Hurto de equipos móviles en América Latina

Políticas e iniciativas actuales

Si tiene algún comentario sobre este reporte, favor enviarlo a: reports@tmgtelecom.com.

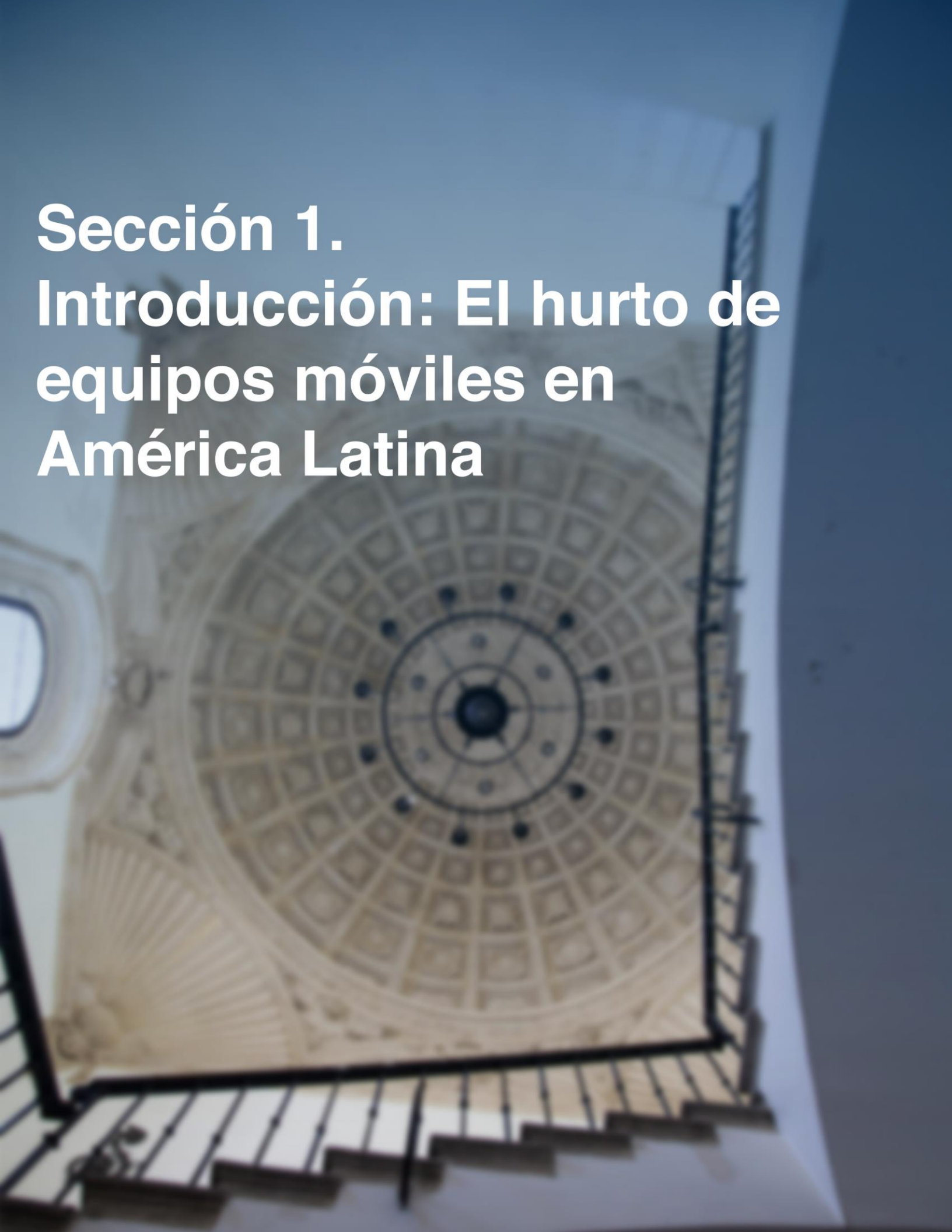
1600 Wilson Blvd., Suite 710

Arlington, VA 22209 USA

Fecha de actualización: Marzo 2018.

Publicado por primera vez en Noviembre de 2017

Índice



Sección 1. Introducción: El hurto de equipos móviles en América Latina

1 Introducción: El hurto de equipos móviles en América Latina

El hurto de equipos móviles en América Latina ha sido un problema desde que se creó el mercado de equipos móviles.[1] Sin embargo, el aumento que se ha visto en la adopción de teléfonos móviles, especialmente con la introducción de los teléfonos inteligentes o smartphones, ha ocasionado un rápido incremento del número de delitos relacionados con equipos móviles en la región. El número de dichos equipos robados pasó de 2.1 millones a 3 millones entre 2009 y 2010–un incremento del 43%.[2] Pese a los esfuerzos por controlarlo, este hurto sigue siendo un fenómeno persistente en toda la región y los números continúan en aumento. En Colombia el robo de celulares fue el delito de más rápido crecimiento durante la primera mitad de 2017 y mas de 1.3 millones de dispositivos robados fueron reportados a las autoridades en 2017 [3], mientras que en Argentina se robaron más de 4.700 teléfonos diariamente en 2016 y en Perú cerca de 6.000 teléfonos móviles fueron robados cada día en 2017. [4]

El crecimiento de este problema y el hecho de que tales robos están acompañados usualmente con actos de violencia[5], ha sido reconocido por la industria, los entes reguladores y el público Esto ha llevado a los gobiernos de las Américas a promulgar políticas dirigidas a combatir el fenómeno. Pero las Américas no están solas al confrontar este problema; organizaciones regionales e internacionales han propuesto iniciativas para afrontarlo, en tanto que los gobiernos de otros países también están adoptando medidas para mitigarlo.

Algunos países de américa latina adoptaron tempranamente políticas dirigidas a identificar equipos hurtados o no autorizados (por medio de las llamadas listas negativas o “listas negras”) y otras que restringen el uso de las redes únicamente a equipos legítimos verificados (por medio de las llamadas listas positivas o “listas blancas”) para enfrentar el hurto de móviles. Desde 2011 los gobiernos latinoamericanos han promulgado políticas dirigidas a combatir el hurto de dispositivos móviles que incluyen la inclusión de dispositivos en listas negativas y listas positivas según su número IMEI. Actualmente más de 18 países han adoptado políticas relacionadas con el hurto de dispositivos móviles.[6] Muchos de estos países han adoptado un enfoque amplio al respecto, centrado no sólo en equipos hurtados, sino también en las imitaciones falsas y en

[1] Salvo si se indica otra cosa, la mención de robo de móviles se refiere al hurto de dispositivos que tienen un número IMEI (International Mobile Equipment Identity) [identidad internacional de equipo móvil] asignado que accede a las redes móviles de telecomunicaciones. Por la naturaleza de las medidas adoptadas, el enfoque se centra únicamente en los dispositivos con IMEI que se conectan a redes móviles. En el discurso popular sobre el tema, en el que participan el público y los entes reguladores, el enfoque se da abrumadoramente en los teléfonos móviles.

[2] CRC, “Condiciones Regulatorias para el Control del Uso De Equipos Terminales Móviles Hurtados y/o Extraviados”, junio de 2011, p. 3, disponible aquí. Se consultó en octubre de 2017.

[3] Fiscalía General de Colombia, “Comunicado de prensa: El bloqueo de los IMEI de los celulares no está funcionando”, 4 de agosto de 2017, disponible aquí. Se consultó en octubre de 2017.Al. Caracol Radio. “Ni el bloqueo de IMEI ni los operativos han servido: robo de celulares sigue disparado en Colombia” Disponible aquí. Recuperado en octubre de 2017

[4] Ver La Nación, “Por día se roban 5000 celulares en la Argentina”, 26 de julio de 2016, disponible aquí. Se accedió en octubre de 2017.

