INICIATIVA QUE REFORMA Y ADICIONA DIVERSAS DISPOSICIONES DE LA LEY FEDERAL DE TELECOMUNICACIONES Y RADIODIFUSIÓN Y DEL CÓDIGO PENAL FEDERAL, SUSCRITA POR EL DIPUTADO SILVANO GARAY ULLOA E INTEGRANTES DEL GRUPO PARLAMENTARIO DEL PT

El suscrito diputado **Silvano Garay Ulloa** , del Grupo Parlamentario del Partido del Trabajo en la LXIV Legislatura de la Cámara de Diputados del Congreso de la Unión, con fundamento en lo que se dispone en los artículos 71, fracción II, de la Constitución Política de los Estados Unidos Mexicanos, y 6, numeral 1, fracción I, y 77 del Reglamento de la Cámara de Diputados, someto a la honorable Cámara de Diputados la presente **iniciativa con proyecto de decreto por la que se reforma la Ley Federal de Telecomunicaciones y Radiodifusión a fin, de conformar una lista negra consolidada de los números de identificación internacional (IMEI) que han sido reportados como robados o que son utilizados para las distintas modalidades de extorsión. Dicha lista se convertirá en una base de datos que permitirá crear una app que emita alerta de peligro o precaución a los usuarios de telefonía celular. De igual forma, se reforma el Código Penal para tipificar la venta ilegal de esta base de datos; la comercialización de los aparatos móviles de comunicación y sus partes; así, como la clonación o alteración del IMEI** , con base en la siguiente:

Exposición de Motivos

El robo de celulares en el mundo se ha convertido en un problema muy común, pero difícil de erradicar. Es un fenómeno que ha sido reconocido por diversas naciones. Esto se deriva de que los teléfonos móviles se han convertido en un artículo accesible para grandes sectores de la población. El teléfono móvil es un objeto bien identificado, cuyo valor tiende a ser bien comprendido en cualquier sociedad.[1] Es un crimen que involucra dos tipos de delitos: el robo del aparato por sí mismo o por los datos que contienen dichos dispositivos.

Además, derivado del simple hecho de que los criminales tienen datos básicos (o no) de los números telefónicos, se ha ampliado la presencia de fraude. Éste puede tomar muchas formas, y los aparatos de comunicación móvil se utilizan para el llamado fraude de servicios (de identidad o de dinero móvil), el spam móvil (propaganda masiva) y, cada vez más, el fraude por "ingeniería social" (por ejemplo, Phishing, SMiShing o Vishing), mediante el que se engaña a la víctima para que revele información sensible sobre su persona y los servicios que consume, sin que se dé cuenta de que su seguridad está en peligro; se recurre a la manipulación para incitar a las personas a tomar medidas peligrosas, tales como divulgar información personal o contraseñas. Una vez que tienen acceso a dicha información privada, los delincuentes pueden registrarla y utilizarla para cometer otros delitos como el fraude bancario.

En el año 2013, de acuerdo con Fiscal General de Estados Unidos, Eric Holder, el delito en ese país había aumentado considerablemente en relación con el año anterior: se calculó en aproximadamente 3,1 millones.[2] En ese mismo año, a uno de cada tres europeos le robaron el teléfono; en Corea del Sur, el hurto se incrementó cinco veces entre 2009 y 2012. Y, en Colombia los ladrones robaron más de un millón de aparatos en 2013.

En Latinoamérica, es precisamente Colombia, el país que encabeza la lista con el mayor número de robos de teléfonos celulares. Según la Asociación de la Industria Móvil (Asomóvil) que agrupa los tres tele-operadores más importantes de esa nación, en el año 2017, cada dos minutos un celular era robado; más de 1.2 millones de dispositivos móviles, la cantidad más alta en toda Sudamérica. Esta cifra alta se explica, en parte, por un detalle: de todos los celulares robados, solo el 4 por ciento denuncia el hecho para que bloqueen el terminal. Esto permite que el resto pueda ser activado nuevamente y puesto en venta de regreso en las calles; o, como ocurre frecuentemente, en otros países. De hecho, la Policía estima que el 30 por ciento se vende en el mercado interno y el 70 por ciento se exporta.[3]

De acuerdo con la Asociación Nacional de Telecomunicaciones (ANTEL), en México los reportes por robo o extravío de dispositivos de teléfonos celulares ha ido incrementándose. En el año 2012, hubo 156 mil 681 reportes, en el año 2013, 341 mil 740; en el año 2014, 442 mil 284; en el año 2015, 609 mil 547; en el año 2016, 892 mil 316;

y, en el 2017, bajo un poco con 786 mil 97. Es evidente que estos datos podrían verse incrementados porque muchos usuarios no reportan que les hayan robado o sustraído sus celulares.[4] De igual forma, debe considerarse que existe una mayor cobertura de personas que tienen celular y por lo tanto, hay mayor probabilidad de robo. De acuerdo con Ernesto Piedras, director de *The Competitive Intelligence Unit* (The CIU) en muchos casos, los mexicanos que son víctimas de robo de celulares no hacen la denuncia correspondiente, ni realizan los métodos de bloqueo pertinentes de los dispositivos móviles.[5]

Un dato más cercano a lo que realmente ocurre sobre el ascenso de este delito, lo presenta la Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (Envipe) de 2019 del Instituto Nacional de Estadística y Geografía (Inegi) que informó que durante el 2018 se cometieron 9.4 millones de asaltos en las calles o en el transporte público lo cual representa una tasa de 10 mil 775 robos por cada 100 mil habitantes. Lo interesante aquí, es que el 55.5 por ciento del total de los casos de lo robado fueron teléfonos celulares.[6]

También con datos de esta Encuesta en 2018 se calculó que en la Ciudad de México al día son robados 1972 aparatos móviles; lo que implica un daño patrimonial de 9 millones 800 mil pesos diarios, considerando un precio medio de 5 mil pesos por teléfono.

El robo de celulares se mantiene como el delito más común en la capital del país, debido a que se asocia a los dos tipos de asalto más lucrativos: el de transeúnte y en el transporte público. En el 2015, la Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública estableció que el 53 por ciento de los asaltos a transeúntes es para robarles el teléfono celular.[7] La razón, es que pueden obtener más dinero al revenderlos en el mercado negro, en relación con la cantidad que cada persona puede pagar y que fomenta este círculo al comprar productos robados.

En noviembre del presente año, Centro Nacional de Información (CNI)[8] órgano del gobierno mexicano que integra y administra las bases de datos criminalísticas y del personal de seguridad pública identificó 11 mil 960 números telefónicos utilizados para extorsionar, desde los que se realizaron 18 mil 855 llamadas extorsivas, en su mayoría desde teléfonos celulares, en el primer semestre del año. 18 entidades del país concentran esta problemática, ubicada como del fuero común, entre las que destacan Puebla, Guanajuato, Hidalgo, Quintana Roo, Sonora, Veracruz, Chihuahua y Tabasco. Este ilícito aumentó 29.6 por ciento en septiembre de este año, si se compara con el mismo mes del año pasado.[9]

El titular de dicho Centro, David Pérez Esparza, estableció que ya se prepara la creación de una base de datos nacional de números extorsivos, la cual va a ser alimentada por el número de denuncias anónimas al 089 a través de Cómputo, Comunicaciones y Contacto Ciudadano de los estados. El delito en su mayor parte se enfoca a la reventa, pero también es utilizado por bandas de criminales que realizan fraudes y extorsiones.

En la última reunión Regional de noviembre de la Conferencias de Secretarios de Seguridad Pública y Seguridad Pública Municipal de la Zona Centro, en la Ciudad de México, el secretario de Seguridad federal, Alfonso Durazo, reconoció que las extorsiones telefónicas siguen como un tema prioritario para la seguridad pública de México y, por ello, se requieren acciones inmediatas, tales como la consolidación de una base de datos nacional.[10]

Por otra parte, en opinión de Salvador Guerrero Chiprés, presidente del Consejo Ciudadano de Seguridad Pública y Procuración de Justicia de la Ciudad de México, en el presente año, a nivel nacional se tiene detectado 5.7 millones de delitos de fraude y extorsión. En la Ciudad de México de enero a noviembre se registraron 31 mil 331 denuncias asociadas a extorsión, un promedio mensual de 3 mil 42. Del total, 27 mil 25 fueron “tentativas de extorsión” y 2 mil 207 se consumaron en los primeros 10 meses de este año, el daño patrimonial causado a las víctimas se valoró entre 8 mil 500 pesos, pero llegaron a presentarse caso, como en el que pagaron 100 mil dólares por el pago de este delito. Han sido identificados 150 mil números telefónicos dedicados a la extorsión.[11]

En opinión de Rosa Icela Rodríguez, secretaria de Gobierno de la Ciudad de México, las llamadas de extorsión se efectúan desde diversos estados del país y principalmente desde los reclusorios Norte, Oriente y el Penal de Santa Martha. Una de las extorsiones que ha ido en ascenso, es la denominada "La Patrona", en la que llaman a los domicilios con las trabajadoras del hogar y se hacen pasar por familiares de los dueños, dicen hablar a su nombre, porque ellos están en problemas y piden que les entreguen en una maleta todos los artículos de valor que tengan.

En el denominado Estudio Estadístico del número de terminales móviles y de llamadas móviles y de casetas telefónicas que operan dentro de una muestra de penales en el país[12] presentado por un Grupo de Trabajo de concesionarios participantes en el Comité Especializado de Estudios e Investigaciones en Telecomunicaciones, se analizaron siete penales en distintas regiones del país con características diversas. Los operadores móviles dieron seguimiento al estudio de 2016 generando información para cada uno de ellos durante tres semanas consecutivas en 2017. Los resultados son tan similares al año anterior que no vale la pena el costo de una "nueva fotografía" adicional a la que se tomó en ese año. En el caso de la telefonía fija, el análisis incluye 4 penales donde se estudió la presencia de equipos móviles, y tres adicionales sobre los que hay datos disponibles para este estudio.

