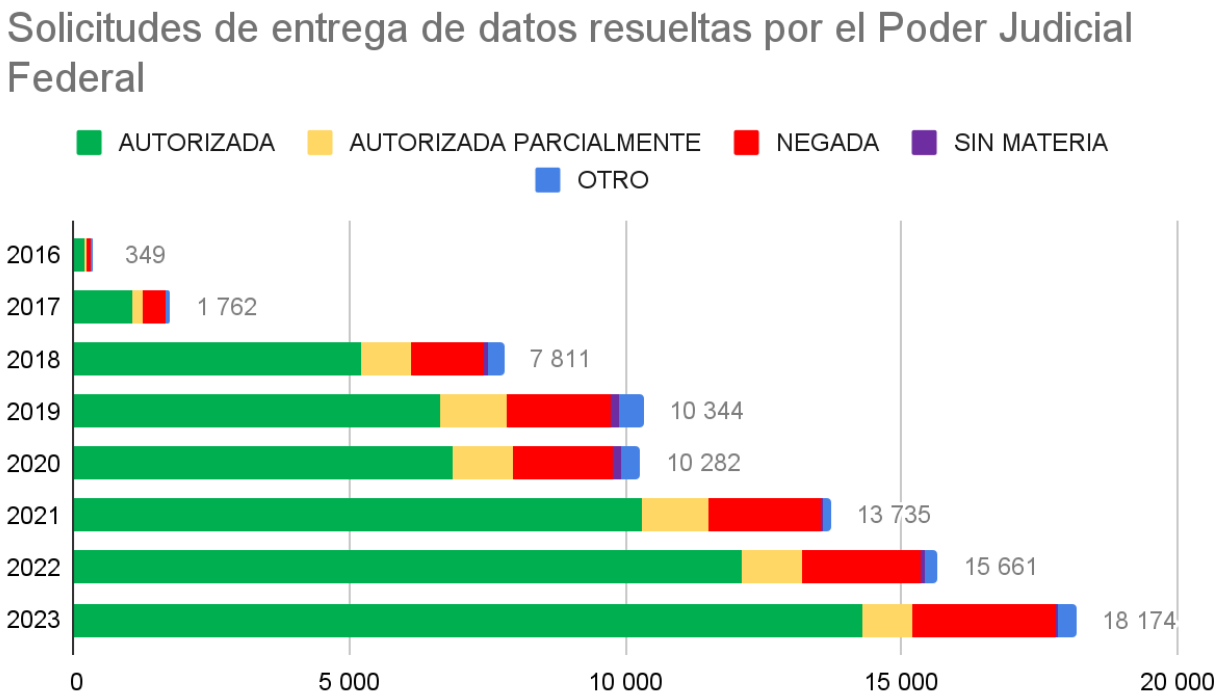
Tabla 2. Plataforma Nacional de Transparencia. Solicitudes de Intervención de Comunicaciones Privadas.

Por su parte, según datos publicados por el Poder Judicial de la Federación, también existe una clara tendencia al alza en la resolución de solicitudes de entrega de datos conservados por parte de jueces federales, especialmente a partir del año 2018:

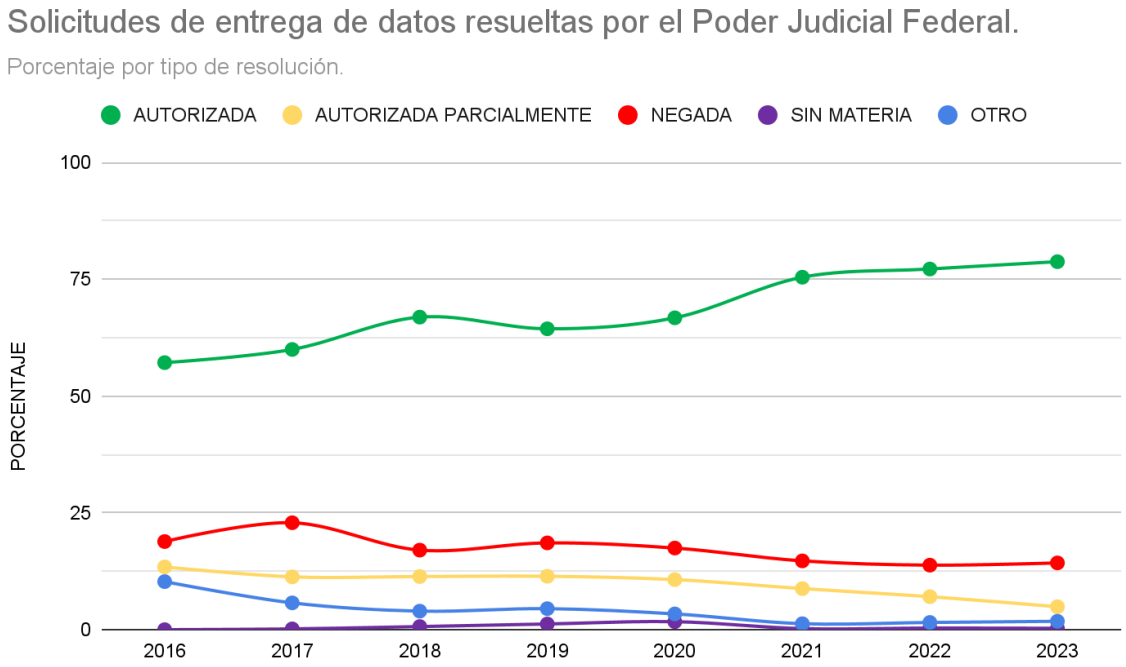


Gráfica 4. CJF. Dirección General de Estadística Judicial. Anexos Estadísticos.