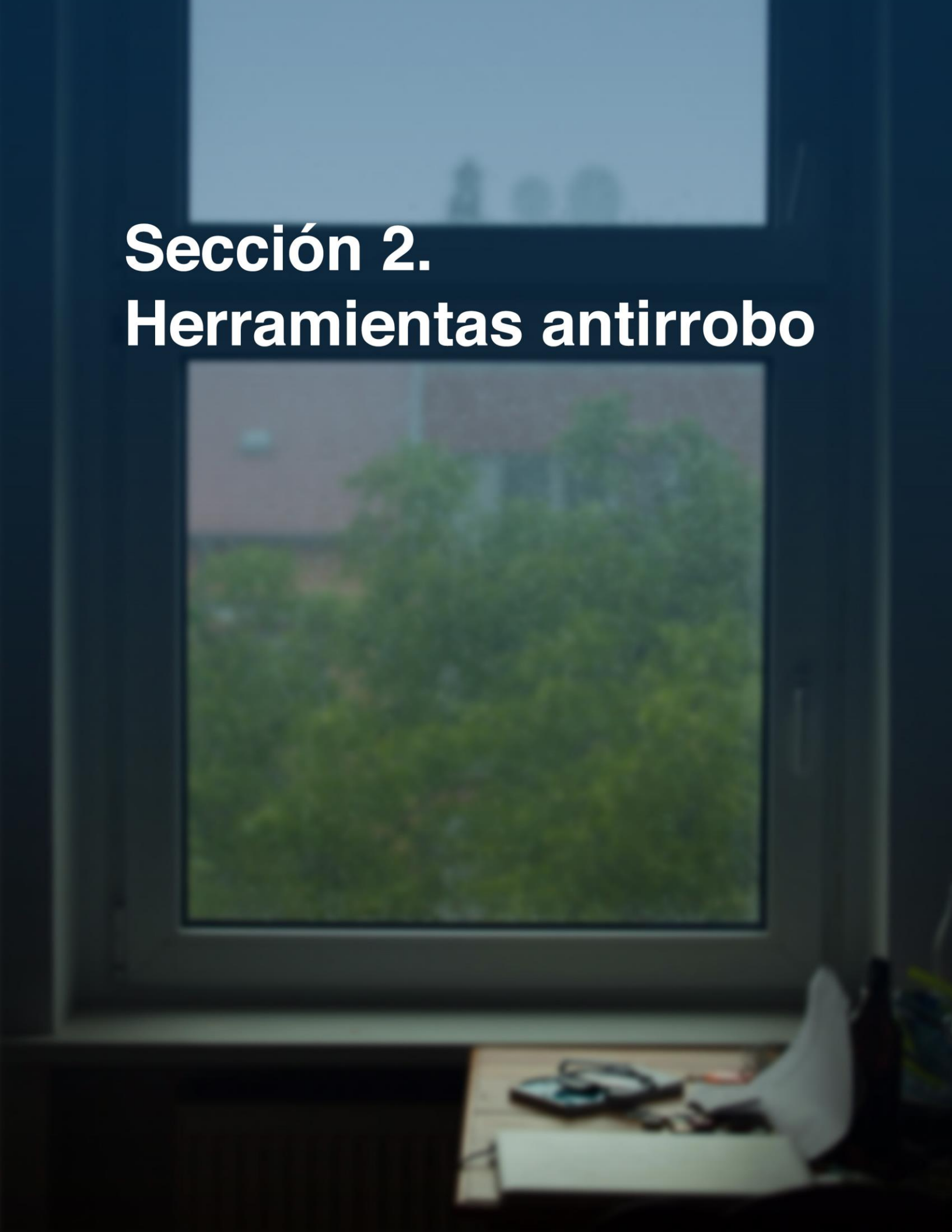
[5] Ver por ejemplo, Fiscal General de Nueva York, “Secure our Smartphones” [“La seguridad de nuestros teléfonos inteligentes”], 2014, pg. 11, disponible aquí, y El Tiempo, “En video quedó registrado el asesinato de joven misionero en Cali”, 21 de octubre de 2016, disponible aquí. Consultado en octubre de 2017.

[6] CITEL, PCC.I/Doc 4477/17 (XXXI-17) “Boletín Trimestral CITEL Intercambio y Bloqueo Equipos Hurtados 1Q2017”, julio de 2017.

equipos fraudulentos. Aunque son bien intencionadas, estas políticas a menudo han generado sus propios inconvenientes incluyendo molestias para los usuarios, incremento de costos en las empresas, mientras que no necesariamente han sido eficaces en cuanto a reducir el robo. Además, las políticas basadas en listas, adoptadas por muchos países, no están diseñadas para tratar todos los aspectos del mercado de equipos robados, como por ejemplo el mercado negro de componentes de dispositivos robados.

Este informe hace un repaso general de las medidas tomadas en las Américas para combatir el hurto de dispositivos móviles y evaluar la efectividad de las mismas. La Sección 2 – Herramientas Antirrobo - trata las principales herramientas empleadas para combatir el hurto de estos dispositivos y compara sus fortalezas y debilidades. La Sección 3 – Iniciativas actualmente en curso en América Latina- examina más de cerca los enfoques adoptados por los gobiernos latinoamericanos y la región en general para contrarrestar el hurto de dispositivos y evalúa la efectividad de dichas medidas. La Sección 4 -La tecnología ofrece una mayor solución- examina cómo mejorar la efectividad de los esfuerzos antirrobo y la Sección 5 – Conclusiones- presenta las conclusiones del informe.

Sección 2.
Herramientas antirrobo



2 Herramientas antirrobo

Respondiendo al problema actual del hurto de dispositivos móviles, los encargados de las políticas públicas y la industria han desarrollado soluciones dirigidas a hacer menos atractivos los equipos móviles para ladrones y compradores potenciales. Estas soluciones generalmente se pueden clasificar en dos categorías: medidas de bloqueo basadas en el IMEI y soluciones técnicas. Las primeras han sido aplicadas ampliamente en toda la América Latina, mientras que, hasta la fecha, las soluciones técnicas han sido empleadas más en Norteamérica y Europa.

2.1 Medidas que bloquean el IMEI – Listas negativas y Listas positivas

Si bien existe cierto nivel de coordinación regional en la lucha contra el hurto de dispositivos móviles, las medidas legislativas y las regulaciones se adoptan a nivel nacional. El resultado de todo esto es un complejo contexto de sistemas, leyes y regulaciones que tratan el mismo tema de diferentes maneras. En términos generales, los sistemas se basan ya sea en listas de dispositivos bloqueados (listas negativas) o de dispositivos permitidos (listas positivas). Algunos países también incluyen otras categorías, tales como listas de dispositivos exportados.[7]

2.1.1 Listas negativas o "blacklists"

Las primeras políticas adoptadas en la región para combatir el hurto de equipos móviles buscaban impedir que los equipos robados, fraudulentos o extraviados pudieran conectarse a las redes móviles. En la práctica, este enfoque depende de una lista centralizada de dispositivos excluidos o lista negativa, que contiene los IMEI de los dispositivos reportados por los usuarios como robados o extraviados. Entonces las empresas operadoras impiden el acceso a sus redes de los dispositivos con los IMEI reportados. La idea detrás de este concepto es que, si no es posible usar estos equipos en las redes móviles, estos tendrán menor valor, lo cual a su vez reduce el incentivo de robarlos. La Asociación GSM (GSMA), una asociación mundial de empresas operadoras móviles, ha venido compilando una base de datos de lista negativa a nivel mundial desde 1996.[8]

Las listas negativas típicamente funcionan en múltiples niveles. Los consumidores o la policía, o ambos reportan los IMEI de dispositivos robados a las empresas operadoras, las cuales a su vez reportan esta información a la base de datos nacional o la comparten con todos los operadores del país. Luego los operadores sincronizan sus bases de datos con la base de datos global de la GSMA. El intercambio de datos con esa misma base de datos es gratuito para los miembros de la asociación y con frecuencia también se permite acceso de cortesía a los entes reguladores oficiales.[9] Muchos gobiernos exigen que el intercambio de información entre los operadores y la GSMA se dé como mínimo cada 24 horas, y en muchos casos, de manera aún más frecuente. De esta manera, si se reporta un teléfono robado en Brasil, por ejemplo, se puede bloquear la conexión del mismo a las redes de la vecina Argentina, golpeando así el comercio transnacional

[7] Por ejemplo, Perú mantiene una lista de dispositivos exportados. Ver el Capítulo III del Artículo 7 del Decreto Legislativo 1338/2017, disponible aquí. Se consultó en octubre de 2017.
[8] CITEL, PCC.I/Doc. 2311 (XVII-11) "GSMA Resources and Position to Support Regional Front to Combat the Theft of Mobile Terminal Equipment [Recursos GSMA y posición para apoyar un frente regional para combatir el hurto de equipos terminales móviles]," septiembre de 2011.
[9] Ver GSMA, "Coloured Lists" ["Listas a color"], disponible aquí, y GSMA, "Accessing the IMEI Database" ["El acceso a la base de datos de IMEI"], disponible aquí. Consultada en octubre de 2017.

de equipos robados. Sin embargo, las listas negativas funcionan mejor cuando sus contenidos están armonizados, si pueden garantizar la precisión de la información que contienen y si son ampliamente –si no uniformemente—aceptadas.

Las listas negativas se han implementado ampliamente en toda la región latinoamericana, pero no todos los operadores las usan, lo cual les resta efectividad. La Figura 1 muestra los operadores que están suscritos a la base de datos global de la GSMA de los IMEI que aparecen en la lista negativa. En América Latina, el número de suscripciones a la base de datos de la GSMA aumentó rápidamente luego de que la Comisión Interamericana de Telecomunicaciones (CITEL) expidió una resolución en el 2011 promoviendo medidas para combatir el hurto de dispositivos, como se comenta en la Sección 3.1.[10] CITEL es el organismo de la Organización de Estados Americanos que trata temas relativos a las telecomunicaciones, y se compone tanto de los gobiernos de las Américas como de los miembros asociados provenientes del sector privado. En la actualidad los operadores móviles de las Américas constituyen la mayoría de quienes participan en la lista negativa de la GSMA.