Con una población estimada de 20 mil reos en los siete penales, la investigación arroja una variación semanal en el número de equipos y de IMSI (Identidad Internacional de Abonado Móvil, por sus siglas en inglés), utilizados para hacer llamadas. Se encontraron 947 equipos terminales "sospechosos" durante la primera semana de levantamiento de datos, relacionados con 2 mil 259 IMSI; durante la segunda semana, se identificaron 1,003 equipos con 2 mil 401 IMSIs asociados; y, para la tercera semana se hallaron 951 terminales utilizando 2 mil 266 IMSI.

Relevantemente, se concluye en este estudio que el uso generalizado de equipos dentro de los siete penales, relacionados a la radio base de al menos una empresa, evidencia la **inutilidad de los equipos bloqueadores de señal instalados,** con interferencias que afectan a los usuarios y a la calidad del servicio. Es importante señalar que detectaron equipos que utilizaron solo un IMSI y que sin embargo registran un elevado índice de intensidad de llamadas. Durante la primera semana, 24 de estos equipos realizaron 3 mil 932 llamadas, con un índice promedio de 164 llamadas por equipo; durante la segunda semana, se registraron 4 mil 950 llamadas y un índice de 138 llamadas; y, en la tercera semana 9 mil 879 llamadas con un índice de intensidad de 173 llamadas por equipo.

En este estudio se afirma que, al analizar la información de cada uno de los penales durante tres semanas consecutivas, permitió identificar otros patrones de comportamiento y el grado de actividad delictiva en los distintos recintos. Por ejemplo, en el recinto penitenciario identificado como "B" se encuentra un número amplio de equipos, sin embargo, realizan en promedio un volumen menor de llamadas pues su índice de intensidad es muy bajo. Aquí destaca el que operen tantos equipos desde el penal. En el recinto "E" hay un número considerable de equipos, 472 durante la primera semana y 522 la segunda y la tercera; el índice de intensidad es el segundo más alto de los 7 penales con 91 llamadas por equipo durante la primera semana, 76 durante la segunda, y 74 en la tercera. Como resultado el total de llamadas cada semana es de 40 mil 496 en promedio. El caso más llamativo es el recinto "C", donde se hallaron pocas terminales sospechosas, que en ningún caso rebasan los 48 en una semana. Sin embargo, ahí se registran los mayores índices de intensidad con 180, 148 y 160 llamadas por equipo durante cada una de las 3 semanas analizadas; esto es, el doble del índice reportado en el inciso anterior, aunque el total de equipos es solo el 10 por ciento del total que operan en el recinto B.

Pero lo que es sumamente interesante es que, a nivel individual, el problema se sale de control. En la segunda semana, "18 usuarios realizan más de 300 llamadas y hay 9 usuarios con más de 500 llamadas cada uno. El usuario que más llamadas registró llegó a 2,457 en el periodo de muestreo." En la tercera semana: "**5 usuarios generaron más de 500 llamadas cada uno, 2 usuarios realizaron más de mil llamadas. El equipo que más llamadas registró fue de 3 mil 537 en el periodo de muestreo utilizando 2 IMSI** ." El conjunto de equipos sospechosos en los 7 penales, cuyo número varió cada semana, fueron la fuente de 219 mil 700 llamadas en el periodo. Si se anualiza esta estadística, arroja una cantidad de 3.7 millones de llamadas.[13]

En esta investigación se concluyó que: hay una cantidad apreciable de equipos sospechosos en el conjunto de los penales de la muestra; y que incluso donde hay pocos equipos puede ocurrir una cantidad de llamadas con propósitos delictivos a lo largo del día, afectando a los usuarios y la calidad del servicio por las interferencias que generan los bloqueadores de señal instalados. “En este sentido, para los concesionarios es clave lo señalado en el artículo 15 fracción XLIV de la Ley Federal de Telecomunicaciones y Radiodifusión (LFTyR); y es especialmente importante el papel que pueden desempeñar las autoridades penitenciarias, para llevar a cabo la adecuación de los equipos bloqueadores de señal a las especificaciones técnicas establecidas en la Disposición Técnica IFT-010-2016, en el menor tiempo posible, a fin de que se atienda lo previsto en el Artículo 190 de la Ley Federal de Telecomunicaciones y Radiodifusión, en especial la fracción VIII que requiere la colaboración de Concesionarios y Autorizados para la cancelación o anulación de señales celulares en los establecimientos penitenciarios, así como en el monitoreo de la funcionalidad u operatividad de los correspondientes bloqueadores de señales”.

Los concesionarios del Comité Especializado urgen a que las autoridades penitenciarias diseñen un programa que reduzca al máximo la introducción de equipos terminales y de IMSI en los recintos penitenciarios; e insiste en la importancia de que los equipos bloqueadores de señal se adecuen a las especificaciones técnicas de la Disposición Técnica IFT-10-2016 en el menor tiempo posible y operen conforme a las Bases Técnicas para la Instalación y Operación de Sistemas de Inhibición, a fin de alcanzar los objetivos de política pública establecidos en los documentos mencionados.

Recientemente, la Ciudad de México y el Consejo Ciudadano de Seguridad Pública y Procuración de Justicia de la Ciudad de México emprendieron una iniciativa para operar una aplicación telefónica denominada, “No Más Extorsiones” para las plataformas Ios y Android, la primera tiene cargado los números detectados como extorsionadores e inmediatamente bloquea la llamada, en la segunda, lanza una alerta para no contestar a ese número marcado. Es decir, bloquea y manda una alerta al número celular que recibe la llamada para evitar que se cometa dicho ilícito. Cabe señalar que, en muchas ocasiones, dichas llamadas se efectúan desde provincia. Esta iniciativa, se inscribe dentro del conjunto de acciones que se ha instrumentado a nivel mundial por los gobiernos y las concesionarias del servicio.

En este contexto, sirve para fines del diseño de esta iniciativa, la descripción de las acciones que se han emprendido en el mundo para palear el fenómeno de los aparatos móviles asociados a actividades delincuenciales, el incremento del hurto de celulares para su venta y/o el uso indebido de los datos que contienen estos aparatos.

De acuerdo con la Asociación Nacional de Telecomunicaciones, Anatel, en el documento denominado, “Estudio e Investigación para el desarrollo de nuevas medidas tecnológicas que permitan inhibir y combatir la utilización de equipos de telecomunicaciones para la comisión de delitos”,[14] en el año 2012, los cuatro operadores móviles del mercado mexicano que operan redes públicas de telecomunicaciones, recibieron en conjunto 39 mil 956 oficios de diversas autoridades judiciales a lo largo y ancho del país. En ellos se incluyó la consulta sobre 82 mil 721 números de telefonía celular para la investigación de delitos. En dicho documento, se afirma que los integrantes de dicha Asociación respetan literalmente la fracción XIV del artículo 44 de la Ley Federal de Telecomunicaciones y Radiocomunicaciones (LFTYR) que establece la obligación que tienen de bloquear de manera inmediata las líneas de comunicación móvil que funcionen bajo cualquier modalidad, y hayan sido reportadas por los clientes como robadas o extraviadas. Esto puede lograrse por la existencia de un software denominado “Registro de Identidad de Equipo” (EIR, por sus siglas en inglés), que facilita la identificación y bloqueo de números telefónicos específicos, mismo que se activa a través del dispositivo contenido en cada equipo de teléfono celular y que es conocido como “**Identidad Internacional de Equipo Móvil** ” (IMEI, por sus siglas en inglés).

El IMEI es el código pregrabado en los equipos terminales (celulares) que utilizan tecnología GSM y/o UMTS. Este código tiene la enorme ventaja de identificar al aparato unívocamente a nivel mundial, y es transmitido por el mismo a la red, de manera automática, al conectarse a ésta. Este código permite, entre otras cosas, que los Operadores

Móviles que prestan el servicio conozcan quién y desde dónde se hace la llamada, así como el equipo o terminal telefónica en que se hizo. La empresa operadora puede usar **el IMEI para verificar el estado del aparato mediante la base de datos EIR, a la que se ha hecho referencia. Dentro de esta base de datos existen dos listas de IMEI: la blanca y la negra.**

En México, el Instituto Federal de Telecomunicaciones instrumentó en su portal de internet, una aplicación para que los usuarios puedan consultar el IMEI de sus dispositivos móviles se encuentra reportado como robado.

La lista blanca es la lista de números de IMEI respecto de equipos terminales móviles que han sido acreditadas para el uso de redes GSM y/o UMTS. Pero, la lista negra incluye los números IMEI de equipos terminales móviles que fueron bloqueados en el EIR de un determinado concesionario, y que han sido cargados a la base de datos.

La lista negra incluye por tanto todos los números que han sido reportados por los clientes como robados o extraviados, a los cuales se les suspende el servicio de manera permanente. Se supone que los datos se mantienen en el sistema cuando menos durante 18 meses.

Las concesionarias pueden rastrear las llamadas de teléfono con voz, SMS y los datos como Whatsapp, correo electrónico, navegación, etc. se pueden interceptar. De forma ilegal, a través de escuchas radiofónicas no permitidas en el caso de voz o a través de los que se denomina un MITM (*Man in the Middle).* Un malhechor coloca una red inalámbrica maliciosa abierta y te conectas. En su servidor malicioso puede ver que recursos de Internet estás utilizando, webs, aplicaciones y contraseñas en texto plano, es decir, legible y apropiarse a posteriori, de lo que quiera.

También se pueden interceptar tanto llamadas como datos si se cuentan con una orden judicial motivada que justifique la vulneración del derecho del investigado al secreto de las comunicaciones por una investigación. Se hace a través del famoso sistema de interceptación de las comunicaciones, "SITEL" de la policía. De esta forma se podrán aportar a posteriori pruebas para un juicio que se obtengan a través de la interceptación pero siempre supervisado por el Juez.