Entre 2016 y 2023, en promedio el 78% de las solicitudes son autorizadas total o parcialmente, mientras que el 17.2% son negadas y el 4% tienen otro resultado no especificado.



Gráfica 5. CJF. Dirección General de Estadística Judicial. Anexos Estadísticos.



Gráfica 6. CJF. Dirección General de Estadística Judicial. Anexos Estadísticos.

No obstante lo anterior, el número de solicitudes de acceso a datos conservados y geolocalización reportados, no permite conocer el número de personas y líneas afectadas, en tanto las autoridades suelen solicitar datos de múltiples personas a través de una sola solicitud.

Por ejemplo, si bien la Guardia Nacional reportó haber solicitado la autorización para el acceso a datos conservados 32 veces en el año 2020, en respuesta[25] a una solicitud de acceso a la información realizada por R3D, la Guardia Nacional reportó haber obtenido los datos de 66 líneas telefónicas (2 líneas por solicitud).

[25] Guardia Nacional, Respuesta a la Solicitud de Información 2800100074421.

Al consultar la PNT se observa un amplio incumplimiento de la obligación de publicación de información estadística por parte de las fiscalías de las 32 entidades federativas, por lo que no resulta posible conocer el volumen de solicitudes llevadas a cabo por la mayoría de dichos entes. Aún en los casos en los que las fiscalías estatales sí han reportado información estadística, la información publicada no coincide con la información entregada a partir de solicitudes de acceso a la información realizadas por R3D.

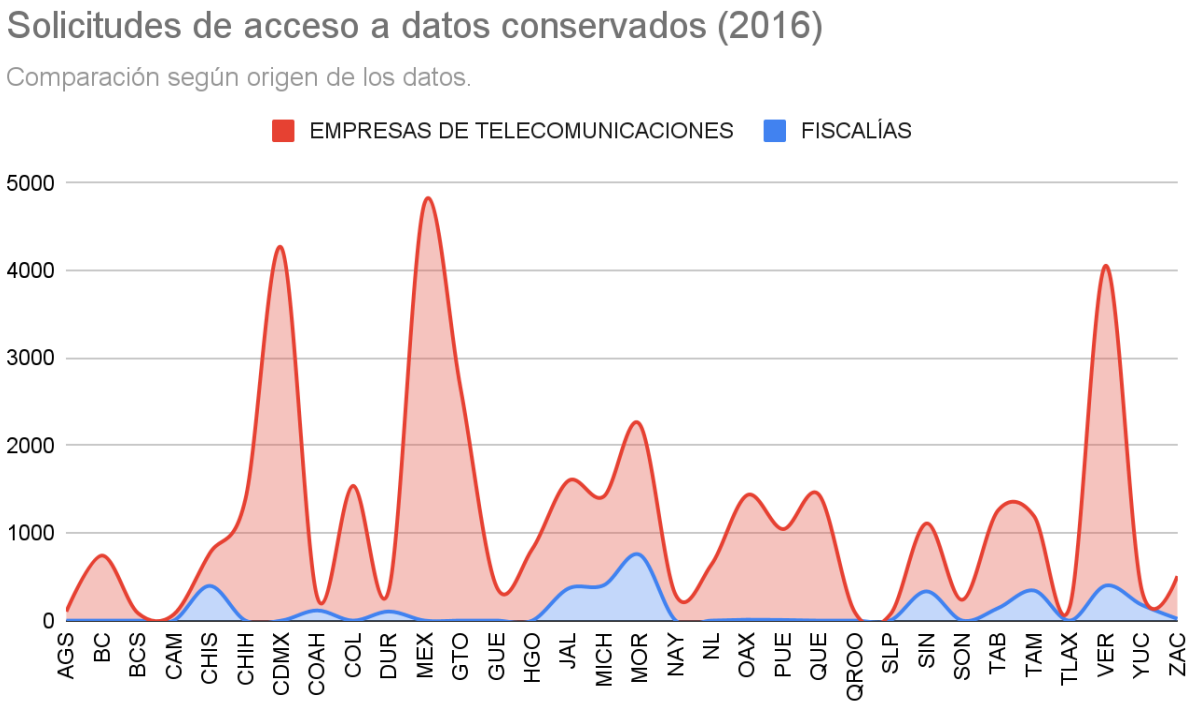
Por ejemplo, en el año 2020, las fiscalías del Estado de México, Guanajuato, Hidalgo y Tamaulipas reportaron ante la PNT haber realizado 1,728, 21, 3,988 y 1,578 solicitudes de acceso a datos conservados y geolocalización, respectivamente. En contraste, en respuesta a solicitudes de acceso a la información realizadas por R3D, dichas fiscalías reportaron haber realizado 37, 96, 116 y 586, respectivamente, siendo amplias las discrepancias detectadas.

Se aprecian aún más inconsistencias si se contrasta la información estadística reportada en respuesta a solicitudes de acceso a la información con la publicada por las concesionarias en materia de telecomunicaciones respecto de los años 2016 y 2017.