[10] CITEL, PCC.I/RES. 189 (XIX-11) “Regional Measures to Combat the Theft of Mobile Terminal Devices” [“Medidas regionales para combatir el hurto de equipos terminales móviles”], septiembre de 2011, disponible aquí.

Figura 1: Suscripción mundial a la Lista negativa de la GSMA

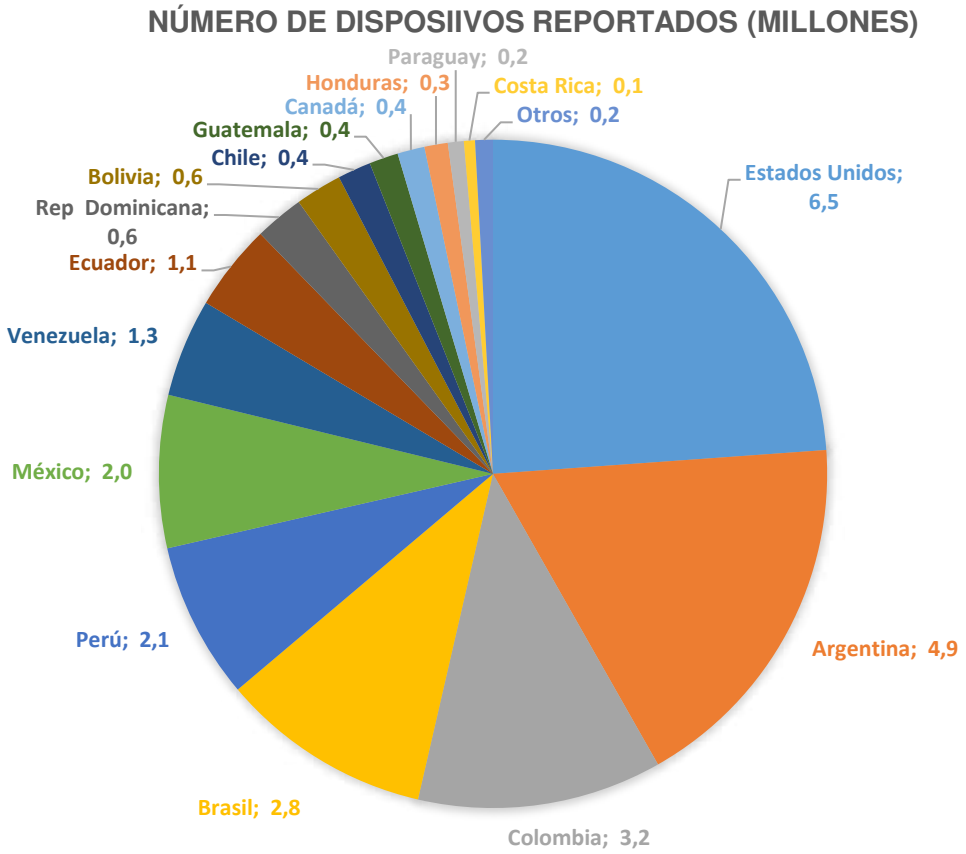
Fuente: TMG con base en datos de la GSMA

Actualmente la base de datos de IMEI de la GSMA tiene más de 39 millones de registros, reportados por los países de las Américas.[11] Esta base de datos ha crecido rápidamente, de la mano con una mayor adopción de la misma en la región, al igual que con el incremento en los hurtos y en la cantidad de equipos móviles en América Latina. En 2004 había menos de un millón de IMEI en esta base de datos.[12] La Figura 2 muestra el número de IMEI en lista negativa reportados por cada país de la región. Después de Estados Unidos, Argentina y Colombia tienen el mayor número de IMEI reportados, con 4.9 y 3.2 millones, respectivamente.

Figura 2: Número de IMEI reportados como extraviados o hurtados por cada país en la

[11] CITEL, PCC.I/Doc 4477/17 (XXXI-17) "Boletín Trimestral CITEL Intercambio y Bloqueo Equipos Hurtados 1Q2017", julio de 2017.
[12] Id.

región



Fuente: TMG con base en la GSMA[13]

Las listas negativas tienen ciertos beneficios que las siguen haciendo atractivas para quienes formulan políticas. Por ejemplo, la implementación de estas listas es relativamente conveniente para los usuarios, ya que únicamente les pide reportar dispositivos extraviados o hurtados. La única interacción adicional que se requiere del usuario final ocurre cuando se agrega un dispositivo legítimo a la lista negativa y el usuario debe resolver el error. Las listas negativas también se pueden diseñar para permitir coordinación no sólo entre distintas empresas operadoras, sino también entre países. El uso generalizado de las listas negativas y la disponibilidad de la lista negativa global de la GSMA, por ejemplo, constituyen un sistema establecido que le resulta atractivo a los encargados de formular políticas.

Sin embargo, las listas negativas también presentan desventajas y en un contexto más amplio, existe poca evidencia que compruebe la efectividad de las listas negativas en la reducción del hurto de dispositivos móviles, como se detalla en la Sección 3.5.

En cada país varía la forma en que se emplean las listas negativas para combatir el hurto de equipos, lo que crea una implementación de uniforme y desarmonizada. Algunos países, como por ejemplo Brasil, además de permitir que se reporten los equipos hurtados o extraviados a

[13]CITEL, PCC.I/Doc 4477/17 (XXXI-17) "Boletín Trimestral CITEL Intercambio y Bloqueo Equipos Hurtados 1Q2017", julio de 2017.

través de las empresas operadoras, también permiten que las autoridades inicien el proceso de bloqueo cuando se reporta un robo.[14] Otros países, como es el caso de Paraguay, obligan al usuario a reportar el equipo directamente a los operadores.[15] El tiempo fijado para cumplir también varía mucho entre los países. Brasil obliga a todos los operadores a bloquear un equipo durante las 72 horas siguientes a la radicación del reporte sobre el IMEI por el usuario, mientras que las regulaciones paraguayas ordenan a los operadores bloquearlos dentro de los siguientes 30 minutos.[16] Además, algunos países requieren detalles tales como el nombre del propietario y el número asociado al dispositivo, mientras que otros sólo piden registrar el IMEI. Si bien hay traslape entre el contenido de las listas negativas de los distintos países, cada uno tiene sus propias reglas sobre el bloqueo de teléfonos, y esto significa que algunos teléfonos que están bloqueados en un país pueden ser legalmente activados en otros. Finalmente, y por razonas prácticas, la mayoría de los países no descargan la totalidad de base de datos de la GSMA en sus listas negativas. Más bien se enfocan en la información de los países vecinos con los cuales tienen mayor probabilidad de intercambiar equipos, lo cual reduce la efectividad regional o global de la lista negativa. Sin embargo, algunas organizaciones criminales mueven los aparatos entre países distantes, o incluso entre regiones.[17] El intercambio selectivo de la información consignada en las listas negativas abre brechas que los delincuentes pueden explotar.

Adicionalmente, los ladrones de dispositivos han desarrollado estrategias que le restan efectividad a las listas negativas, como alterar el IMEI de los dispositivos que están en la lista para permitir su reconexión a las redes móviles, o simplemente trasladar los dispositivos a países que no comparten listas negativas con los países de los robos. Ante la habilidad de los ladrones para retirar equipos de las listas negativas unilateralmente, en América Latina se han contemplado otros enfoques, como por ejemplo las listas positivas o “listas blancas”.

Una lista negativa es valiosa únicamente si tiene información precisa sobre equipos hurtados, extraviados u otros equipos excluidos. Si una base de datos incluye errores tales como los que se derivan de reportes imprecisos o error humano al registrar los IMEI, puede llevar a que le sea negado el acceso a las redes a equipos legítimos, y en términos generales constituye un punto único de falla en el enfoque antirrobo. Además, los errores producidos por los administradores de las bases de datos pueden producir un efecto dominó cuando la base de datos de IMEI se relaciona con otras bases de datos, tales como de registro de equipos que no han sido homologados o que no tienen IMEI registrado o cuyo IMEI está duplicado, es inválido o no ha sido formateado, como ocurre en Colombia. Además, los errores cometidos en los procesos y la base de datos de un país pueden introducir errores en la base de datos de la GSMA, por ejemplo. Dado que las distintas bases de datos se actualizan múltiples veces al día, existen abundantes oportunidades para que los errores de un país produzcan errores más allá de las fronteras nacionales.

Otra desventaja potencial se deriva de los costos. No importa cómo maneje un país su lista negativa, crearla y mantenerla implica costos, al igual que coordinarla con otros países y/o con una base de datos centralizada como la de la GSMA. Incluir más información, además del número

[14] CITEL, PCC.I Doc. 4226p1 (XXX-17) “CCP.I/DEC. 254 (XXIX-16) – RESPUESTAS DE BRASIL”, abril de 2017.
[15] Ministerio de Obras Públicas y Comunicaciones, Decreto 6728/2017, disponible aquí. Consultado en octubre de 2017.
[16] Ver Paraguay, Ministerio de Obras Públicas y Comunicaciones, Decreto 6728/2017, Capítulo IV, Art. 13, disponible aquí, y CITEL, PCC.I Doc. 4226p1 (XXX-17) “CCP.I/DEC. 254 (XXIX-16) – RESPUESTAS DE BRASIL”, abril de 2017.
[17] Ver por ejemplo: Salinas, Lucía “Celulares y autopartes, de Colombia al mercado negro de Argentina”, Clarín, 13 de mayo de 2014, disponible aquí. Consultado en octubre de 2017.