El dispositivo físico tiene contenida la información en una base de datos a la cual se accede a través de diferentes medios ya sea por una extracción física o lógica de la información. Aunque no se pueda acceder al contenido si el software del teléfono (es sistema operativo) está dañado, o no hay una forma de hacerlo con herramientas forenses, se puede a través de la extracción del método "chip off" de la memoria NAND del microprocesador del teléfono o circuito integrado. Es costoso, difícil y se dañar el chip pero se puede. Ese chip está comunicado con el teléfono y para acceder a su contenido, necesitas saber la clave de bloqueo y acceso al terminal.[15]

De acuerdo con la investigadora Marianne Díaz, existe una tendencia global de las naciones por regular las telecomunicaciones de modo más estricto, bajo la justificación de combatir el terrorismo y el crimen organizado; no obstante, esto va en contra de los estándares internacionales de derechos humanos.[16] Ella realizó un examen de la legislación vigente en materia de retención de datos y registro de teléfonos móviles en Argentina, Brasil, México, Perú y Chile (con énfasis en este último), en relación con los principios y parámetros de derechos humanos que rigen las restricciones en el acceso a las comunicaciones y la libertad de expresión.

Es importante señalar que el derecho de libertad de expresión que se asocia con las llamadas en los móviles se contrapone con el derecho al anonimato; las tecnologías de la información, pueden generar que los usuarios queden al descubierto en sus pláticas, relaciones o datos. El anonimato, ha sido valorado de manera importante por las Naciones Unidas como una garantía a la libertad de expresión y al libre flujo de ideas en el contexto de una sociedad. Por esta razón, las concesionarias deben tener límite al momento de poder acceder a los datos de los usuarios.

Se enfatiza la confrontación del derecho a la expresión y a la protección a la intimidad. En el balance de esta tensión, la Convención Americana sobre Derechos Humanos contempla los requisitos mínimos que debe contener cualquier restricción a la libertad de expresión en la región. Dichas medidas deben cumplir con cinco requisitos: (1) legalidad, (2) búsqueda de una finalidad imperativa, (3) necesidad, idoneidad y proporcionalidad de la medida en relación con el fin perseguido, (4) garantías judiciales, y (5) satisfacción del debido proceso. Para Marianne Díaz, **las legislaciones latinoamericanas en materia de retención de datos y registro de tarjetas SIM resultan inconsistentes en el cumplimiento de estos parámetros.**

Estos mismos estándares se encuentran desarrollados en los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, elaborados con el consenso de la sociedad civil para determinar la legitimidad de las medidas de vigilancia en el contexto de las comunicaciones. El Consejo de Derechos Humanos de la ONU ha reconocido el riesgo que existe sobre la mera posibilidad de que la información relativa a las comunicaciones sea capturada. La retención de datos obligatoria por parte de terceros, en la que los gobiernos requieren que las compañías telefónicas y los proveedores de servicios de internet almacenen los datos y metadatos relativos a las comunicaciones de sus clientes no es considerada por Naciones Unidas como necesaria o proporcional.

En varios países, las medidas son tomadas sorteando el principio de legalidad, a través de una orden ejecutiva, poniendo en riesgo garantías mínimas del sistema democrático. En otros, se permite el acceso por parte de los órganos públicos a los datos sin la garantía de una orden judicial, lo cual violenta el debido proceso y ubica a los ciudadanos en un estado de indefensión que afecta gravemente sus derechos humanos.

Como relata la investigadora Marianne Díaz, una tendencia reciente ha incluido mecanismos de registro sobre uno de los números que identifica a cada teléfono móvil, como el denominado IMEI. Las medidas de retención de datos carecen de estándares mínimos que pudieran contribuir a profundizar una relación de desequilibrio de poder entre los usuarios, las compañías de telefonía móvil y los estados; un desequilibrio que afecta la capacidad de los ciudadanos para exigir el cumplimiento de sus derechos fundamentales.

No obstante, existe actualmente una marcada tendencia global hacia la expansión y puesta en práctica de normativas prescriptivas que obligan al requerimiento y retención de una mayor cantidad de datos al usuario de teléfonos móviles por parte de las compañías prestadoras del servicio. La ola de implementación de registros obligatorios de tarjetas SIM se inicia en 2003, con las normativas de Brasil, Alemania y Suiza **y para 2016 alrededor de 90 países requerían registro obligatorio a los usuarios de tarjetas SIM.**

Es importante mencionar que para poder comprar un chip (tarjeta SIM) en Europa solo se necesita una identificación oficial esto aplica para turistas, residentes o nacionales. Los costos varían según el país y el lugar de venta. Se maneja la modalidad de plan y prepago. En los últimos años se ha implementado una nueva manera de operar el servicio de telefonía (chips online), servicio disponible en 71 países. En Estados Unidos, sólo se pide una identificación para la adquisición de un equipo telefónico nuevo. En caso de querer adquirir solo el chip se puede adquirir en la diversidad de tiendas telefónicas reguladas que sí piden identificación oficial y también se pueden encontrar en negocios no regulados a un menor precio y sin necesitar algún tipo de identificación oficial.

Ahora bien, hay dos mecanismos para la prestación del servicio, que puede ser post-pagado o prepagada, este último caso conforma un alto porcentaje de la totalidad del mercado móvil, alcanzando hasta el 90 por ciento en países como México. El avance de las tecnologías, ha llevado al crecimiento en el número de funciones que estos dispositivos, que pueden acumular un número mucho mayor de datos, no solo de la comunicación propiamente dicha, sino de la ubicación del usuario, de su historial de navegación y un sinnúmero de otros puntos de información.[17]

A pesar de la amplitud con la cual este tipo de medidas siguen siendo implementadas hoy en día, existe también evidencia de su eliminación en algunos países. La aplicación efectiva de estas medidas en diversos países del globo

ha demostrado la inexistencia de un vínculo claro entre las medidas de registro obligatorio y la prevención del terrorismo o del crimen organizado (*Privacy International* , 2004). Un caso emblemático a nivel internacional, estuvo centrado en nuestro país, que en 2009 modificó su legislación procesal penal nacional y de telecomunicaciones, con la finalidad de crear el Registro Nacional de Usuarios de Telefonía Móvil (Renaut), el cual obligaba a que los proveedores de servicios de telecomunicaciones llevaran un registro en el cual cada teléfono celular estuviera asociado de manera clara a un ciudadano, siendo este registro accesible a petición del Ministerio Público, que tendría acceso a datos como la geolocalización del dispositivo o el contenido de las comunicaciones. Sin embargo, estas disposiciones se derogaron apenas tres años después, puesto que, en lugar de disminuir, el porcentaje de comisión de los delitos en cuestión aumentó dentro de la vigencia del régimen.

En nuestro país, el mencionado Renaut estableció el registro obligatorio de las SIM; pero a tres años de su implementación se incrementó el robo de equipos. Luego de consultas a la industria, la academia y las ONG, el programa de registro Renaut cesó sus operaciones en el año 2012. La base de datos fue desactivada y se dio por perdida la importante inversión financiera realizada por los operadores de redes y las autoridades. Para abordar la situación específica del mercado mexicano, se incorporó un programa alternativo a la Ley de Telecomunicaciones y Radiodifusión, en vigencia desde 2014.

Con el Renaut los delincuentes registraban las líneas con la clave de terceros y por tal seguían impunes, entre otras muchas debilidades de la figura y para colmo la base de datos se filtró y entonces tuvo que ser eliminado el registro y destruida toda la información recabada; siendo alrededor de 98 millones de números telefónicos ligados a una CURP de un supuesto propietario los que fueron destruidos en un acto público encabezado por la Secretaría de Gobernación federal en el año de 2012.

También en el año 2014 el Tribunal de Justicia de la Unión Europea declaró inválida la directiva sobre conservación de datos, normativa que buscaba armonizar las disposiciones de los Estados miembros con respecto a la conservación de datos generados o tratados por los proveedores de los servicios de telecomunicaciones.

Sin duda alguna, el registro y retención de la información asociada a las comunicaciones móviles plantea una serie de consideraciones en torno a la privacidad y la intimidad de los ciudadanos, quienes pueden verse afectados por diversos factores: la adquisición, manejo y almacenamiento de los datos, las posibilidades de los ciudadanos de controlar la información que sobre ellos exista en manos de terceros, y la seguridad y protocolos en torno al procesamiento de dicha información.

El registro obligatorio de tarjetas SIM suele tener por finalidad principal la regulación y control de las transacciones anónimas. En general, los organismos dedicados al cumplimiento de la ley tienden a mostrar preocupación acerca del vínculo aparente entre el mercado anónimo de telefonía móvil prepagada y las actividades criminales y terroristas. No obstante, **la existencia real de este vínculo es dudosa, siendo el caso que dos tercios de los terroristas operan bajo su identidad real, y el 80 por ciento de los países que han sido más afectados por actividades terroristas ya tienen sistemas nacionales de identidad** (un tercio de los cuales utiliza incluso tecnologías biométricas). No existe evidencia alguna de que la implementación de dichos sistemas nacionales de identidad haya tenido ningún tipo de influencia sobre la actividad terrorista.[18] En Canadá es considerado una invasión de la privacidad.

La investigadora concluye que lo más probable es que los criminales adopten una táctica alternativa, ya sea clonar ilícitamente las tarjetas SIM de terceros, utilizar SIM extranjeras en modalidad de roaming o adoptar tecnologías de telefonía satelital y de internet (Donovan & Martin, 2014).

No obstante, existe un cierto consenso sobre los beneficios de la utilización del IMEI (*International Mobile Equipment Identity*) que es un número conformado por quince dígitos decimales que permiten identificar la marca y modelo de un dispositivo móvil, así como su número serial. A través del código IMEI, un operador móvil puede

rastrear la utilización de un dispositivo específico con mucha rapidez, si es usado en la misma red móvil. El principal argumento empleado para defender la imposición de medidas de registro obligatorio de IMEI suele ser la persecución del delito de robo de teléfonos. Este número es la base para la integración de las llamadas listas negras y blancas.