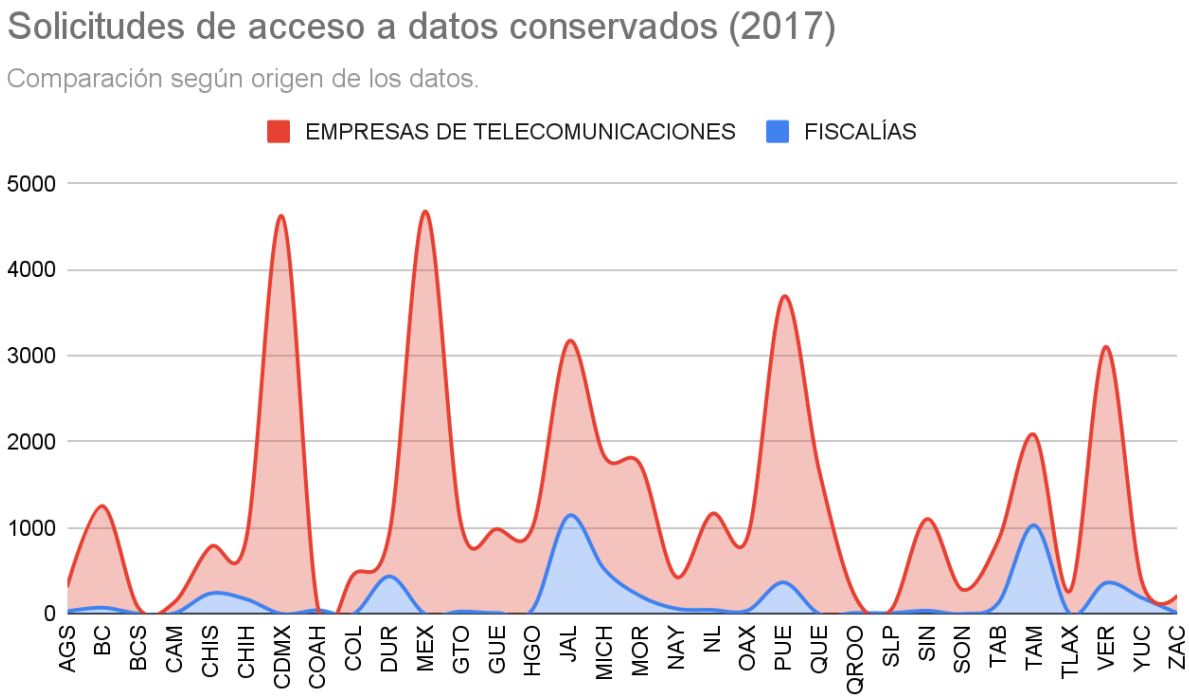
Por ejemplo, en respuesta a solicitudes de acceso a la información, la entonces Procuraduría General de la República (PGR) reportó haber realizado 10,444 solicitudes de acceso a datos conservados en 2016 y 7,073 en 2017. Sin embargo, según los datos reportados por empresas de telecomunicaciones, la PGR solicitó la entrega de datos conservados en 13,052 ocasiones en 2016 y 12,160 veces en 2017. Una discrepancia del 25% en 2016 y 72% en 2017.

Las empresas de telecomunicaciones reportaron haber recibido solicitudes de acceso a datos conservados de otras autoridades federales como el CISEN, la Secretaría de Hacienda y Crédito Público (SHCP) y la Secretaría de Marina, a pesar de que éstas reportaron en 0 en respuesta a solicitudes de acceso a la información y de que algunas de dichas autoridades ni siquiera poseen facultades legales para llevar a cabo dichos requerimientos.

En el caso de las Fiscalías Estatales las discrepancias son también notorias y generalizadas como se aprecia en las siguientes gráficas:



Gráfica 7. Respuestas a solicitudes de acceso a la información y Reportes de empresas de telecomunicaciones.



Gráfica 8. Respuestas a solicitudes de acceso a la información y Reportes de empresas de telecomunicaciones.

Asimismo, existen indicios de que un número importante de solicitudes de acceso a datos conservados en las que se invoca el mecanismo excepcional establecido en el artículo 303 del CNPP no son sometidas a ratificación por parte de la autoridad judicial federal.[26]

Entre los abusos que se han documentado, se encuentra evidencia revelada por *The New York Times* en noviembre de 2023 sobre cómo la Fiscalía General de Justicia de la Ciudad de México accedió a registros telefónicos, mensajes de texto y datos de localización de diversas figuras políticas, tanto del partido gobernante como de la oposición.[27]

---

[26] Abi-Habib, Maria, *et. al.*, "Políticos y funcionarios, blanco de vigilancia en México", *The New York Times*, 9 de noviembre de 2023, disponible en: https://www.nytimes.com/es/2023/11/09/espanol/mexico-vigilancia-fiscalia-telcel.html

[27] *Ibidem*.

La Fiscalía solicitó esta información a la empresa de telecomunicaciones Telcel, argumentando que estos datos serían utilizados en investigaciones sobre secuestros y desapariciones e invocando las causales de excepción de la autorización judicial previa a las que se refiere el artículo 303 del CNPP.

Este *modus operandi* de las autoridades también fue denunciado en 2019 por la periodista Marcela Turati; la cofundadora del Equipo Argentino de Antropología Forense (EAAF), Mercedes Doretti, y la defensora de derechos humanos Ana Lorena Delgadillo, quienes señalaron que la Subprocuraduría Especializada en Investigación de Delincuencia Organizada (SEIDO) accedió a sus registros telefónicos al incluirlas en la misma carpeta donde se investigaba a integrantes de una organización delictiva.[28]

La SEIDO investigó a Turati, Delgadillo y Doretti por los delitos de desaparición forzada y secuestro. De este modo, las autoridades accedieron a su información personal, los teléfonos que usaron y su ubicación geográfica. En el caso de Turati, además obtuvieron los datos personales que entregó a la Secretaría de Relaciones Exteriores para tramitar su pasaporte.

Cabe precisarse que el acceso a datos conservados se realizó sin autorización judicial y que bajo ninguna circunstancia puede considerarse justificado el acceso a dicha información en tanto no existe indicio alguno de que la periodista, defensora y perito, respectivamente, hayan participado en la comisión de delito alguno, sino que su participación en dicho caso consistía exclusivamente en el acompañamiento a las familias de las víctimas denunciantes.