IMEI, como por ejemplo los números de los abonados e información personal de los clientes, puede ampliar el tamaño de la base de datos y así mismo el costo de su mantenimiento. En varios países son los operadores móviles (y de esta manera, en últimas, los usuarios) quienes asumen el costo del mantenimiento de las listas de IMEI bloqueados y de la sincronización de las bases de datos con la de la GSMA. Vale resaltar por ejemplo, que el costo de acceder a la base de datos de la GSMA varía mucho según el tipo de acceso y el estado del suscriptor, pero sí puede implicar el pago de una tarifa, y este costo en últimas lo pagan los consumidores en tarifas más altas que pagan por los servicios. Incluso en los casos en que las bases de datos son responsabilidad de los gobiernos o cuando éstas están subsidiadas, los costos no son insignificantes y se hace necesario comprometer recursos públicos que pueden ser escasos. Con frecuencia las bases de datos las mantienen contratistas privados a quienes les pagan los operadores participantes, y éstos últimos incluyen estos costos en los precios que cobran por sus servicios.

Es posible mejorar las listas negativas para que permitan identificar IMEI clonadas y duplicadas, si para ello también se registra otra información como los números de las tarjetas SIM y números de abonado, si bien estos enfoques aumentan la complejidad de la base de datos.

2.1.2 Listas positivas o “whitelists”

Los reguladores han venido ampliando progresivamente el alcance de las medidas que bloquean los IMEI[18] Al incluir el uso de las listas positivas. En contraste con las listas negativas, que impiden la conexión a la red de los equipos marcados como hurtados o extraviados, la lista positiva o “lista blanca” consta de los únicos equipos que están autorizados para conectarse a las redes móviles. La implementación de las listas positivas refleja la intención de tratar no sólo el hurto sino también el comercio de equipos ilegales, falsos y fraudulentos, así como de complementar las soluciones de listas negativas. Concretamente, las listas positivas buscan enfrentar la dificultad que implica usar listas negativas para capturar dispositivos cuyo IMEI ha sido alterado o que de otra forma es inválido.

Para ser incluido en una lista positiva –y así poderse conectar a una red— los equipos deben cumplir con criterios específicos, tales como ser registrados tanto por los importadores de equipos como por los usuarios finales, lo cual les agrega más obligaciones a estos dos actores clave.

En muchos casos es posible completar el registro en las listas positivas en línea,[19] lo cual implica una carga significativa para los usuarios que no cuentan con acceso fácil a Internet. En algunos casos se debe hacer el registro personalmente. En Argentina, todos los equipos deben estar asociados con la información personal del usuario,[20] información que debe incluir el Documento Nacional de Identidad (DNI) del usuario. Los ciudadanos extranjeros que no poseen un DNI

[18] En Ecuador, los datos de 2012 indican que únicamente el 52% de los IMEI reportados a la lista negativa fueron bloqueados, principalmente debido a la presencia de múltiples dispositivos con el mismo IMEI. El ente regulador citó este hecho como parte de la razón por la cual se necesitaba una lista positiva. Ver CITEL, PCC.I Doc. 3655 (XVII-15) “Carpeta Técnica: Terminales Móviles Robadas y Perdidas,” septiembre de 2015.
[19] CRC, “Como Registrar tu celular?” disponible aquí. Consultado en octubre de 2017.
[20] ENACOM, Resolution 8507/2016, December, 2016, disponible aquí. Consultado en octubre de 2017.

deben presentar personalmente su pasaporte para verificar su autenticidad y lograr así activar su dispositivo en la red.[21]

Además de registrar al consumidor, los países que emplean la opción de la lista positiva requieren que se registren todos los dispositivos nuevos que se venden en el país. En Perú y Colombia, por ejemplo, los importadores deben registrar y reportar todos los IMEI de los dispositivos vendidos en esos países.[22] Si esos IMEI ya aparecen en alguna lista negativa o lista positiva, incluso por error o porque dispositivos fraudulentos se han apropiado los IMEI de equipos legítimos que aún no han sido importados al país, los dispositivos importados no se pueden vender legalmente en el país. Los requisitos de la información que se debe registrar en una lista positiva varían ampliamente entre los países. En Chile, por ejemplo, los importadores no sólo deben reportar los IMEI de los equipos importados, sino también las versiones de software instaladas.[23]

En contraste con las listas negativas, existe muy poca coordinación regional de listas positivas, y los países no comparten ampliamente dicha información. Cada país que tiene una lista positiva de IMEI desarrolla sus requisitos de cumplimiento, lo cual lleva a que este enfoque sea aún menos uniforme que el de las listas negativas. Incluso si se compartiera la información, la variedad de estándares, composición y prácticas de reportes que presentan las listas positivas indica que sería extremadamente difícil armonizar las listas positivas de múltiples países tal como éstas se encuentran hoy. Muchos menos países tienen listas positivas que negativas, pero aun así algunos entes reguladores de países que no tienen listas positivas han indicado que las están considerando como opción.[24] Dado que el hurto de equipos móviles sigue siendo motivo de preocupación para el público, es probable que se sigan implementando las listas positivas en la región.[25]

Es más difícil implementar una lista positiva que una negativa. Comparadas con las listas negativas, las positivas generalmente cuestan más, son más complejas y causan más incomodidad a los usuarios. Técnicamente es más difícil implementar listas positivas porque, además de los dispositivos nuevos que ingresan al mercado, se deben agregar a la lista todos los dispositivos legítimos que existan cuando ésta es implementada. Esto requiere una campaña concertada de generación de conciencia para motivar a los usuarios a registrar sus equipos. Este reto de motivar a los usuarios a que registren sus dispositivos llevó a Colombia a introducir su lista positiva en forma escalonada durante cuatro años, entre mayo de 2013 y julio de 2017.[26] Incluso con grandes campañas de concientización, resulta inevitable ocasionar molestias a los consumidores.

---

[21] Id.
[22] Ver Perú, Decreto Legislativo 1338/2017, disponible aquí, y Colombia, Ministerio de Comercio, Industria y Turismo, Decreto 2025/2015, disponible aquí. Consultado en octubre de 2017.
[23] Subsecretaría de Telecomunicaciones (SUBTEL), Resolución 1463, Artículo 3, junio de 2016, disponible aquí. Consultada en octubre de 2017.
[24] Las consultas efectuadas con el regulador de Paraguay, CONATEL, indicaron que aunque el país todavía no emplea una lista blanca, están contemplando implementarla y evaluar la conveniencia potencial de la misma para los usuarios.
[25] En el año de 2017, el ente regulador peruano, OSIPTEL, se basó en el hecho de que 8 de cada 10 ciudadanos temían ser víctimas de hurto de dinero, de la billetera o del teléfono móvil para justificar una nueva política de lista positiva en el Perú. Ver el Decreto Legislativo 1338/2017, disponible aquí. Consultado en octubre de 2017.
[26] CITEL, PCC.I Doc. 4303p1 (XXX-17) CRC: “Avances del Sistema de Control de IMEI en Colombia,” abril de 2017.

Incluso si no hay lista positiva, algunos países exigen a los operadores desconectar equipos que no cumplen con ciertas condiciones. Por ejemplo, Argentina ha iniciado un proceso de bloqueo de líneas telefónicas "anónimas" que carecen de información sobre la identidad de los respectivos usuarios de las mismas.[27] Este enfoque toma prestados algunos de los aspectos de las listas positivas, concretamente el hecho de que los equipos deben cumplir con ciertas condiciones para conectarse a la red, pero sin mantener de hecho una lista positiva. En el caso de Argentina, los equipos asociados a líneas anónimas se agregan a la lista negativa nacional.

Las listas positivas también ocasionan complicaciones imprevistas a los usuarios de dispositivos legítimos. La Comisión de Regulación de las Comunicaciones (CRC) de Colombia observa que, entre otras formas de alterar los números IMEI, sus listas positivas también incluyen los duplicados de números IMEI legítimos. En estos escenarios, se bloquean los dos equipos con número IMEI duplicado, ya que no hay forma de saber cuál es el usuario legítimo. Este sistema lleva a desconectar de las redes a usuarios inocentes y legítimos cuyos IMEI han sido duplicados. En Colombia el problema de los IMEI duplicados es generalizado. En julio de 2017 el Ministerio de las Tecnologías de la Información y las Comunicaciones (MINTIC) estimó que en Colombia hay 925.000 equipos con IMEI duplicado.[28]

El alto grado de precisión necesario para el éxito de las listas positivas, combinado con el bajo porcentaje de hurtos que se denuncian a la policía y a los operadores móviles en Latinoamérica, reducen notoriamente la efectividad del sistema. Dado que muchos robos no son reportados, es inevitable que las listas positivas incluyan muchos equipos robados nunca reportados como tales. Resulta imposible conocer el alcance de este problema. Además, es necesario fijar procedimientos apropiados para retirar de las listas positivas a los IMEI que han sido aprobados mediante fraude o por error.