En la mayoría de los países predomina el sistema de lista negra para el registro de IMEI. En Guatemala, por ejemplo, se creó en 2013 la Ley de Equipos Terminales Móviles (Decreto 8-2013), que estableció la obligación por parte de las empresas operadoras de telefonía móvil de dar de baja las líneas que los usuarios no hubieran registrado en un plazo de tres años, que se cumplió el 8 de octubre de 2016. Otros países han adoptado sistemas de lista blanca parcial o fragmentada: en Ecuador, desde 2014, es obligatorio que todos los teléfonos móviles que ingresen al país por vía aérea sean registrados en una base de datos llevada por la Superintendencia de Telecomunicaciones del Ecuador (Supertel) y el Servicio Nacional de Aduana del Ecuador (Senae). Para que un dispositivo pueda ser registrado, la marca y modelo debe estar homologada en el Ecuador y no estar reportado por robo en Ecuador, Colombia, Perú y Bolivia

En Colombia, el Decreto 1704 rige la medida de retención de datos de las comunicaciones en el contexto de la investigación criminal, mientras la Ley 1621 de 2013 hace lo propio con respecto a actividades de inteligencia. El Decreto 1704 exige a los proveedores de servicio conservar la información de las comunicaciones de sus clientes que permita saber su geolocalización en tiempo real. El Decreto 1630, de mayo de 2011, crea un registro nacional de teléfonos móviles, a través de la adopción de dos bases de datos. La base de datos negativa contiene los IMEI de los dispositivos que hayan sido reportados como hurtados o extraviados, tanto en Colombia como en el extranjero.

En Brasil en el año 2013, se dictó una medida con la finalidad de denegar el servicio de telefonía móvil a dispositivos falsificados (denominados “xing-ling”) a partir de enero de 2014. Para ese momento, se calculaba que estos dispositivos representaban más del 12 por ciento de todo el mercado. Sin embargo, la implementación efectiva de esta medida ha resultado cuando menos problemática, al tratarse de un banco de datos gigantesco y complejo.

En Perú el Decreto Legislativo número 1182 de julio de 2015 (popularmente conocido como Ley Stalker) instauró un mandato obligatorio de retención de datos “derivados de las telecomunicaciones” por tres años. Este mandato pone a disposición de los organismos policiales detalles relativos a las comunicaciones cuya extensión y alcance no está precisada por la normativa, si bien sí establece como requisito la existencia previa de una autorización judicial. Desde el año 2015, las empresas que prestan servicios de telefonía móvil en Perú están obligadas a verificar la identidad de sus usuarios de servicios prepago al momento de la contratación.

En Argentina, noviembre de 2016, a través de la Resolución Conjunta número 6-E/2016, el Ministerio de Comunicaciones y el Ministerio de Seguridad crearon el Registro de Identidad de Usuarios del Servicio de Comunicaciones Móviles. Bajo esta normativa, se busca impulsar la nominación de todas las líneas telefónicas existentes en el país, responsabilidad que recae en las operadoras del servicio de telefonía.

En Chile, el juez de garantía tendrá competencia para ordenar, a petición del Ministerio Público, la interceptación y grabación de las comunicaciones telefónicas o de otra índole de una persona, cuando existan fundadas sospechas, basadas en hechos determinados, de que dicha persona hubiere cometido o participado en la preparación o comisión, o preparare actualmente la comisión o participación en un hecho punible que mereciera pena de crimen. Para esta finalidad, dichos proveedores deberán mantener un listado actualizado, con carácter reservado y a disposición del Ministerio Público, que contenga sus rangos autorizados de direcciones IP, así como un registro mínimo de un año de los números IP de las conexiones que realicen sus abonados. En marzo de 2017, Chile implementó una política de pre-registro de códigos IMEI, es decir, un sistema de lista blanca que requiere que los dispositivos móviles aparezcan en el registro antes de ser activados. Hasta el momento, Chile manejaba un registro de lista negra, que permitía a los usuarios reportar los dispositivos cuando éstos fueran robados o hurtados, con la finalidad de que las operadoras móviles pudieran proceder a su bloqueo.

La GMSA (Asociación *Global System for Mobile Communications* , por sus siglas en inglés) se ha convertido en un aporte fundamental en el análisis de este tema, debido a que la Asociación representa los intereses de los operadores móviles de todo el mundo, reuniendo a casi 800 operadores con unas 300 compañías del amplio ecosistema móvil.

En el caso de México, los operadores móviles pertenecen a la Asociación Nacional de Telecomunicaciones, se sumaron a GSMA en agosto de 2012, a través del Memorando de entendimiento sobre el intercambio de datos de dispositivos móviles robados.

En su investigación, titulada Seguridad, privacidad y protección del ecosistema móvil. Cuestiones clave e implicancias de las políticas públicas, GMSA establece que, en las últimas tres décadas, el mercado de servicios de telecomunicaciones móviles creció hasta representar más de 7 mil 600 millones de conexiones móviles, brindándole servicios a 4 mil 700 millones de suscriptores móviles únicos a nivel mundial. Se estima que este crecimiento continuará y se prevé que para el año 2020, casi tres cuartas partes de la población mundial podrán disfrutar los beneficios que ofrece una suscripción móvil.[19]

Es más que lógico saber que a medida que se desarrollan servicios más avanzados y complejos, también aumenta la lista de posibles amenazas y el alcance de los daños que pueden causar. Las estafas y los ataques son cada vez más sofisticados, la capacidad de los criminales de interceptar comunicaciones aumenta con frecuencia y va desde el robo de grandes cantidades de datos hasta el hackeo y la divulgación de comunicaciones privadas durante las elecciones estadounidenses en 2016.

Las concesionarias del servicio de telefonía reconocen que tienen que enfrentar el aumento de inseguridad pública. Ocho de cada diez consumidores no están tranquilos con la cantidad de datos personales que se comparten. Dada la gran diferencia entre el estándar de protección de datos que se aplica en distintas jurisdicciones y, especialmente, entre el sector de telecomunicaciones versus el de los proveedores de servicios en línea, un operador de redes móviles solo puede comprometerse a proteger los datos de su usuario directo y a concientizar al usuario final de que posiblemente esté compartiendo demasiados datos con organizaciones que exceden el control del operador.

En este sentido, a diferencia de lo establecido por la investigadora Marianne Díaz, la GSMA establece que los concesionarios deben cumplir con el objetivo principal de la protección de la privacidad y generar la confianza en que los datos privados están protegidos de forma adecuada y conforme con las reglamentaciones y requerimientos de privacidad aplicables. Para ello, todas las partes involucradas deben adoptar una estrategia coherente, con neutralidad tecnológica y congruencia a través de todos los servicios, sectores y geografías.[20] Por esta razón, las concesionarias se comprometen a respetar los avisos de privacidad.

En varios mercados, los operadores móviles han lanzado servicios que automáticamente bloquean llamadas no deseadas. Además, existen servicios para propietarios de teléfonos básicos, tales como '*Banglalink Emergency'* [Emergencia Banglalink], que envían automáticamente una alerta por SMS a tres contactos previamente registrados cuando el usuario marca un número corto. La ubicación del usuario también es enviada a esos contactos, mejorando así su nivel de seguridad.

Es la GSMA quien asigna el identificador, IMEI a los fabricantes cuyos dispositivos se diseñan conforme al Proyecto de Asociación de Tercera Generación [*3rd Generation Partnership Project* o 3GPP, por sus siglas en inglés]. En su Base de Datos de IMEI, la GSMA registra los rangos asignados y toda la información relacionada con el modelo del dispositivo al cual fue asignado, incluidos el nombre del fabricante y del modelo del dispositivo, como también las principales funcionalidades de red (por ejemplo, bandas de frecuencia, interfaces de radio y tipos de dispositivos).

Todos los miembros de la GSMA conectados a la Base de Datos de IMEI para compartir información sobre dispositivos robados tienen acceso a esa lista central, comúnmente conocida como la "lista negra". Cuando los

operadores de redes móviles detectan que un dispositivo registrado en la lista negra se conecta a su red, pueden bloquear su uso. Cuando un ladrón se da cuenta de que la probabilidad de que un consumidor compre un dispositivo robado es baja, dado que posiblemente haya quedado deshabilitado inmediatamente después de haber sido extraído, el robo de dispositivos perderá su atractivo.

En este sentido, la GSMA alienta a sus miembros a implementar, sobre la base de ciertos estándares, un Registro de Identidad de Equipos [*Equipment Identity Register,* EIR] en sus redes para bloquear la conexión de todo dispositivo robado en base al identificador IMEI.

La GSMA estableció que el bloqueo de IMEI en base a la lista negra tuvo un impacto positivo en muchos países, pero es necesario, para que una campaña antirrobo sea totalmente efectiva implementar otras medidas adicionales. **El robo y la venta de dispositivos es un problema internacional** . Aun cuando todos los operadores de redes móviles de una región bloqueen un IMEI, el dispositivo móvil puede ser utilizado en cualquier otra región en la que los operadores de redes móviles no estén conectados a la Base de Datos de IMEI de la GSMA. Los esfuerzos de la GSMA se han concentrado en conectar la mayor cantidad de operadores de redes móviles posible a la Base de Datos de IMEI. **Hasta fines de 2016, la lista negra de la Base de Datos de la GSMA era utilizada por más de 140 operadores de redes móviles en más de 40 países del mundo para compartir diariamente información sobre dispositivos robados.** En América Latina, donde la incidencia de este problema es altísima, son 18 los países conectados a la Base de Datos de IMEI, con la participación activa de la mayoría de los operadores de redes móviles de la región. **A fin de empoderar y ayudar aún más al consumidor y los negocios minoristas, en algunos mercados se encuentra disponible un servicio público de Verificación de IMEI de Dispositivos que permite verificar el estado del dispositivo que se encuentra a la venta.** Estos servicios se implementaron como parte de la campaña "Nos Importa", a cargo de la GSMA, con más de 1,5 millones de búsquedas realizadas hacia fines de 2016.

Es importante que todos los interesados –fabricantes, operadores de redes móviles, gobiernos y consumidores– colaboren en garantizar la total integridad del IMEI y la inmediata corrección de cualquier problema que surja.