A partir de estos casos se ha apreciado un *modus operandi* en el que las fiscalías abren una investigación o usan una existente y, con base en "información anónima", solicitan a las empresas de telecomunicaciones que les den información de números que no guardan relación con algún delito. De esta forma se utilizan carpetas sobre secuestro u otros delitos graves con la intención de eludir la obligación de obtener autorización judicial federal de manera previa. Además, en ningún caso someten a ratificación judicial las solicitudes de acceso a datos conservados, contraviniendo lo establecido en el artículo 303 del CNPP. Para ello, argumentan que no encontraron utilidad en la información y por ello no tenía sentido solicitar la ratificación judicial, por lo que, de manera imposible de comprobar procedieron a su destrucción.

El esquema documentado sugiere que podrían existir muchos más casos en los que autoridades han obtenido de las empresas de telecomunicaciones, metadatos de comunicaciones y la geolocalización en tiempo real de manera fraudulenta, sin que se lleven a cabo investigaciones que permitan identificar a otras víctimas y sancionar a los responsables.

---

[28] R3D, "SEIDO accedió a registros telefónicos para espiar a periodista y defensoras por investigar masacre de San Fernando", 26 de noviembre de 2021, disponible en: https://r3d.mx/2021/11/26/seido-accedio-a-registros-telefonicos-para-espiar-a-periodista-y-defensoras-por-investigar-masacre-de-san-fernando/

Adicionalmente, existen otros indicios de acceso no autorizado a los datos conservados, como son las revelaciones de que la Agencia de Seguridad Nacional de los Estados Unidos tendría acceso completo a todos los metadatos conservados por las empresas de telecomunicaciones[29] o las declaraciones del entonces Gobernador del Estado de Puebla, Miguel Barbosa Huerta, en donde reveló que el acceso no autorizado a las "sábanas de llamadas", es decir, a los datos que por virtud del artículo 190, fracción II de la LFTR conservan las empresas de telecomunicaciones, es frecuente:

> "(...) saben qué hacen las gentes de empresas privadas y de gobiernos (...) y de gobiernos, con las empresas como Telmex y todas las operadoras de cuestiones de telecomunicación, a los empleados, les compran las sábanas.
>
> (...) compran a los trabajadores de las telecomunicadoras, de las telefónicas. Compran las sábanas de las llamadas, , compran las llamadas en sí y dan seguimiento a las comunicaciones que quieren. Esa es una práctica viciosa, delincuencial que sigue existiendo. Y que hay empresas que lo hacen ¿eh?"[30] (SIC)

Finalmente, como se puede observar, la transparencia estadística es una herramienta útil para detectar irregularidades. Si bien las obligaciones de transparencia estadística fueron reincorporadas recientemente por el IFT en los Lineamientos de Colaboración en Materia de Seguridad y Justicia, resulta indispensable que la obligación de generar dichos reportes estadísticos provenga desde la propia Ley, para evitar que dichas obligaciones sean removidas arbitrariamente, como sucedió previamente, privando a la población de información estadística proveniente de empresas de telecomunicaciones desde 2018.

b. Propuesta

A partir del análisis anterior, se propone modificar los artículos 159 y 160 fracciones I y III, de manera que queden establecidas con mayor claridad las autoridades competentes para realizar los requerimientos y el control judicial de las medidas. Además, se propone establecer la participación amplia en el proceso de elaboración de lineamientos y orientar los mismos al establecimiento de salvaguardas contra el abuso, la transparencia y la rendición de cuentas y no solamente la eficacia y oportunidad.

En particular respecto de la transparencia, se propone lenguaje orientado a garantizar que a las personas usuarias de telecomunicaciones no les sea impedido acceder a sus propios datos conservados por empresas de telecomunicaciones y se ofrece

[29] La Jornada. La NSA registra cada llamada celular en México. 20 de mayo de 2014. Disponible en: https://www.jornada.com.mx/2014/05/21/mundo/026n1mun
[30] La Jornada de Oriente. El Gobernador pide investigar a empresas telefónicas que venden sábanas de llamadas de clientes. Video publicado en la plataforma YouTube el 22 de julio de 2021. Disponible en: https://www.youtube.com/watch?v=b0k0-deR58o

lenguaje específico respecto de la obligación de emitir reportes estadísticos comparables con las obligaciones de transparencia estadística que las autoridades deben emitir de conformidad con el artículo 65, fracción XLV de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP). Sin embargo, se admite que dicho nivel de precisión podría dejarse a los Lineamientos, siempre y cuando se establezca una obligación general de producir reportes estadísticos.

LEY VIGENTE	INICIATIVA	PROPUESTA A
Artículo 189. Los concesionarios de telecomunicaciones y, en su caso, los autorizados y proveedores de servicios de aplicaciones y contenidos están obligados a atender todo mandamiento por escrito, fundado y motivado de la autoridad competente en los términos que establezcan las leyes. Los titulares de las instancias de seguridad y procuración de justicia designarán a los servidores públicos encargados de gestionar los requerimientos que se realicen a los concesionarios y recibir la información correspondiente, mediante acuerdos publicados en el Diario Oficial de la Federación.	**Artículo 159.** Los concesionarios de telecomunicaciones y, en su caso, los autorizados y los proveedores de servicios de aplicaciones y contenidos, están obligados a atender todo mandamiento por escrito, fundado y motivado de la autoridad competente en los términos que establezcan las leyes. Los titulares de las instancias de seguridad y procuración de justicia designarán a los servidores públicos encargados de gestionar los requerimientos que se realicen a los concesionarios y, en su caso, autorizados a recibir la información correspondiente, mediante acuerdos publicados en el Diario Oficial de la Federación.	**Artículo 159.** Los concesionarios de telecomunicaciones y, en su caso, los autorizados y proveedores de servicios de aplicaciones y contenidos están obligados a atender todo mandamiento por escrito, fundado y motivado de la autoridad competente en los términos que ~~**establezcan las leyes**~~ **establece el Código Nacional de Procedimientos Penales, la Ley de Seguridad Nacional, la Ley de la Guardia Nacional y el Código Militar de Procedimientos Penales, previa autorización judicial federal.** Los titulares de las instancias de seguridad y procuración de justicia **competentes de conformidad a lo que señala el párrafo anterior** designarán a los servidores públicos encargados de gestionar los requerimientos que se realicen a los concesionarios y recibir la información correspondiente, mediante acuerdos publicados en el Diario Oficial de la Federación.