Además, las listas positivas --y hasta cierto grado también algunas listas negativas-- crean grandes bases de datos de información personal, lo cual genera el riesgo de un acceso no autorizado a esa información. Y más allá del acceso criminal a dichas bases de datos, existe también el riesgo del error humano y de medidas de control ineficaces para proteger los datos personales del acceso por usuarios no autorizados. En un ejemplo de las implicaciones de estas medidas para la privacidad de los datos, la concentración de información que identifica a los usuarios de un equipo particular con información técnica sobre ese equipo, incluyendo el IMEI, le permitiría a los gobiernos, en un momento dado, rastrear la ubicación de un grupo de personas con base en la ubicación de la señal de sus dispositivos móviles.[29] El costo que implica el desarrollo y mantenimiento de protocolos de seguridad apropiados agrega costos y complejidad a la solución de las listas positivas, y pese a los mejores esfuerzos en este sentido, es muy poco probable que una base de datos de este tipo pueda ser protegida íntegramente.[30]

---

[27] ENACOM, Resolución 8507/2016, diciembre de 2016, disponible aquí. Consultada en octubre de 2017.
[28] MINTIC, "49,6 millones de celulares fueron registrados en Colombia", 14 de julio de 2017, disponible aquí. Consultado en octubre de 2017.
[29] Ver Castañeda, Juan Diego, "Un Rastreador en tu Bolsillo", Fundación Karisma, julio de 2017, pp. 24-25, disponible aquí. Consultado en octubre de 2017.
[30] En el Reino Unido los ciberataques dejaron expuestos los datos de millones de suscriptores de las empresas operadoras locales en el 2016. Ver McGoogan, Cara y Swinford, Steve, "Three Mobile cyber hack: six million customers' private information at risk after employee login used to access database" ["Tres ciber hacks móviles: seis millones de [unidades de] información privada de los clientes puestas en riesgo al usarse el login de empleado para acceder a la base de datos"], The Telegraph, 18 de noviembre de 2016, disponible aquí. Consultado en octubre de 2017.

Las listas positivas también imponen restricciones al movimiento legal de equipos en la región. Por ejemplo, un equipo legítimo transportado desde el Perú para venderse en Colombia debe ser retirado de la lista positiva peruana al dejar Perú y registrado nuevamente en la lista positiva al ingresar a Colombia. Un equipo que está aprobado en un país no va a ser aprobado automáticamente en otro. Así, las listas positivas restringen el movimiento de equipos en la región y limitan la facilidad con la que un equipo se puede conectar a las redes de múltiples países.

La implementación y el mantenimiento de estas listas genera cargas a los usuarios, sin ofrecer un claro beneficio a cambio. Además de los retos asociados a la implementación y el mantenimiento de las listas positivas, hay poca evidencia de que realmente puedan reducir el hurto de equipos. De hecho, tal como organizaciones de la sociedad civil como la Fundación Karisma en Colombia han podido observar, concentrar información personal valiosa en las listas positivas puede poner en riesgo a los usuarios de los dispositivos ante otras formas de hurto derivadas de la pérdida o el tratamiento inadecuado de dichos datos.[31]

2.2 Soluciones técnicas

En comparación con las soluciones de bloqueo de los IMEI que exigen los gobiernos y coordinan las empresas operadoras, los enfoques técnicos dirigidos a combatir el hurto de equipos móviles no dependen del bloqueo ni de la aprobación de los IMEI. Estos enfoques han demostrado ser capaces de ejercer un impacto significativo en la tasa de hurtos de equipos. Han sido los fabricantes quienes han asumido el liderazgo al respecto, al desarrollar y utilizar estas soluciones técnicas para mitigar el hurto de equipos, como lo evidencia el compromiso asumido por la industria en los Estados Unidos a través del Smartphone Anti-Theft Voluntary Commitment [Compromiso Voluntario Anti Hurto] (CTIA) para abordar el problema en los Estados Unidos. El compromiso fue firmado por 16 empresas operadoras, fabricantes y otras partes interesadas de Estados Unidos y se cumplió en el año 2015, lo cual agregó otra dimensión a las medidas dirigidas a combatir el hurto de dispositivos a escala global.[32] Mientras que en los Estados Unidos hubo una amplia difusión de información sobre esta iniciativa, las soluciones técnicas en la América Latina han recibido comparativamente poco apoyo significativo.

La solución técnica más frecuente es una herramienta antirrobo ubicada en el dispositivo, que ha sido denominada "*killswitch*" o mecanismo de desactivación total. Esta solución ha demostrado ser capaz de reducir las tasas de robo. Si bien la funcionalidad específica de esta característica varía según los dispositivos, generalmente viene preinstalada o se puede descargar en los teléfonos inteligentes y le permite al usuario bloquear el teléfono remotamente, borrar su contenido o impedir el uso del mismo, haciéndolo inutilizable, y estas soluciones producen efecto inmediato. De manera similar, los usuarios también pueden reactivar fácil e instantáneamente un dispositivo recuperado sin necesidad de que intervenga la empresa operadora y sin necesidad de hacer cambios en una base de datos centralizada.

Los principales actores en la industria, incluyendo Apple y Samsung, adoptaron tempranamente esta tecnología antirrobo en el año 2013 y 2014 respectivamente. Un informe de 2014 del Fiscal General del Estado de Nueva York encontró que en Londres y San Francisco el hurto de productos Apple se redujo un 24% en Londres y un 38% en San Francisco durante los seis meses

[31] Castañeda, Juan Diego, "Un Rastreador en tu Bolsillo", Fundación Karisma, julio de 2017, pp. 24-25, disponible aquí. Consultado en octubre de 2017.
[32] CTIA, "Smartphone Anti-Theft Voluntary Commitment" ["Compromiso Voluntario Antirrobo"], abril de 2014, disponible aquí. Consultado en octubre de 2017.

siguientes a la introducción de esta tecnología del botón de desactivación total o "killswitch".[33] Durante ese mismo período, el robo de productos Samsung, empresa que aún no había incorporado ampliamente esta tecnología, aumentó un 3% en Londres y un 12 % en San Francisco.[34] Durante el año siguiente a la introducción de este mecanismo de desactivación en los teléfonos inteligentes por parte de múltiples fabricantes, el hurto de teléfonos celulares se redujo un 16% en Nueva York, un 27% en San Francisco y un 38% en Londres.[35]

En los Estados Unidos, un estudio de 2015 de Consumer Reports sobre el hurto de dispositivos móviles encontró que el hurto de teléfonos inteligentes disminuyó de 3.1 millones en el 2013 a 2.1 millones en 2014.[36] Esta reducción correspondió con la introducción del botón de desactivación total por parte de muchos fabricantes. Los resultados no demuestran que dichos mecanismos "killswitch" ocasionaron la reducción, pero los autores consideran que la reducción sí se debió al menos en parte a la introducción de esta tecnología antirrobo. Estas estadísticas sugieren que la tecnología antirrobo puede ser un importante factor disuasivo contra el robo de dispositivos, que además no le agrega costos ni a operadores, usuarios ni a gobiernos y entes reguladores.

Resulta claramente beneficioso para todas las partes interesadas adoptar tanto como sea posible esta solución, que está fácilmente disponible, para reducir el robo de dispositivos.

Como se ha mencionado anteriormente, otra característica importante de la tecnología antirrobo es que permite a los usuarios borrar los datos del teléfono. En una era en que los teléfonos inteligentes guardan cada vez más información delicada e importante, protegerla puede ser igual o incluso más importante para el usuario que la suerte que corra el dispositivo mismo.