Asimismo, los gobiernos deben reconocer el rol central de la integridad del IMEI en el bloqueo de dispositivos robados y penalizar el cambio no autorizado del IMEI de un dispositivo móvil (también denominado reprogramación o adulteración de IMEI). De acuerdo con GMSA en algunos países, este cambio realizado luego de su fabricación es un delito penal. Una forma de impedir el robo de dispositivos móviles es el "*kill switch* " [Interruptor de desactivación]. Un kill switch es una forma de deshabilitar las funcionalidades esenciales de un dispositivo móvil.[21]

Los operadores de tiendas de aplicaciones pueden obtener los IMEI de los dispositivos robados de la GSMA y utilizarlos para denegar el acceso de los dispositivos denunciados como robados a sus tiendas. GSMA exhorta a los gobiernos a introducir legislación para penalizar la reprogramación no autorizada de un IMEI y, además, apoyar los esfuerzos de la industria y los organismos de seguridad en la lucha contra el robo de dispositivos. Establecen que las listas negras son la solución óptima para prevenir el uso a nivel de red de los dispositivos perdidos o robados.

Es fundamental, el desarrollo de una base de datos nacional de identificadores de dispositivos representa gastos y esfuerzos innecesarios. La base de datos de IMEI de la GSMA, que ya existe, puede satisfacer toda necesidad de bloqueo e intercambio de información de dispositivos.

En muchos casos, los teléfonos móviles robados cruzan las fronteras para aprovechar las oportunidades de arbitraje de precios y/o encontrar alternativas para eludir las iniciativas del país en el que se realizó el robo destinadas a bloquear los dispositivos utilizando el IMEI. Por lo tanto, para verdaderamente combatir este problema, es vital que la información sea compartida entre los operadores de un mismo país y que también sea posible hacerlo a nivel regional y mundial. **Se estima que, en 2013, se vendieron 143 millones de dispositivos móviles ilegales en todo el mundo.** [22]

No es fácil identificar y bloquear los dispositivos móviles falsificados porque muchos tienen un IMEI que parece legítimo. Hoy en día es común que los falsificadores pirateen rangos de números de IMEI asignados a fabricantes de dispositivos legítimos para utilizarlos en sus productos, dificultando aún más la diferenciación entre los productos legítimos y los falsificados. El IMEI no se puede aplicar a los dispositivos móviles que se trafican e importan fuera del proceso aduanero como contrabando: en este caso, la aduana y los organismos de seguridad deben concentrarse en combatir el tráfico ilegal.

En general, los estafadores que interactúan con sus potenciales víctimas desarrollan una relación de empatía y confianza, muchas veces aprovechando la información disponible públicamente. El fraude por ingeniería social está en aumento y la organización internacional de policía criminal, Interpol, lo identificó como una de las tendencias emergentes de fraude a nivel mundial. Entre esta modalidad, se encuentra el *Phishing* método utilizado para infectar una computadora o un dispositivo móvil con el objeto de obtener acceso a valiosa información personal. *SMiShing* o 'SMS *phishing* ' es el uso de mensajes de texto para presentar un "señuelo" que luego conduce a las personas a divulgar su información personal. Y el *Vishing* que es cuando los defraudadores persuaden a las víctimas a suministrar información personal o transferir dinero, por teléfono, haciéndose pasar por un servicio legítimo como puede ser un banco.[23]

El fraude, en todas sus formas, es un problema de alta complejidad y, en la mayoría de los casos, es considerado ilegal en gran parte de los países. Por ello, la legislación y la regulación deberían enfocarse en los autores del delito.

Es importante mencionar que las leyes sobre privacidad, cuando las hubiere, varían de una jurisdicción a otra y no existe un marco interoperable a nivel mundial. Esto puede complicarse aún más si el proveedor de servicios almacena y procesa los datos en un tercer país.

Algunas prácticas utilizadas por aplicaciones y servicios en línea llevan al consumidor a "aceptar" términos y condiciones relativos a la privacidad sin leer el aviso ni entender las implicancias de sus decisiones. Un estudio encargado por la GSMA muestra que el 82 por ciento de los usuarios acepta los avisos de privacidad sin leerlos porque son demasiado extensos o contienen demasiado lenguaje jurídico.[24]

Por esta razón, la información personal se debe proteger utilizando garantías razonables y adecuadas a la sensibilidad de la información. **Solo se debe recolectar la mínima cantidad de información personal necesaria para cumplir con los fines comerciales legítimos y para proporcionar, suministrar, mantener o desarrollar aplicaciones o servicios. La información personal no se debe mantener más tiempo que el necesario para los fines comerciales legítimos o para cumplir con las obligaciones legales correspondientes, y luego debe ser eliminada o se deben anonimizar dichos datos personales.**

Nuevos marcos legales, tales como las Reglas de Privacidad Transfronteriza [*Cross Border Privacy Rules* , CBPR] de APEC [Foro de Cooperación Económica Asia-Pacífico] y las Normas Corporativas Vinculantes de la UE establecen los principios internacionales comunes, incluidos los mecanismos de responsabilidad que rigen la forma en que se deben tratar los datos durante su transferencia entre países. Sin embargo, el éxito de la adopción de estos principios se ve afectado por la implementación, por parte de los gobiernos, de normas de 'localización de datos' (también conocidas como 'soberanía de datos') que imponen requerimientos locales de almacenamiento o uso de tecnología, y pueden encontrarse en una amplia variedad de normas específicas para un sector o una temática, incluyendo a los proveedores de servicios financieros, el secreto profesional o el sector público.

Otra forma de restringir las comunicaciones móviles es la utilización de inhibidores de señal, también conocidos como bloqueadores [*jammers*]. Se trata de dispositivos que generan una interferencia que interrumpe, en forma intencional, los servicios de radiocomunicación al obstruir la conexión entre el terminal móvil y la estación radiobase. En general, estas herramientas rudimentarias se utilizan para impedir las comunicaciones en centros penitenciarios

o entre terroristas o grupos políticos considerados subversivos, a menudo, en lugares donde se realizan manifestaciones públicas masivas. Los inhibidores de señal también se utilizan como herramienta para imposibilitar el uso de dispositivos móviles en áreas prohibidas.

Sin embargo, el bloqueo de la señal no soluciona la raíz del problema, el hecho de que los dispositivos móviles llegan a manos de los reclusos ilegalmente. El costo de los bloqueadores, la pérdida de ingresos legítimos y, muchas veces, la mala reputación que genera la interrupción del servicio, redunda en un impacto negativo en los operadores móviles. Cualquier interrupción en las redes de comunicaciones, los servicios de red o el internet (tales como redes sociales, motores de búsqueda o sitios de noticias) tiene el potencial de afectar la seguridad pública y restringir el acceso a servicios vitales de emergencia, pagos y salud. Por ejemplo, una restricción de servicio puede limitar la capacidad del usuario móvil de ponerse en contacto con los servicios de emergencia y puede interferir en el funcionamiento de las alarmas móviles conectadas o dispositivos médicos personales. Por estos motivos, las restricciones de servicios deben ser mínimas y se deben considerar los efectos colaterales negativos para todos los usuarios.[25]

El tercer aspecto de seguridad pública que ha sido objeto de gran debate en los últimos años es el registro obligatorio de tarjetas SIM móviles prepagas, en virtud del cual se requiere a todos los usuarios que demuestren su identidad al momento de comprar una tarjeta de módulo de identificación del suscriptor [*Subscriber Identity Module,* SIM]. Varios gobiernos argumentaron que esta modalidad permite a los delincuentes aprovechar el anonimato para llevar a cabo diferentes actividades ilegales, como, por ejemplo, pedir un rescate después de un secuestro o planear un ataque terrorista. La percepción es que este anonimato hace más difícil rastrear el uso de la tarjeta SIM móvil a un usuario real. En respuesta, algunos gobiernos exigieron que los operadores de redes móviles lleven un registro de todos sus clientes, actuales y futuros.

Una vez implementadas, estas medidas tuvieron una serie de consecuencias no deseadas, incluyendo: La exclusión de usuarios, que no contaban con la documentación necesaria, del acceso a los servicios móviles, generalmente aquellos en condiciones más pobres y vulnerables. El aumento del robo de dispositivos móviles y el surgimiento de un mercado negro de tarjetas SIM registradas en forma fraudulenta o robadas, originado por el deseo de algunos consumidores -incluidos los delincuentes- de mantener su anonimato. Una mayor preocupación del consumidor en relación con el acceso, seguridad, uso y retención de sus datos personales, en particular ante la ausencia de leyes nacionales sobre privacidad y libertad de expresión.

Por otra parte, los usuarios podrían utilizar algunos programas informáticos para saber quién está llamando o si se trata de SPAM o no; pero siguen siendo un instrumento limitado. Uno de los más populares es *WhoCalledMe* , ya que cuenta con una importante base de datos de números de teléfonos e información adicional sobre quiénes son sus propietarios. Otro servicio similar es *QuienHaLlamado* , que cuenta con una base de datos similar a la de una guía telefónica, pero con números de teléfono no deseados o desconocidos. Para usar este servicio, basta con ir al sitio web e indicar el número de teléfono del que hemos recibido la llamada para informarnos de quién es. Cuenta con gran cantidad de usuarios que aportan información sobre estos números de teléfonos no deseados. *ListaSpam* es otro sitio donde podemos acudir para saber de quién es un número de teléfono desconocido que nos está llamando. Se trata de un servicio gratuito para realizar búsquedas de teléfonos inversas y donde podemos descubrir de quién es un número de teléfono y cuál o cuáles son sus intenciones. Además, puedes añadir nuevas denuncias de teléfonos spam para ayudar al resto de personas que visiten el sitio.[26]

De esta manera, aunque existe un incesante crecimiento de la delincuencia vinculada por la indebida posesión de datos telefónicos o de los propios aparatos, también existen esfuerzos de talla internacional y nacional para enfrentarlos. Recientemente en este año, la Agencia Digital de Innovación Pública del Gobierno de la Ciudad de México (ADIP), promovió una estrategia denominada **bloquea tu equipo móvil a través del código de identidad de fabricación del equipo** (IMEI)" esto en cumplimiento a las disposiciones previstas en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México. La finalidad de este Sistema es dar a

conocer a la ciudadanía, que la ADIP podrá recabar datos personales de los ciudadanos que deseen registrar y resguardar el número IMEI de sus equipos móviles de los usuarios de telefonía móvil en la Dirección General de Contacto Ciudadano (Locatel), así como recibir acompañamiento de éste, ante las operadoras telefónicas para solicitar la suspensión de la línea telefónica y el bloqueo de sus equipos móviles, en caso de robo o extravío.