Artículo 190. Los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán: **I.** Colaborar con las instancias de seguridad, procuración y administración de justicia, en la localización geográfica, en tiempo real, de los equipos de comunicación móvil, en los términos que establezcan las leyes. Cualquier omisión o desacato a estas disposiciones será sancionada por la autoridad, en los términos de lo previsto por la legislación penal aplicable. El Instituto, escuchando a las autoridades a que se refiere el artículo 189 de esta Ley, establecerá los lineamientos que los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán adoptar para que la colaboración a que se refiere esta Ley con dichas autoridades, sea efectiva y oportuna;	**Artículo 160.** Los concesionarios de telecomunicaciones y, en su caso, los autorizados **que determine la Agencia**, deberán: I. Colaborar con las instancias de seguridad, procuración y administración de justicia, en la localización geográfica, en tiempo real, de los equipos terminales, en los términos que establezcan las leyes; Cualquier omisión o desacato a estas disposiciones será sancionada por la autoridad, en los términos de lo previsto por la legislación penal aplicable. **La Agencia**, escuchando a las autoridades a que se refiere el artículo **158** de esta Ley, establecerá los lineamientos que los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán adoptar para que la colaboración a que se refiere esta Ley con dichas autoridades, sea efectiva y oportuna;	**Artículo 160.** Los concesionarios de telecomunicaciones y, en su caso, los autorizados **que determine la Agencia** deberán: I. Colaborar con las ~~**instancias de seguridad, procuración y administración de justicia**~~ **autoridades competentes en términos del artículo anterior**, en la localización geográfica, en tiempo real, de los equipos de comunicación móvil, en los términos que establezcan las leyes. Cualquier omisión o desacato a estas disposiciones será sancionada por la autoridad, en los términos de lo previsto por la legislación penal aplicable. **La Agencia**, escuchando a las autoridades a que se refiere el artículo ~~**158**~~ **159** de esta Ley, **a las empresas concesionarias, autorizadas, a los proveedores de servicios, aplicaciones y contenidos, así como a las organizaciones de la sociedad civil, personas académicas y otras partes interesadas**, establecerá los lineamientos que los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán adoptar para que la colaboración a que se refiere esta Ley con dichas autoridades, sea efectiva~~,~~ ~~y~~ oportuna **y con salvaguardas para prevenir, detectar y remediar abusos, incluyendo medidas de registro,**

		transparencia, supervisión y notificación a las personas usuarias afectadas;
II. Conservar un registro y control de comunicaciones que se realicen desde cualquier tipo de línea que utilice numeración propia o arrendada, bajo cualquier modalidad, que permitan identificar con precisión los siguientes datos: a) Nombre, denominación o razón social y domicilio del suscriptor; b) Tipo de comunicación (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluidos el reenvío o transferencia de llamada) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia y avanzados); c) Datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil: número de destino, modalidad de líneas con contrato o plan tarifario, como en la modalidad de líneas de prepago; d) Datos necesarios para determinar la fecha, hora y duración de la comunicación, así como el servicio de mensajería o multimedia;	**II.** Conservar un registro y control de comunicaciones que se realicen desde cualquier tipo de equipo terminal o línea que utilice numeración propia o arrendada, bajo cualquier modalidad, que permitan identificar con precisión los siguientes datos: a) Nombre, denominación o razón social y domicilio del suscriptor; b) Tipo de comunicación (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluidos el reenvío o transferencia de llamada) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, mensajes instantáneos, servicios multimedia y avanzados); c) Datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil: número de destino, modalidad de líneas con contrato o plan tarifario, como en la modalidad de líneas de prepago; d) Datos necesarios para determinar la fecha, hora y duración de la comunicación, así como el servicio de mensajería o multimedia;	**II.** Conservar un registro y control de comunicaciones que se realicen desde cualquier tipo de línea que **sea requerida por autoridad competente, ya sea que** utilice numeración propia o arrendada, bajo cualquier modalidad, que permitan identificar con precisión los siguientes datos: a) Nombre, denominación o razón social y domicilio del suscriptor; b) Tipo de comunicación (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluidos el reenvío o transferencia de llamada) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia y avanzados); c) Datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil: número de destino, modalidad de líneas con contrato o plan tarifario, como en la modalidad de líneas de prepago; d) Datos necesarios para determinar la fecha, hora y duración de la comunicación, así como el servicio de