Una desventaja del "killswitch" o mecanismo de desactivación y de soluciones similares es que únicamente se pueden usar en teléfonos inteligentes. Por lo tanto, únicamente pueden ser empleados para disuadir el hurto de teléfonos inteligentes y éstos constituían aproximadamente el 50% del mercado móvil latinoamericano en 2016.[37] Sin embargo, se espera que esta cifra suba al 70% para el año 2020.[38] Adicionalmente, En algunos países los teléfonos inteligentes ya dan cuenta de la gran mayoría de las ventas de teléfonos móviles. En Brasil en 2016, por ejemplo, 9 de cada 10 teléfonos móviles vendidos fueron teléfonos inteligentes.[39] Además, la mayoría de esos aparatos se vendieron con tecnología antirrobo instaladas de fábrica o con la posibilidad de

---

[33] New York State Attorney General [Fiscal General de Nueva York], "Secure our Smartphones" ["La seguridad de nuestros teléfonos inteligentes"], 2014, disponible aquí. Consultado en octubre de 2017.
[34] Id.
[35] San Francisco District Attorney, "Press Release: A.G. Schneiderman, London Mayor Johnson and D.A. Gascon Welcome Dramatic Global Drop in Smartphone Thefts Following Introduction of Kill Switch" ["Nota de prensa: El Fiscal de Distrito Scheiderman, el Alcalde de Londres Johnson y el Fiscal de Distrito Gascon Celebran la Reducción Dramática en el Robo de Teléfonos Inteligentes Tras la Introducción del Mecanismo de Desactivación"] February 11, 2015, disponible aquí. Consultado en octubre de 2017
[36] Consumer Reports, "Smart phone thefts rose to 3.1 million in 2013" ["El hurto de teléfonos inteligentes subió a 3.1 millones en el 2013], mayo de 2013, disponible aquí, y "Smartphone thefts drop as kill switch usage grows" ["Se reduce el hurto de teléfonos inteligentes al aumentar el uso del mecanismo de desactivación "kill switch"], junio de 2015, disponible aquí. Consultado en octubre de 2017.
[37] GSMA, "The Mobile Economy Latin America and the Caribbean 2016" ["La economía móvil en América Latina y el Caribe en el 2016"], 2017, disponible aquí. Consultado en octubre de 2017.
[38] Id.
[39] Counterpoint Research "Despite Recession, Brazil LTE Smartphones Grew 53% Annually in 2016" ["Pese a la recesión, los teléfonos inteligentes LTE en Brasil crecieron un 53% anual en 2016"], 3 de marzo de 2017, disponible aquí. Consultado en octubre de 2017.

descargarla de Internet.[40] A medida que la penetración de los teléfonos inteligentes en América Latina sigue aumentando rápidamente, la gran mayoría de los dispositivos móviles de la región tendrá incluida tecnología antirrobo. Estas tendencias deben ser cuidadosamente consideradas por las partes interesadas para poder darle el mejor uso posible a todas las herramientas que están disponibles para disuadir el hurto de equipos.

Una segunda desventaja de las tecnologías de mecanismo de desactivación o "killswitch" es que requieren que el usuario active este servicio, mediante selección expresa de la opción respectiva ["opt-in"], antes de que el dispositivo se extravíe o sea hurtado. Este enfoque es necesario porque el propietario de un dispositivo nuevo debe pasar por el proceso de registro o de alguna forma de vinculación del dispositivo al servicio antirrobo, para habilitar así a un dispositivo distinto (como un PC o el teléfono celular de un amigo) para que éste último, remotamente, pueda ubicar o deshabilitar el dispositivo extraviado o hurtado, o borrarle toda la información que contiene. Si el equipo móvil es hurtado o extraviado antes de que el usuario active el servicio antirrobo, no se podrá deshabilitar ni desactivar remotamente. Sin embargo, los ladrones no tienen manera de saber de antemano si el usuario ha seleccionado la opción del servicio antirrobo, y esto precisamente hace que todos los teléfonos inteligentes con tecnología antirrobo sean igualmente poco apetecibles o poco atractivos para los ladrones.

Aunque la mayor parte del cubrimiento de prensa y de la investigación sobre las soluciones de mecanismo de desactivación o "killswitch" se refiere a los Estados Unidos y el Reino Unido, la funcionalidad está disponible para todos los usuarios de teléfonos inteligentes a nivel mundial, en virtud de que es posible habilitarla mediante una aplicación que se puede descargar de Internet. En América Latina, sin embargo, son pocos los esfuerzos que han dedicado las empresas operadoras, los gobiernos o las entidades reguladoras para educar al consumidor sobre la disponibilidad de estas herramientas.

Tabla 1: Comparación de las soluciones disponibles

	Beneficios	Desventajas
Listas negativas o "Blacklists"	• Menos incómodas para los usuarios que las listas positivas. • Se pueden coordinar a nivel regional e incluso global. • Ya están ampliamente implementadas y aceptadas por los reguladores y los operadores.	• Poca evidencia que indique que las listas negativas reduzcan o impidan el robo. • No se aplican uniformemente en la región, lo cual genera problemas de armonización. • Requieren informes precisos, lo cual rara vez se da. • Los ladrones han desarrollado contramedidas o "atajos" (duplicación y alteración de IMEI, traslado de dispositivos robados a otros países) • Alto nivel de exigencia de mantenimiento de base de datos

[40] Durante el primer trimestre de 2017 los dispositivos Android e iOS, todos los cuales cuentan con tecnología antirrobo, constituyeron el 99.7% del mercado global de smartphones. Ver International Data Corporation "Smartphone OS Market Share, 2017 Q1" ["Participación en el mercado de los sistemas operativos de smartphones, 2017, T1"], disponible aquí. Consultado en octubre de 2017.

	Beneficios	Desventajas
		e infraestructura, así como en costos.
Listas positivas o "Whitelists"	• Pueden incluir dispositivos con IMEI no formateados o duplicados que son tipos de fraude que a veces ignoran las listas negativas.	• Los requisitos de registro incomodan a los usuarios. • Dificultad de aplicación por el requerimiento de añadir teléfonos actuales a la lista blanca. • No se aplican uniformemente en la región, lo cual genera problemas de armonización y fragmentación del mercado regional de dispositivos. Pueden obstaculizar el movimiento transfronterizo de dispositivos, incluso el legítimo. • Con frecuencia se combinan con requerimientos de importación y exportación que son onerosos para los negocios. • Requieren alto nivel de precisión en la base de datos para ser eficaces. • Su efectividad no está comprobada. • Altos costos iniciales asociados a la infraestructura necesaria para procesar, registrar y almacenar la información de todos los dispositivos del país. • Altos costos permanentes asociados al personal y la infraestructura necesarios para registrar los datos de todos los dispositivos importados.
Mecanismo de desactivación total o "Killswitch"	• Impide la conexión a la red del dispositivo hurtado. • Puede borrar la información personal de los equipos robados y proteger la privacidad del usuario. • De fácil acceso mediante apps descargables o preinstaladas. • Controlado por el usuario. • NO requiere incómodos procesos de reporte.	• Funciona únicamente con teléfonos inteligentes o smartphones, no con los convencionales [feature phones]. América Latina tiene un porcentaje importante de teléfonos móviles convencionales. • Con frecuencia requiere selección explícita por parte del usuario [user opt-in]. • No funciona si el teléfono está apagado o en modo avión.

	Beneficios	Desventajas
	• No implica costos de mantenimiento o adopción de bases de datos para los gobiernos. • No hay problemas transfronterizos ni de armonización regional. • Fácilmente reversible cuando se recupera el dispositivo.	

2.3 Papel de los organismos de seguridad

Además de las soluciones que bloquean el IMEI y las que emplean tecnología, los organismos de seguridad son participantes clave en la lucha contra el hurto de equipos. Idealmente los organismos de seguridad podrían enfocarse en los aspectos del uso de los dispositivos que permiten la proliferación del robo a gran escala, tales como la modificación sistemática de los IMEI de equipos robados y el ingreso de equipos ilegales a un país. Sin embargo, los enfoques adoptados actualmente en América Latina no han logrado reducir significativamente el robo, como se plantea en la Sección 3.5, y esto ha llevado a una situación en que los organismos de seguridad deben comprometer recursos para recibir denuncios sobre el hurto de dispositivos y rastrear los dispositivos robados.