En esta iniciativa participan el Consejo Ciudadano y Locatel, en colaboración con los tres principales operadores de telefonía móvil en México. Al bloquear definitivamente el aparato mediante la estrategia, se restan incentivos a la delincuencia porque ya no podrán revenderlos: a nadie le interesa un celular que no se puede desbloquear.

Se explicará a la ciudadanía que la clave para realizar la operación de bloqueo consiste en conocer el IMEI del celular (para ello, se debe marcar desde el teléfono la clave *#06#). La ventaja de resguardar el IMEI en Locatel es que en el momento de un robo o extravío, la persona puede llamar a Locatel al 5658-1111 para que esta institución lo acompañe en el proceso de bloqueo durante la llamada a la compañía telefónica con la que el usuario tiene el contrato, sin necesidad de tener a la mano el IMEI dado que ya fue proporcionado con anterioridad.[27]

Los datos personales que se recaban son los mínimos necesarios para que Locatel esté en posibilidad de operar la estrategia “Bloquea tu cel”, y que son utilizados única y exclusivamente para dicha finalidad, principalmente, para la debida autenticación del propietario del equipo. Cualquier uso distinto que se le dé a los datos recabados, será sancionado en los términos de la Ley de Responsabilidades Administrativas de la Ciudad de México, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México y demás normatividad aplicable. Los datos recabados sólo pueden ser transmitidos a aquellas autoridades que, en ejercicio de sus atribuciones, los requieran mediante mandamiento escrito, debidamente fundado y motivado, como pueden ser, órganos de fiscalización, órganos jurisdiccionales o el propio órgano garante (Infodf), para atender alguna queja o denuncia relacionada con su tratamiento o el servicio prestado. Los ciudadanos podrán ejercer sus derechos Arco (Acceso, Rectificación, Corrección u Oposición) de los datos personales que proporcionaron a la ADIP, y que lo pueden hacer valer ante la Unidad de Transparencia.[28]

Recordemos que en México, se pueden ejercer los derechos de acceso, rectificación o cancelación (Arco) de datos personales, mediante el aviso de privacidad del proveedor de servicios telefónicos.[29]

Así en nuestra nación, los usuarios están protegidos a través de Ley de Protección de datos Personales y las concesionarias telefónicas deben salvaguardar su información, en estricto apego al Artículo 190 de la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR). Esta Ley también mantuvo los derechos de portabilidad; solicitar el desbloqueo del equipo una vez que concluya la vigencia del contrato o hayas liquidado su costo, y a ser bonificado por las fallas en el servicio. La Norma Oficial identificada como NOM-184-SCFI-2012 define qué información deben proporcionarte los operadores de telefonía móvil.

De acuerdo con la LFTR la información sobre las características de los aparatos y los metadatos que deben conservar las empresas de telefonía móvil, se estable en los numerales I y II y son los siguientes:

“**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;

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;

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 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."

En torno a estas disposiciones, llama la atención la resolución que tuvo el Instituto Nacional de Acceso a la Información en 2016, cuando la empresa AT&T por negligencia se negó a entregar los datos solicitados por un usuario.[30] El INAI resolvió que la información recabada por las operadoras por obligación del artículo 190 de la LFTR son datos personales y que los particulares pueden tener acceso a ellos (por supuesto a los propios). Además, ordenó iniciar un proceso de imposición de sanciones contra AT&T por su presunta negligencia en la tramitación de la solicitud del particular.

El 7 de enero el particular, cliente de AT&T, solicitó a la compañía acceso a sus datos recabados por obligación del artículo 190. La compañía se negó, por considerar que los datos sólo son disponibles para las autoridades, aunque después pidió al consumidor que acudiera a un centro de atención a solicitar ahí la información. AT&T envió por correo electrónico al particular un documento de 755 páginas que, de acuerdo con la resolución, no comprenden toda la información señalada por la LFTR. Además, tampoco explicó los códigos, siglas y abreviaturas contenidas en el documento. Dos meses después, el particular solicitó la protección del INAI y se inició el procedimiento de protección de derechos (PPD) que culminó en la sesión del pleno del 13 de 2016.

La constitucionalidad de la determinación del INAI fue ratificada por la Suprema Corte de Justicia de la Nación el 4 de mayo de 2016. El mencionado artículo 190 obliga a todas las operadoras a recabar y resguardar datos sobre las comunicaciones de todos sus clientes (casi 110 millones en todo el país), con los que se pueden hacer inferencias sobre la vida privada de las personas.

En la resolución al expediente PPD.0050/16 firmada por el pleno el 13 de julio, el INAI ordena a AT&T, el tercer operador de telefonía móvil en México por número de usuarios, a entregar a su cliente todos los datos mencionados en el 190 en un plazo de 10 días.

Se conforma así la violación por parte de AT&T del artículo 63 de la Ley de Protección de Datos Personales, "por su presunta negligencia en la tramitación y respuesta de la solicitud de acceso de datos personales". Se garantiza la facultad del consumidor para conocer datos básicos de su línea telefónica; tipos, origen y destino de sus comunicaciones; fecha, hora, duración, generales del teléfono (terminal), y ubicación geográfica de la línea a través del tiempo.

Con ello, debe quedar claro que los concesionarios de servicios de telecomunicaciones deben conservar los datos referentes al registro y control de comunicaciones de los particulares durante doce meses en sistemas que permitan su consulta y entrega en tiempo real a las autoridades competentes, a través de medios electrónicos y que una vez concluido el plazo anterior, se deberán conservar por doce meses adicionales en sistemas de almacenamiento electrónico.

En este contexto, diversos legisladores han presentado iniciativa para combatir la extorsión telefónica, así, como el robo de los aparatos de comunicación móviles y sus partes. Actualmente está pendiente de aprobación en la Cámara de Senadores, una minuta de la Colegisladora, mediante la que se adiciona el 190 Bis de la LFTR y se adiciona un Artículo 166 Ter al Código Penal Federal. Dicha reforma es la siguiente:

> "**Artículo 190 Bis.** Queda prohibida la fabricación, comercialización, adquisición, así como la instalación, portación, uso y operación de equipos que bloqueen, cancelen o anulen las señales de telefonía celular, de radiocomunicación o de transmisión de datos o imagen.

Con excepción de lo dispuesto en el párrafo anterior, se podrá instruir la fabricación, comercialización, adquisición, instalación, portación para el uso y operación por parte de las autoridades encargadas de los centros de reinserción social, establecimientos penitenciarios o centro de internamiento para menores, para efectos de los dispuesto por la

fracción VIII del artículo 190 de esta ley, así como para el uso y operación de los mismos por parte de las instancias de seguridad pública federales y de seguridad nacional en cumplimiento de sus atribuciones.

Se adicionan un artículo 168 Ter al Código Penal Federal, para quedar como sigue:

> **Artículo 168 Ter.** Se sancionará con pena de 12 a 15 años de prisión, a quien fabrique, comercialice, adquiera, instale, porte, use u opere equipos que bloqueen, cancelen o anulen las señales de telefonía celular, de radiocomunicación o de transmisión de datos o imagen con excepción de lo establecido en el segundo párrafo artículo 190 Bis de la Ley Federal de Telecomunicaciones y Radiodifusión.

Los equipos a que hace referencia el primer párrafo del artículo 190 Bis de la Ley Federal de Telecomunicaciones y Radiodifusión, serán asegurados en términos de lo que establece el Código Nacional de Procedimientos Penales y posteriormente deberán ser destruidos en su totalidad.

Si el delito al que se refiere el primer párrafo de este artículo, fuera cometido por servidores públicos, y sin autorización expresa escrita debidamente acreditada por su superior inmediato, se le impondrá la pena de 15 a 18 años de prisión."

Esta minuta tiene que ver con los bloqueadores de señales, que no deben de utilizarse por los efectos negativos que pudieran ocasionar en el entorno donde son implementados; salvo, en los centros de reclusión, porque existe la evidencia que, desde allí, se procesan múltiples llamadas para extorsionar.

Con base en la información que presenté anteriormente, me permito presentar a esta honorable asamblea modificaciones a la Ley Federal de Telecomunicaciones y Radiodifusión con la finalidad de precisar que las concesionarias deberán solicitar los nombres y domicilios de los usuarios, de cualquier tipo de modalidad en el servicio a fin de que los usuarios estén debidamente acreditados; para ello, bastará presentar una identificación oficial; en el caso, de la credencial para votar con fotografía, podrá servir también como comprobante de domicilio.

De la misma manera, propongo que las concesionarias actualicen y estén en comunicación permanente, para conformar una base de datos con los números de identificación internacional de equipo móvil que son reportados como robados, o utilizados como canales para la extorsión, a fin de construir un programa o app que esté cargado o que se pueda cargar de manera gratuita a los dispositivos a fin de que se emitan las alertas para que los usuarias sepan que esos números son parte de la lista negra, de donde provienen las extorsiones en sus distintas modalidades.

Esta propuesta busca que exista un enfoque que permita contar con una base de datos más completa respecto a las listas negras y que realmente sean utilizadas para combatir la delincuencia. Para que esta medida sea realmente exitosa, es necesario que el gobierno federal y los gobiernos estatales promuevan campañas permanentes de información, a fin de que los usuarios están informados sobre los instrumentos que tienen para protegerse.