e) Además de los datos anteriores, se deberá conservar la fecha y hora de la primera activación del servicio y la etiqueta de localización (identificador de celda) desde la que se haya activado el servicio; f) En su caso, identificación y características técnicas de los dispositivos, incluyendo, entre otros, los códigos internacionales de identidad de fabricación del equipo y del suscriptor; g) La ubicación digital del posicionamiento geográfico de las líneas telefónicas, y h) La obligación de conservación de datos, comenzará a contarse a partir de la fecha en que se haya producido la comunicación. Para tales efectos, el concesionario deberá conservar los datos referidos en el párrafo anterior durante los primeros doce meses en sistemas que permitan su consulta y entrega en tiempo real a las autoridades competentes, a través de medios electrónicos. Concluido el plazo referido, el concesionario deberá conservar dichos datos por doce meses adicionales en sistemas de almacenamiento electrónico, en cuyo caso, la entrega de la información a las autoridades competentes se realizará	e) Además de los datos anteriores, se deberá conservar la fecha y hora de la primera activación del servicio y la etiqueta de localización (identificador de celda) desde la que se haya activado el servicio; f) En su caso, identificación y características técnicas de los dispositivos, incluyendo, entre otros, los códigos internacionales de identidad de fabricación del equipo y del suscriptor; g) La ubicación digital del posicionamiento geográfico de las líneas telefónicas; y h) La obligación de conservación de datos, comenzará a contarse a partir de la fecha en que se haya producido la comunicación. Para tales efectos, el concesionario y en su caso, el autorizado deberá conservar los datos referidos en el párrafo anterior durante los primeros doce meses en sistemas que permitan su consulta y entrega en tiempo real a las autoridades competentes, a través de medios electrónicos. Concluido el plazo referido, el concesionario y en su caso, el autorizado deberá conservar dichos datos por doce meses adicionales en sistemas de almacenamiento electrónico, en cuyo caso, la entrega de la información a las	mensajería o multimedia; e) Además de los datos anteriores, se deberá conservar la fecha y hora de la primera activación del servicio y la etiqueta de localización (identificador de celda) desde la que se haya activado el servicio; f) En su caso, identificación y características técnicas de los dispositivos, incluyendo, entre otros, los códigos internacionales de identidad de fabricación del equipo y del suscriptor; g) La ubicación digital del posicionamiento geográfico de las líneas telefónicas, y h) La obligación de conservación de datos, comenzará a contarse a partir de la fecha en que se haya producido la comunicación. Para tales efectos, el concesionario deberá conservar los datos referidos en el párrafo anterior**, respecto de las líneas que sean especificadas en el requerimiento, hasta por un tiempo máximo de noventa días a partir del requerimiento, sujeto a una sola prórroga por 90 días adicionales.** ~~**durante los primeros doce meses en sistemas que permitan su consulta y entrega en tiempo real a las autoridades competentes, a través de**~~

dentro de las cuarenta y ocho horas siguientes, contadas a partir de la notificación de la solicitud. La solicitud y entrega en tiempo real de los datos referidos en este inciso, se realizará mediante los mecanismos que determinen las autoridades a que se refiere el artículo 189 de esta Ley, los cuales deberán informarse al Instituto para los efectos de lo dispuesto en el párrafo tercero, fracción I del presente artículo. Los concesionarios de telecomunicaciones y, en su caso, los autorizados, tomarán las medidas técnicas necesarias respecto de los datos objeto de conservación, que garanticen su conservación, cuidado, protección, no manipulación o acceso ilícito, destrucción, alteración o cancelación, así como el personal autorizado para su manejo y control. Sin perjuicio de lo establecido en esta Ley, respecto a la protección, tratamiento y control de los datos personales en posesión de los concesionarios o de los autorizados, será aplicable lo dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares;	autoridades competentes se realizará dentro de las cuarenta y ocho horas siguientes, contadas a partir de la notificación de la solicitud. La solicitud y entrega en tiempo real de los datos referidos en este inciso, se realizará mediante los mecanismos que determinen las autoridades a que se refiere el artículo **159** de esta Ley, los cuales deberán informarse a la Agencia para los efectos de lo dispuesto en el párrafo tercero, fracción I del presente artículo. Los concesionarios de telecomunicaciones y, en su caso, los autorizados **que determine la Agencia**, tomarán las medidas técnicas necesarias respecto de los datos objeto de conservación, que garanticen su conservación, cuidado, protección, no manipulación o acceso ilícito, destrucción, alteración o cancelación, así como el personal autorizado para su manejo y control. Sin perjuicio de lo establecido en esta Ley, respecto a la protección, tratamiento y control de los datos personales en posesión de los concesionarios o de los autorizados, será aplicable lo dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares;	~~**medios electrónicos. Concluido el plazo referido, el concesionario deberá conservar dichos datos por doce meses adicionales en sistemas de almacenamiento electrónico, en cuyo caso, la entrega de la información a las autoridades competentes se realizará dentro de las cuarenta y ocho horas siguientes, contadas a partir de la notificación de la solicitud.**~~ La solicitud y entrega ~~**en tiempo real**~~ de los datos referidos en este inciso, se realizará mediante **los mecanismos establecidos en las Leyes y en los Lineamientos a los que se refiere la fracción I de este artículo.** ~~**que determinen las autoridades a que se refiere el artículo 159 de esta Ley, los cuales deberán informarse al Instituto para los efectos de lo dispuesto en el párrafo tercero, fracción I del presente artículo.**~~ Los concesionarios de telecomunicaciones y, en su caso, los autorizados, tomarán las medidas técnicas necesarias respecto de los datos objeto de conservación, que garanticen su conservación, cuidado, protección, no manipulación o acceso ilícito, destrucción, alteración o cancelación, así como el personal autorizado para su manejo y control. **Los concesionarios de**