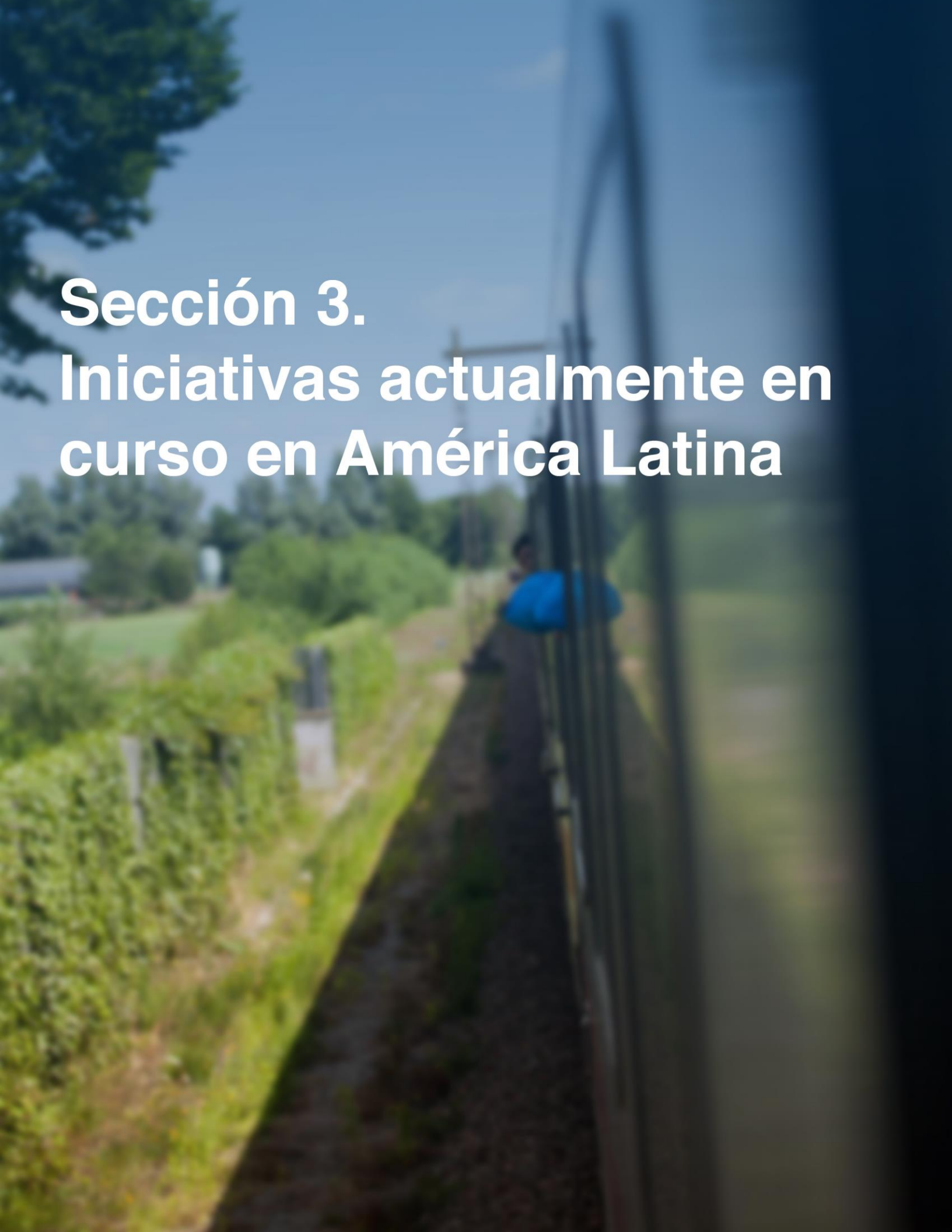
Si bien el hurto constituye un delito en los países en donde el hurto de equipos móviles es un problema, no todas las acciones que hacen parte del ciclo de vida de los dispositivos robados reciben igual prioridad por parte de los organismos de seguridad. Esto es especialmente válido para la clonación o modificación de los números IMEI de los equipos, un componente clave de la actividad criminal de los dispositivos robados que sólo recientemente se ha tipificado como delito en muchos países.[41] Las actividades que permiten a los equipos robados reingresar al mercado y frecuentemente presentarse como actividades legítimas, deben combatirse con el mismo rigor con que se enfrenta el robo mismo. Resulta esencial asociarse con los organismos de seguridad para combatir el mercado negro de equipos robados. En el Ecuador, la información recabada en el proceso de bloqueo de dispositivos sobre las ubicaciones donde se pueden estar vendiendo equipos robados, se comparte con los organismos de seguridad.[42] Las fuerzas policiales de Buenos Aires también han empleado esta técnica para identificar almacenes que venden dispositivos robados.[43] Esta clase de cooperación, que hace uso de la información que poseen los operadores con el fin de rastrear actividades ilegales, es un ejemplo del papel positivo que pueden ejercer los organismos de seguridad.

[41] Ver por ejemplo Honduras, en donde el Senado aprobó medidas para sancionar la modificación de IMEI en agosto de 2017. Congreso Nacional, "Congreso Nacional aprueba decreto que sanciona fuertemente a quienes clonen IMEI de teléfonos celulares", disponible aquí. Consultado en octubre de 2017.
[42] CITEL, PCC.I Doc. 3655 (XVII-15) "Carpeta Técnica: Terminales Móviles Robadas y Perdidas", septiembre de 2015.
[43] Ver: Vía Buenos Aires, "La Policía busca a los dueños de 2.500 celulares que fueron recuperados", 12 de mayo de 2017, disponible aquí. Consultado en octubre de 2017.

Si bien los organismos de seguridad juegan un papel clave al apoyar la búsqueda de una solución al hurto de equipos móviles, en algunos casos también pueden acabar menoscabando los esfuerzos dedicados a combatir el mismo robo. En la República Dominicana, la ley requiere que los usuarios notifiquen a las empresas operadoras sobre los equipos robados.[44] Sin embargo, con frecuencia la policía aconseja a los consumidores no hacerlo, con la esperanza de usar la señal del dispositivo para rastrear su ubicación.[45] Esta clase de mensajes contradictorios menoscaba el éxito del enfoque entero de lucha contra el robo. Para tener éxito, es necesario que operen de manera concertada los organismos de seguridad, las entidades reguladoras y las empresas operadoras.

Una implementación de las soluciones tecnológicas a mayor escala modificaría el papel de los organismos de seguridad en cuanto al hurto de dispositivos y convierte a los usuarios individuales en participantes activos de los esfuerzos dirigidos a proteger sus propios equipos y sus datos. Opciones tales como los mecanismos de desactivación o "killswitch" le otorgan poder a los usuarios al permitirles ubicar y, si lo consideran necesario, borrar y desactivar sus dispositivos, al mismo tiempo que liberan los recursos de los organismos de seguridad de la obligación de investigar cada hurto individualmente. Según la información disponible sobre Estados Unidos y el Reino Unido, los enfoques basados en el mecanismo de desactivación han logrado reducir el hurto de equipos en términos generales, permitiéndole a los organismos de seguridad dedicar más tiempo y recursos a enfrentar actores más grandes del ecosistema de los equipos robados, incluyendo a los que alteran equipos y a los que los transportan y venden en grandes cantidades.

[44] CITEL, PCC.I Doc. 4226p2 (XXX-17) "Informe sobre la consulta de los procesos de intercambio y bloqueo entre países de los IMEI de dispositivos móviles con reporte de hurto o extravío", abril de 2017.
[45] Id.



Sección 3. Iniciativas actualmente en curso en América Latina

3 Iniciativas actualmente en curso en América Latina

3.1 Iniciativas regionales

El hurto de equipos es un problema transnacional, pues los teléfonos robados pueden ser trasladados con facilidad entre fronteras para evitar ser detectados, frecuentemente asociados con el crimen organizado.[46] Como lo han reconocido los gobiernos latinoamericanos, este tipo de crimen transnacional requiere iniciativas regionales. En el 2011, por iniciativa del gobierno colombiano, CITEL aprobó una resolución invitando a los Estados Miembros y miembros asociados a que "adopten, refuercen o complementen las medidas necesarias, cada uno en el ámbito de sus competencias, para contrarrestar el hurto de equipos terminales móviles y su activación y comercialización a nivel regional"".[47] Esto sirvió de punto de partida para generar una mayor actividad regional y cooperación sobre el tema. La resolución condujo a CITEL a conformar una Relatoría sobre el Control de Fraude, Prácticas Antirreglamentarias en Telecomunicaciones y Medidas Regionales Contra el Hurto de Equipos Terminales Móviles, dentro del Comité Consultivo Permanente I: Telecomunicaciones / Tecnologías de la Información y la Comunicación (PCC.I), para enfocarse en estos temas. Luego de las actuaciones de la Relatoría, el PCC.I solicitó a los Estados Miembros aportar actualizaciones sobre las medidas que están adoptando para tratar el fraude y el hurto de equipos móviles. Lo más destacado es un documento de trabajo que compila dichas medidas, el PCC.I Doc. 3655/15 rev.1 (XXVII-15), cuya última actualización se hizo en el 2015.[48] La Relatoría también ha celebrado talleres para tratar temas relativos al hurto de equipos, el más reciente de los cuales se celebró en marzo de 2016. El grupo abogó por un seminario sobre equipos falsos y robados, que se aprobó en abril de 2017 y que se celebrará conjuntamente con la próxima reunión del PCC.I fijada para marzo de 2018.[49]

La GSMA también ha sido muy proactiva con el desarrollo de una respuesta regional sobre este tema y ha tenido éxito al abogar por el intercambio de los datos de las listas negativas de los operadores. Dado que el 77% de los operadores de la región están conectados de alguna manera a la lista negativa de la GSMA, esto representa una de las respuestas regionales más integrales al hurto de dispositivos.[50]

En abril de 2013, la Comunidad Andina de Naciones (CAN), conformada por Bolivia, Colombia, Ecuador y Perú, publicó la Decisión 786, “Intercambio de información de equipos terminales móviles extraviados, robados o hurtados y recuperados en la Comunidad Andina de Naciones”

---

[46] El Comercio, “Las mafias movilizan los celulares robados entre los países de la Región,” 2014, disponible aquí.

[47] CITEL, PCC.I/RES. 189 (XIX-11) “Regional Measures to Combat the Theft of Mobile Terminal Devices” [“Medidas regionales para combatir el hurto de equipos terminales móviles”], septiembre de 2011, disponible aquí. Consultado en octubre de 2017.