De igual forma, propongo la incorporación de un nuevo artículo 168 bis del Código Penal Federal para castigar a quien cambie o clone los números IMEI con fines delictivos; hay que recordar que existe un tráfico permanente de celulares robados entre diversas naciones y esto debe de ser controlado a fin de evitar la extorsión internacional. De igual, los delincuentes modifican el IMEI para evitar estar en las listas negras. Con la modificación al artículo 368 del mencionado Código, se equipará como robo y se castiga como tal, el aprovechamiento o apoderamiento de teléfonos móviles o de sus partes, así como los datos personales contenidos en éstos, sin consentimiento de sus propietarios, esto porque parto de la idea, de que, si no hay castigo, seguirá incrementándose este fenómeno delictivo.

De gua forma, se tipifica como delito el hecho de que personas físicas o morales vendan las bases de datos con nombres y teléfonos de los usuarios a fin de la información sea utilizada de manera indebida no sólo para extorsionar, sino para promocionar servicios o productos que no han sido solicitados por los duelos de los aparatos móviles.

Dada la alta frecuencia de las llamadas para extorsionar desde los penales o centros de readaptación social, es evidente que algunos de sus empleados, personal o custodios se encuentran coludidos con los delincuentes y prestan las facilidades necesarias para que la extorsión siga creciendo; por ello, se incorporará a este personal, como probables sujetos de responsabilidad penal, por dichos actos.

A fin de presentar una versión esquemática de las propuestas de esta iniciativa, me permito adjuntar el siguiente cuadro comparativo:

LEY FEDERAL DE TELECOMUNICACIONES Y RADIODIFUSIÓN	PROPUESTA DE MODIFICACIÓN
Artículo 118. Los concesionarios que operen redes públicas de telecomunicaciones deberán: I a IX…….	Artículo 118. Los concesionarios que operen redes públicas de telecomunicaciones deberán: I. **Solicitar para la venta o activación de una línea telefónica, en cualquier modalidad, identificación oficial con fotografía y comprobante de domicilio, así como datos del establecimiento mercantil o distribuidor, fecha, hora y lugar de la venta y forma de pago.** Se recorren los subsecuentes I al X.
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…… El Instituto…… **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)** a h) …… **c)** Para tales …… La solicitud ……	**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…… El Instituto…… **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 **tanto para el plan por contrato o tarifario, así como en la modalidad de prepago. Esto deberá acreditarse mediante un documento de identificación oficial** a) a h) …… Para tales ……

Los concesionarios ……	La solicitud ……
	Los concesionarios ……
III. Entregar …… Queda …… Los concesionarios …. …	**III.** Entregar …… Queda …… Los concesionarios …. …
IV. Contar con …… Para efectos……	**IV.** Contar con …… Para efectos……
V. Establecer procedimientos expeditos para recibir los reportes de los usuarios del robo o extravío de los equipos o dispositivos terminales móviles y para que el usuario acredite la titularidad de los servicios contratados. Dicho reporte deberá incluir, en su caso, el código de identidad de fabricación del equipo o **Identidad Internacional de Equipo Móvil (IMEI)**;	**V.** Establecer procedimientos expeditos para recibir los reportes de los usuarios del robo o extravío de los equipos o dispositivos terminales móviles y para que el usuario acredite la titularidad de los servicios contratados. Dicho reporte deberá incluir, en su caso, el código de identidad de fabricación del equipo o **Identidad Internacional de Equipo Móvil (IMEI)**;
VI. Realizar la suspensión del servicio de los equipos o dispositivos terminales móviles reportados como robados o extraviados, a solicitud del titular. Los concesionarios deberán celebrar convenios de colaboración que les permitan intercambiar listas de equipos de comunicación móvil reportados por sus respectivos clientes o usuarios como robados o extraviados, ya sea que los reportes se hagan ante la autoridad competente o ante los propios concesionarios;	**VI.** Realizar la suspensión del servicio de los equipos o dispositivos terminales móviles reportados como robados o extraviados, a solicitud del titular. Los concesionarios deberán celebrar convenios de colaboración que les permitan intercambiar listas de equipos de comunicación móvil reportados por sus respectivos clientes o usuarios como robados o extraviados, ya sea que los reportes se hagan ante la autoridad competente o ante los propios concesionarios; **Con base en el IMEI, los concesionarios diseñarán y mantendrán comunicación permanente para la actualización de una base de datos actualizada de los números asociados a la actividad delincuencial (llamada lista negra). Esta información**

	será utilizada para el diseño de una aplicación (app) que deberá estar precargada o sin costo alguno en las tiendas virtuales que a efecto se requieran, mediante la cual, se emitirá una alerta a los usuarios de los números identificados con extorsiones, números de spam (aquellos que se dedican a promocionar o vender productos sin que el usuario de telefonía lo haya pedido) y números de teléfonos robados. De tal manera, que se procuré la protección y la seguridad pública.
VII. Realizar ……..	**VII.** Realizar ……..
VIII. Colaborar …….	**VIII.** Colaborar …….
El bloqueo ……..	El bloqueo ……..
Los ……..	Los ……..
IX. Implementar ……..	**IX.** Implementar ……..
X. Informar……..	**X.** Informar……..
XI. En los términos ……	**XI.** En los términos ……
XII. Realizar ……..	**XII.** Realizar ……..
Las comunicaciones privadas son …… ….	Las comunicaciones privadas son …… ….

CÓDIGO PENAL FEDERAL	PROPUESTA
NO EXISTE	**Artículo 168 bis.- Se impondrán de seis meses a dos años de prisión y de trescientos a tres mil días multa, a quien sin derecho:** **I. Cambie los números de decodificación de los códigos de seguridad de equipos o dispositivos terminales móviles.** **II. Modifique o clone el código de fabricación de equipos o dispositivos terminales móviles (IMEI) con fines delictivos.** III. **Ingrese mediante páginas o mensajes falsos, con el objetivo de introducir virus u obtener datos de los usuarios, para extorsionarlos.**
Artículo 368.- Se equiparán al robo y se castigarán como tal: **I.-** El apoderamiento o destrucción dolosa de una cosa propia mueble, si ésta se halla por cualquier título legítimo en poder de otra persona y no medie consentimiento; y **II.-** El uso o aprovechamiento de energía eléctrica, magnética, electromagnética, de cualquier fluido, o de cualquier medio de transmisión, sin derecho y sin consentimiento de la persona que legalmente pueda disponer de los mismos.	**Artículo 368**.- Se equiparán al robo y se castigarán como tal: **I.-** El apoderamiento o destrucción dolosa de una cosa propia mueble, si ésta se halla por cualquier título legítimo en poder de otra persona y no medie consentimiento; y **II.-** El uso o aprovechamiento de energía eléctrica, magnética, electromagnética, de cualquier fluido, o de cualquier medio de transmisión, sin derecho y sin consentimiento de la persona que legalmente pueda disponer de los mismos. IV. **El apoderamiento o aprovechamiento de los teléfonos móviles o de sus partes, así como de los datos personales contenidos en éstos, sin consentimiento de sus propietarios. La comercialización de partes o accesorios de equipos móviles con un IMEI reportado como robado o utilizado para la extorsión.**
Artículo 390.- Al que sin derecho obligue a otro a dar, hacer, dejar de hacer o tolerar algo, obteniendo un lucro para sí o para otro o causando a alguien un perjuicio patrimonial, se le aplicarán de dos a ocho años de prisión	Artículo 390.- Al que sin derecho obligue a otro a dar, hacer, dejar de hacer o tolerar algo, obteniendo un lucro para sí o para otro o causando a alguien un perjuicio patrimonial, se le aplicarán de dos a ocho años de prisión

y de cuarenta a ciento sesenta días multa. Las penas se aumentarán hasta un tanto más si el constreñimiento se realiza por una asociación delictuoso, o por servidor público o ex-servidor público, o por miembro o ex-miembro de alguna corporación policial o de las Fuerzas Armadas Mexicanas. En este caso, se impondrá además al servidor o ex-servidor público y al miembro o ex-miembro de alguna corporación policial, la destitución del empleo, cargo o comisión y la inhabilitación de uno a cinco años para desempeñar cargo o comisión público, y si se tratare de un miembro de las Fuerzas Armadas Mexicanas en situación de retiro, de reserva o en activo, la baja definitiva de la Fuerza Armada a que pertenezca y se le inhabilitará de uno a cinco años para desempeñar cargos o comisión públicos."	y de cuarenta a ciento sesenta días multa. **A las concesionarias telefónicas o a cualquier persona física o moral que venda las bases de datos que contienen números telefónicos y nombres de usuarios. De igual forma, a las personas morales o física, quienes de manera indebida utilizan dicha información para promover servicios o productos que no han sido solicitados por los dueños de los aparatos móviles.** Las penas se aumentarán hasta un tanto más si el constreñimiento se realiza por una asociación delictuosa, o por servidor público o ex-servidor público, o por miembro o ex-miembro de alguna corporación policial o de las Fuerzas Armadas Mexicanas, **así como de aquellos funcionarios que sean o hayan sido parte del sistema penitenciario.** En este caso, se impondrá además al servidor o ex-servidor público y al miembro o ex-miembro de alguna corporación policial **o personal del sistema penitenciario,** la destitución del empleo, cargo o comisión y la inhabilitación de uno a cinco años para desempeñar cargo o comisión público, y si se tratare de un miembro de las Fuerzas Armadas Mexicanas en situación de retiro, de reserva o en activo, la baja definitiva de la Fuerza Armada a que pertenezca y se le inhabilitará de uno a cinco años para desempeñar cargos o comisión públicos."

Por lo anteriormente expuesto, me permito presentar a honorable soberanía, el siguiente proyecto de:

Decreto

Artículo Primero. Se adiciona una fracción I, pasando a ser el actual I, II y así subsecuente del artículo 118. Se reforma el inciso a) del numeral II y el numeral V, así como se adiciona un nuevo párrafo segundo del numeral VI, todos del artículo 190 de la Ley Federal de Telecomunicaciones y Radiodifusión.