		telecomunicaciones y, en su caso, los autorizados que determine la Agencia mantendrán medidas de registro y control de los requerimientos en los que se incluirá el nombre de los empleados encargados de la tramitación de los requerimientos y otros datos que señale el Instituto en los Lineamientos. Sin perjuicio de lo establecido en esta Ley, respecto a la protección, tratamiento y control de los datos personales en posesión de los concesionarios o de los autorizados, será aplicable lo dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, **incluyendo respecto del derecho de acceso a los usuarios a los datos conservados en virtud de esta fracción**;
III. Entregar los datos conservados a las autoridades a que se refiere el artículo 189 de esta Ley, que así lo requieran, conforme a sus atribuciones, de conformidad con las leyes aplicables. Queda prohibida la utilización de los datos conservados para fines distintos a los previstos en este capítulo, cualquier uso distinto será sancionado por las autoridades competentes en términos administrativos y penales que resulten.	**III.** Entregar los datos conservados a las autoridades a que se refiere el artículo **159** de esta Ley, que así lo requieran, conforme a sus atribuciones, de conformidad con las leyes aplicables. Queda prohibida la utilización de los datos conservados para fines distintos a los previstos en este Capítulo, cualquier uso distinto será sancionado por las autoridades competentes en términos de las disposiciones jurídicas administrativas y penales que resulten **aplicables**.	III. Entregar, **previa autorización judicial federal**, los datos conservados a las autoridades a que se refiere el artículo **159** de esta Ley, que así lo requieran, conforme a sus atribuciones, de conformidad con las leyes aplicables. **Excepcionalmente podrán entregarse datos conservados o el acceso a la geolocalización, en tiempo real, de equipos de comunicación móvil, sin previa autorización judicial en los casos establecidos explícitamente en**

Los concesionarios de telecomunicaciones y, en su caso, los autorizados, están obligados a entregar la información dentro de un plazo máximo de veinticuatro horas siguientes, contado a partir de la notificación, siempre y cuando no exista otra disposición expresa de autoridad competente;	Los concesionarios de telecomunicaciones y, en su caso, los autorizados que determine la Agencia, están obligados a entregar la información dentro de un plazo máximo de veinticuatro horas siguientes, contado a partir de la notificación, siempre y cuando no exista otra disposición expresa de autoridad competente;	**las leyes correspondientes. Transcurrido el plazo para la ratificación de la medida por parte del Juez de Control, los concesionarios, y en su caso, los autorizados darán aviso a la autoridad judicial federal competente.** Queda prohibida la utilización de los datos conservados para fines distintos a los previstos en este capítulo, cualquier uso distinto será sancionado por las autoridades competentes en términos administrativos y penales que resulten. Los concesionarios de telecomunicaciones y, en su caso, los autorizados, están obligados a entregar la información dentro de un plazo máximo de veinticuatro horas siguientes, contado a partir de la notificación, siempre y cuando no exista otra disposición expresa de autoridad competente; **Los concesionarios de telecomunicaciones y, en su caso, los autorizados, así como los proveedores de aplicaciones, contenidos y servicios en Internet deberán entregar al Instituto, en los meses de enero, abril, julio y octubre de cada año, un informe trimestral electrónico a través del mecanismo que para tales efectos establezca el Instituto, relativo a los requerimientos de colaboración para la intervención de comunicaciones**

		privadas, geolocalización ,en tiempo real, de equipos de comunicación móvil, así como la conservación y acceso a datos conservados. **Dicho informe deberá contener y observar lo siguiente:** **I. El número total y por autoridad, de requerimientos de colaboración para la intervención de comunicaciones privadas, de localización geográfica en tiempo real, de conservación de datos y de acceso a datos conservados de comunicaciones, desglosando las recibidas, entregadas y no entregadas mensualmente, así como las que fueron recibidas previa autorización judicial y las que se realizaron en los casos de excepción, de las cuales deberá indicarse el número de requerimientos excepcionales cuya ratificación por parte del Juez de control fue notificada, utilizando el formato que defina el Instituto.** **II. El número total y por autoridad de avisos de notificación de medidas excepcionales en los términos en que señala el presente artículo.** **La información estadística contenida en los informes trimestrales será publicada en el portal de Internet del Instituto en términos de lo establecido en la Ley General de Transparencia y**

		Acceso a la Información Pública y demás disposiciones aplicables. **Los concesionarios y autorizados de telecomunicaciones y, en su caso, los proveedores de aplicaciones, contenidos y servicios en Internet, colaborarán con la autoridad judicial federal para la notificación de personas objeto de medidas de intervención de comunicaciones privadas, geolocalización, en tiempo real, de equipos de comunicación móvil y el acceso a datos conservados, en los términos que señale la autoridad judicial federal y las leyes correspondientes.** **En caso de que los sistemas de conservación de datos hayan sido vulnerados y los Datos Personales de las personas usuarias finales se encuentren comprometidos, los Concesionarios y Autorizados deberán notificar inmediatamente a la Agencia, a la Secretaría Anticorrupción y Buen Gobierno y a las personas usuarias afectadas e indicará las medidas que la persona usuaria podrá tomar para disminuir o contrarrestar cualquier afectación derivada de esta vulneración.**
IV. Contar con un área responsable disponible las veinticuatro horas del día y los trescientos sesenta y cinco días del	**V.** Contar con un área responsable disponible las veinticuatro horas del día y los trescientos sesenta y cinco días del	**V.** Contar con un área responsable disponible las veinticuatro horas del día y los trescientos sesenta y cinco días del

año, para atender los requerimientos de información, localización geográfica e intervención de comunicaciones privadas a que se refiere este Título. Para efectos de lo anterior, los concesionarios deberán notificar a los titulares de las instancias a que se refiere el artículo 189 de esta Ley el nombre del responsable de dichas áreas y sus datos de localización; además deberá tener facultades amplias y suficientes para atender los requerimientos que se formulen al concesionario o al autorizado y adoptar las medidas necesarias. Cualquier cambio del responsable deberá notificarse previamente con una anticipación de veinticuatro horas;	año, para atender los requerimientos de información, localización geográfica e intervención de comunicaciones privadas a que se refiere este Título. Para efectos de lo anterior, los concesionarios deberán notificar a los titulares de las instancias a que se refiere el artículo **159** de esta Ley el nombre del responsable de dichas áreas y sus datos de localización; además deberá tener facultades amplias y suficientes para atender los requerimientos que se formulen al concesionario o al autorizado y adoptar las medidas necesarias. Cualquier cambio del responsable deberá notificarse previamente con una anticipación de veinticuatro horas;	año, para atender los requerimientos de información, localización geográfica e intervención de comunicaciones privadas a que se refiere este Título. Para efectos de lo anterior, los concesionarios deberán notificar a los titulares de las instancias a que se refiere el artículo **159** de esta Ley el nombre del responsable de dichas áreas y sus datos de localización; además deberá tener facultades amplias y suficientes para atender los requerimientos que se formulen al concesionario o al autorizado y adoptar las medidas necesarias. Cualquier cambio del responsable deberá notificarse previamente con una anticipación de veinticuatro horas;
		Transitorios **VIGÉSIMO OCTAVO.** El artículo 160, fracción II entrará en vigor a los dos años posteriores a la publicación del presente Decreto. Mientras tanto se estará a lo que dispone la ley vigente. La Agencia actualizará los Lineamientos de Colaboración en Materia de Seguridad y Justicia dentro de los 180 días posteriores a la publicación del presente Decreto.

R3D
Red en Defensa de los Derechos Digitales

Registro de personas usuarias de telefonía

Los artículos 8, fracción LXIV y 160, fracción IV proponen nuevamente la creación de un registro de todas las personas usuarias de telefonía móvil. Aunque en esta legislación no desarrolla en qué consiste este registro, en otras iniciativas que se encuentran siendo procesadas por el Congreso se advierte que se pretende asociar cada línea telefónica a una identificación oficial, la CURP o el RFC en caso de personas morales El registro se contempla como una condicionante para el acceso a la telefonía móvil e incluso plantea la cancelación de todas las líneas telefónicas vigentes que no sean registradas.

Este registro representa una reedición del fallido Registro Nacional de Usuarios de Telecomunicaciones (RENAUT), creado en 2008 durante el gobierno de Felipe Calderón y eliminado en 2011, después de que su base de datos fue vulnerada y puesta a la venta en el mercado negro. Lejos de incidir en la reducción del crimen, durante la operación del RENAUT, el delito de extorsión aumentó 40 por ciento y el de secuestro, 8 por ciento.

Esta iniciativa también emula al Padrón Nacional de Usuarios de Telefonía Móvil (PANAUT), aprobado en 2020 por el gobierno de Andrés Manuel López Obrador y declarado inconstitucional por la Suprema Corte de Justicia de la Nación (SCJN) en 2022, incluyendo por los Ministros Arturo Zaldívar y Loretta Ortiz.

Como ha sido demostrado anteriormente y reconocido por la SCJN, no existe evidencia de que el registro obligatorio de líneas telefónicas reduzca la actividad criminal. Por el contrario, resulta inverosímil creer que la delincuencia utilice teléfonos registrados a su nombre para llevar a cabo actos delictivos.

Además, el Padrón sería eludible sin dificultad mediante las múltiples técnicas y mecanismos actualmente utilizados 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, el enmascaramiento de números telefónicos, entre otros, por lo que podría incriminarse fácilmente a personas inocentes.

El registro masivo, obligatorio y centralizado de personas usuarias de telefonía móvil también pone a la población en un estado de riesgo frente al acceso no autorizado por vulneraciones de datos o de actos de corrupción cometidos por autoridades federales, estatales, e incluso municipales, quienes tendrían acceso al registro sin control judicial ni supervisión de una autoridad de protección de datos profesional y autónoma –tras la desaparición del INAI– y sin que se contemplen otras salvaguardas como el derecho de notificación a las personas afectadas.

Lo anterior resulta aún más grave cuando se toma en cuenta la frecuente colusión entre las autoridades municipales y estatales con la propia delincuencia, la cual, de obtener acceso al registro, podrá utilizar la información registrada para cometer delitos en contra de la población.

Así mismo, el condicionamiento del acceso a la telefonía móvil a la entrega de datos personales —además de constituir una violación al principio de consentimiento, según ha establecido la SCJN— vulnera el derecho de acceso a las tecnologías de la información y comunicación, reconocido en la Constitución, en tanto obstaculiza de manera innecesaria el acceso a Internet, lo cual impacta particularmente a poblaciones en situación de pobreza y poblaciones rurales.

Por todo lo anterior, se propone la eliminación de la facultad de la Agencia de expedir lineamientos para el registro de usuarios del servicio móvil y la correspondiente obligación de los concesionarios y autorizados de permitir el acceso a autoridades (indefinidas) la consulta de dicho registro.

LEY VIGENTE	INICIATIVA	PROPUESTA
(Sin correlativo)	**Artículo 8.** Para el ejercicio de sus atribuciones corresponde a la Agencia: **LXIV. Expedir los lineamientos para el registro de usuarios del servicio móvil que estará a cargo de los concesionarios y, en su caso, autorizados de dicho servicio y será de observancia obligatoria;**	**Artículo 8.** Para el ejercicio de sus atribuciones corresponde a la Agencia: **LXIV.** ~~**Expedir los lineamientos para el registro de usuarios del servicio móvil que estará a cargo de los concesionarios y, en su caso, autorizados de dicho servicio y será de observancia obligatoria;**~~
(Sin correlativo)	**Artículo 160.** Los concesionarios de telecomunicaciones y, en su caso, los autorizados **que determine la Agencia**, deberán: **IV. Permitir a las autoridades a que se refiere el artículo 159, la consulta al**	**Artículo 160.** Los concesionarios de telecomunicaciones y, en su caso, los autorizados **que determine la Agencia**, deberán: **IV.** ~~**Permitir a las autoridades a que se refiere el artículo 159, la consulta al**~~

	registro de usuarios del servicio móvil, conforme a los criterios y condiciones que establezca la Agencia en los lineamientos que emita para tal efecto;	~~**registro de usuarios del servicio móvil, conforme a los criterios y condiciones que establezca la Agencia en los lineamientos que emita para tal efecto;**~~