Artículo 118. Los concesionarios que operen redes públicas de telecomunicaciones deberán:

I. Solicitar para la venta o activación de una línea telefónica, en cualquier modalidad, identificación oficial con fotografía y comprobante de domicilio, así como datos del establecimiento mercantil o distribuidor, fecha, hora y lugar de la venta y forma de pago.

II. al **X. ...**

Artículo 190. Los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán:

I. ...

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 tanto para el plan por contrato o tarifario, así como en la modalidad de prepago. Esto deberá acreditarse mediante un documento de identificación oficial y comprobante de domicilio.

b) a la h) . ...

...

...

...

...

III. a la IV. ...

V. Establecer procedimientos expeditos para recibir los reportes de los usuarios del robo o extravío de los equipos o dispositivos terminales móviles y para que el usuario acredite la titularidad de los servicios contratados. Dicho reporte deberá incluir, en su caso, el código de identidad de fabricación del equipo o **Identidad Internacional de Equipo Móvil (IMEI);**

VI. Realizar la suspensión del servicio de los equipos o dispositivos terminales móviles reportados como robados o extraviados, a solicitud del titular.

Los concesionarios deberán celebrar convenios de colaboración que les permitan intercambiar listas de equipos de comunicación móvil reportados por sus respectivos clientes o usuarios como robados o extraviados, ya sea que los reportes se hagan ante la autoridad competente o ante los propios concesionarios;

Con base en el IMEI, los concesionarios diseñarán y mantendrán comunicación permanente para la actualización de una base de datos actualizada de los números asociados a la actividad delincuencial (llamada lista negra). Esta información será utilizada para el diseño de una aplicación (app) que deberá estar precargada o sin costo alguno en las tiendas virtuales que a efecto se requieran, mediante la cual, se emitirá una alerta a los usuarios de los números identificados con extorsiones, números de spam (aquellos que se dedican a promocionar o vender productos sin que el usuario de telefonía lo haya pedido) y números de teléfonos robados. De tal manera, que se procuré la protección y la seguridad pública.

VII. a la XII. ...

....

Artículo Segundo. Se adiciona un artículo 168 Bis; se adiciona un numeral III al artículo 368; se adiciona un segundo párrafo y se reforman el párrafo subsecuente del artículo 390 del Código Penal Federal

Artículo 168 Bis. Se impondrán de seis meses a dos años de prisión y de trescientos a tres mil días multa a quien sin derecho:

I. Cambie los números de decodificación de los códigos de seguridad de equipos o dispositivos terminales móviles.

II. Modifique o clone el código de fabricación de equipos o dispositivos terminales móviles (IMEI) con fines delictivos.

III. Ingrese mediante páginas o mensajes falsos, con el objetivo de introducir virus u obtener datos de los usuarios, para extorsionarlos.

Artículo 368. Se equiparán al robo y se castigarán como tal:

I. El apoderamiento o destrucción dolosa de una cosa propia mueble, si ésta se halla por cualquier título legítimo en poder de otra persona y no medie consentimiento; y

II. El uso o aprovechamiento de energía eléctrica, magnética, electromagnética, de cualquier fluido, o de cualquier medio de transmisión, sin derecho y sin consentimiento de la persona que legalmente pueda disponer de los mismos.

III. El apoderamiento o aprovechamiento de los teléfonos móviles o de sus partes, así como de los datos personales contenidos en éstos, sin consentimiento de sus propietarios. La comercialización de partes o accesorios de equipos móviles con un IMEI reportado como robado o utilizado para la extorsión.

Artículo 390. Al que sin derecho obligue a otro a dar, hacer, dejar de hacer o tolerar algo, obteniendo un lucro para sí o para otro o causando a alguien un perjuicio patrimonial, se le aplicarán de dos a ocho años de prisión y de cuarenta a ciento sesenta días multa.

A las concesionarias telefónicas o a cualquier persona física o moral que venda las bases de datos que contienen números telefónicos y nombres de usuarios. De igual forma, a las personas morales o física, quienes de manera indebida utilicen dicha información para promover servicios o productos que no han sido solicitados por los dueños de los aparatos móviles.

Las penas se aumentarán hasta un tanto más si el constreñimiento se realiza por una asociación delictuosa, o por servidor público o ex-servidor público, o por miembro o ex-miembro de alguna corporación policial o de las Fuerzas Armadas Mexicanas, **así como de aquellos funcionarios que sean o hayan sido parte del sistema penitenciario** . En este caso, se impondrá además al servidor o ex-servidor público y al miembro o ex-miembro de alguna corporación policial **o personal del sistema penitenciario,** la destitución del empleo, cargo o comisión y la inhabilitación de uno a cinco años para desempeñar cargo o comisión público, y si se tratare de un miembro de las Fuerzas Armadas Mexicanas en situación de retiro, de reserva o en activo, la baja definitiva de la Fuerza Armada a que pertenezca y se le inhabilitará de uno a cinco años para desempeñar cargos o comisión públicos.

Notas

1 https://www.unodc.org/documents/data-andanalysis/Crimestatistics/Manual_Victimization_surveys_2009_spanish.pdf

2 https://www.bbc.com/mundo/noticias/2014/06/140620_tecnologia_dispositivo_anti_robo_celulares_ar

3 https://www.periodistadigital.com/tecnologia/telefonia/20180120/

pais-mundo-roban-smartphone-2-minutos-noticia-689400244875/

4 http://www.anatel.org.mx/programaseguridad.php

5 https://www.eleconomista.com.mx/finanzaspersonales/

Hay-poca-cultura-para-denunciar-robo-de-celulares-20190715-0112.html

6 https://www.inegi.org.mx/contenidos/programas/envipe/2019/doc/envipe2019_presentacion_nacional.pdf

7 https://www.eluniversal.com.mx/articulo/metropoli/df/2015/10/2/robo-de-celulares-el-delito-mas-lucrativo

8 http://www.secretariadoejecutivo.gob.mx/unidades-secretariado/centro-na cional-informacion.php

9 https://www.eluniversal.com.mx/nacion/seguridad/usan-hasta-12-mil-lineas-telefonicas-para-extorsionar

10 https://www.diariodemexico.com/ante-incremento-de-extorsiones-crear porcientoC3por cientoA1n-base-de-datos-de-nporcientoC3porcientoBAmeros-sospechosos

11 https://www.excelsior.com.mx/comunidad/extorsion-la-patrona-surge-desde -3-penales-de-la-cdmx/1346914

12 http://anatel.org.mx/docs/interes/Estudio-Fijos-y-Moviles-2017.pdf

13 Loc. Cit.

14 http://www.anatel.org.mx/programadeseguridad.pdf

15 https://www.derechosdigitales.org/wp-content/uploads/informe-marianne-r etencion-de-datos.pdf

16 Díaz, Marianne. Retención de datos y registro de teléfonos móviles. Chile en el contexto latinoamericano. Edit. Derechos Digitales, América Latina y Ford Foundation, Chile, 2017, 37 pp.

17 Ibídem, p. 7

18 Ibídem, p. 11

19 https://www.gsma.com/latinamerica/wp-content/uploads/2017/06/Seguridad-privacidad-y-proteccio porcientoCCporciento81n-del-ecosistema-mo porcientoCCporciento81vil.pdf. P. 3

20 Ibídem, p. 8

21 Ibídem, p. 26

22 Ibídem, p. 28

23 Ibídem, p. 29

24 Ibídem, p.33

25 Ibídem, p. 46

26 https://www.adslzone.net/internet/saber-de-quien-es-numero-telefono/

27 https://adip.cdmx.gob.mx/comunicacion/nota/estrategia-para-la-reduccion-del-robo-de-telefonos-celulares

28 https://adip.cdmx.gob.mx/comunicacion/nota/

nota-informativa-sobre-el-tratamiento-de-datos-personales-recabados-al-amparo-de-la-estrategia-bloquea-tu-cel

29 https://sontusdatos.org/2019/07/08/

telefonia-celular-y-datos-personales-sabes-que-datos-recolecta-sobre-ti-una-compania-de-telefonia-celular/

30 https://www.eleconomista.com.mx/empresas/INAI-ordena-sancion-a-ATT-por-negligencia-sobre-datos-personales-20160814-0062.html

Dado en el Palacio Legislativo de San Lázaro, a los 11 días de febrero de 2020.

Diputados: Silvano Garay Ulloa (rúbrica), Mary Carmen Bernal Martínez (rúbrica), Claudia Angélica Domínguez Vázquez (rúbrica), Francisco Favela Peñuñuri (rúbrica), Alfredo Femat Bañuelos (rúbrica), Gerardo Fernández Noroña (rúbrica), Margarita García García (rúbrica), Ana Ruth García Grande (rúbrica), Hildelisa González Morales (rúbrica), Santiago González Soto (rúbrica), Óscar González Yáñez (rúbrica), Ana Laura Bernal Camarena (rúbrica), Francisco Javier Huacus Esquivel (rúbrica), María Rosella Jiménez Pérez (rúbrica), Claudia Elena Lastra Muñoz (rúbrica), Emilio Manzanilla Téllez (rúbrica), Maribel Martínez Ruiz (rúbrica), María Teresa Marú Mejía (rúbrica), José Luis Montalvo Luna (rúbrica), Alfredo Porras Domínguez (rúbrica), Armando Reyes Ledesma (rúbrica), Maricruz Roblero Gordillo (rúbrica), Ángel Benjamín Robles Montoya (rúbrica), Ana Karina Rojo Pimentel (rúbrica), Martha Huerta Hernández (rúbrica), Reginaldo Sandoval Flores (rúbrica), Dionicia Vázquez García (rúbrica), Javier Armando Zertuche Zuani (rúbrica), Luis Enrique Martínez Ventura (rúbrica), Olga Juliana Elizondo Guerra (rúbrica), José Luis García Duque (rúbrica), Nelly Maceda Carrera, Jesús Fernando García Hernández (rúbrica) y José de la Luz Sosa Salinas.