[48] La creación del documento técnico fue aprobada por CITEL, PCC.I/RES. 217 (XXIII-13) “Technical Notebook on Stolen, Robbed and/or Lost Mobile Terminals” [Cuaderno técnico sobre terminales móviles hurtadas, robadas y/o extraviadas”], disponible aquí. Consultado en octubre de 2017.

[49] CITEL, PCC.I/RES. 280 (XXX-17) “Seminar on Control of Mobile Devices with Altered/Duplicate Identifiers” [Seminario sobre el control de dispositivos móviles con identificadores alterados o duplicados”], mayo de 2017, disponible aquí. Consultado en octubre de 2017.

[50] CITEL, PCC.I/Doc 4477/17 (XXXI-17) “Boletín Trimestral CITEL Intercambio y Bloqueo Equipos Hurtados 1Q2017” julio de 2017.

con el ánimo de crear un marco jurídico sobre el hurto de equipos entre los operadores móviles de la Comunidad Andina.[51] Sus decisiones son vinculantes para los miembros y se deben incorporar en la legislación de cada país. Según la Decisión 786, los proveedores móviles deben: (i) intercambiar información relacionada con equipos terminales móviles extraviados, robados o hurtados y recuperados a nivel comunitario; (ii) bloquear los equipos terminales móviles reportados como extraviados o hurtados; (iii) hacer uso de la base de datos de IMEI de la GSMA; y (iv) desarrollar información y campañas dirigidas a los usuarios móviles sobre la importancia y necesidad de reportar a los proveedores y a las autoridades correspondientes, los dispositivos móviles extraviados o hurtados.[52]

La Comisión Técnica Regional de Telecomunicaciones (COMTELCA) es una organización oficial centroamericana que coordina y armoniza el desarrollo regional de la industria de las telecomunicaciones. Sus estados miembros son Costa Rica, República Dominicana, El Salvador, Guatemala, Honduras, Nicaragua y Panamá. Todos los prestadores de servicios móviles de estos países han establecido acuerdos de cooperación con la GSMA para intercambiar la información de sus listas negativas, pero hasta la fecha algunas empresas operadoras aún no se han conectado con la base de datos de la GSMA.[53]

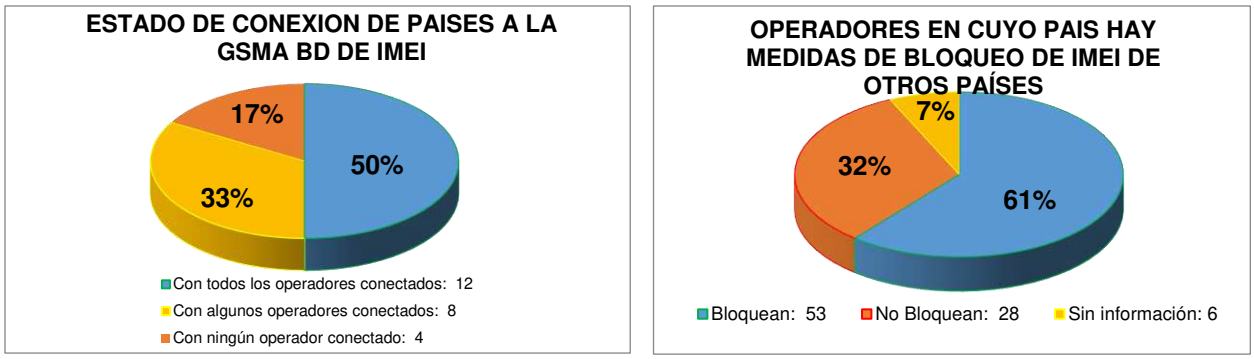
La coordinación regional ha sido un factor importante que ha facilitado la aprobación de las medidas que tratan el hurto entre múltiples países. Las medidas promovidas por los organismos regionales también ofrecen una hoja de ruta a los países que estén considerando adoptar nuevas medidas para combatir el hurto de dispositivos móviles. Sin embargo, es importante observar que en la realidad las políticas se han desarrollado a nivel nacional, produciendo como resultado una multitud de sistemas distintos en su forma y función en toda la región. La falta de consistencia reduce la eficacia general del sistema y aumenta los costos, especialmente cuando los dispositivos se trasladan entre países y deben cumplir con múltiples regímenes regulatorios distintos.

3.2 Políticas de listas negativas y listas positivas

La mayoría de los países latinoamericanos han adoptado algún tipo de medidas para combatir el hurto de dispositivos. Para marzo de 2017, 64 de 87 operadores móviles en las Américas estaban conectados con la base de datos de IMEI de la GSMA y tres operadores más se encontraban en fase de pruebas, con miras a lograr una conexión plena con esa base de datos.[54] Como se muestra en la Figura 3, la gran mayoría de los operadores de la región están suscritos a la lista negativa, pero, como se anotó anteriormente, no todos usan la base de datos de la misma manera.

[51] Gaceta Oficial No. 2186, "Decisión 786: Intercambio de información de equipos de terminales móviles extraviados, robados o hurtados y recuperados en la Comunidad Andina", 26 de abril de 2013, disponible aquí. Consultada en octubre de 2017.
[52] Id.
[53] Ver la presentación de COMTELCA "Joint Online ITU-CITEL Workshop on Global Strategies against Mobile Device Theft" ["Taller conjunto UIT-CITEL sobre estrategias globales contra el hurto de equipos móviles"], diapositiva 12, 16 de marzo de 2016, disponible aquí. Consultada en octubre de 2017. Además, para conocer el estado actual de las conexiones de operadoras a la base de datos de la GSMA, ver CITEL, PCC.I/Doc 4477/17 (XXXI-17) "Boletín Trimestral CITEL Intercambio y Bloqueo Equipos Hurtados 1Q2017" de julio de 2017.
[54] CITEL, PCC.I/Doc 4477/17 (XXXI-17) "Boletín Trimestral CITEL Intercambio y Bloqueo Equipos Hurtados 1Q2017" de julio de 2017.

Figura 3: Estado de la conexión de los operadores con la base de datos de la GSMA



Fuente: GSMA[55]

Aún con la suscripción generalizada a la base de datos de la GSMA, cada país mantiene sus propios procesos de bloqueo de dispositivos y sus propias reglas para el intercambio de información de listas negativas lo que limita el potencial de las políticas de armonización regional. Como los muestra laFigura 3 con respecto a los requisitos para bloquear los IMEI que aparecen en listas negativas de otros países, hay 28 operadores (el 32% de los encuestados) cuyos países en que operan no les piden bloquear los IMEI incluidos en las listas negativas de otros países, aunque en algunos casos, como el de República Dominicana, cada operador fija sus propias políticas sobre el uso de la lista negativa de la GSMA.[56] Esta falta de participación en la base de datos compartida constituye una debilidad del sistema de las listas negativas, al crear un pool de operadores que tienen mayor probabilidad de permitir la activación de dispositivos robados, porque los números IMEI no se verifican contra las listas negativas de otros países.

3.3 Soluciones tecnológicas

En contraste con los esfuerzos de las listas negativas y positivas, los gobiernos latinoamericanos han hecho poco énfasis en las soluciones tecnológicas en comparación con otras regiones. En una publicación del 2015 de la Comisión de Regulación de Comunicaciones de Colombia, se 20 países de las Américas fueron encuestados sobre sus esfuerzos ante fabricantes dirigidos a reducir el hurto de equipos móviles, incluyendo el uso de mecanismos de desactivación o "killswitches".[57] De los 12 países que respondieron, el 73% no había hecho nada y únicamente Estados Unidos mantenía activas iniciativas relativas a dichos mecanismos de desactivación o "killswitches".

Pese a la relativamente escasa promoción efectuada por diversos actores del sector (por ej., los gobiernos y las empresas operadoras), la tecnología de los mecanismos de desactivación o "killswitches" sí ha sido cubierta ocasionalmente por los principales medios masivos. Por ejemplo,

[55] CITEL, PCC.I/Doc 4477/17 (XXXI-17) "Boletín Trimestral CITEL Intercambio y Bloqueo Equipos Hurtados 1Q2017" de julio de 2017.
[56] CITEL, PCC.I Doc. 4226p2 (XXX-17) "Informe sobre la consulta de los procesos de intercambio y bloqueo entre países de los IMEI de dispositivos móviles con reporte de hurto o extravío", abril de 2017.
[57] CRC, "Fortalecimiento de las bases de datos dentro de la estrategia nacional contra el hurto de equipos terminales móviles. Documento soporte propuesta", pág. 31, agosto de 2015, disponible aquí. Consultado en octubre de 2017.

un popular periódico argentino reportó sobre la oferta de “killswitches” en equipos con sistemas operativos de Apple, Google, Microsoft y BlackBerry.[58]

3.4 Políticas actuales por países

Quizás el componente más importante para entender sobre los enfoques nacionales sobre el hurto de equipos en América Latina es que el enfoque de cada país es ligeramente distinto. Si bien ciertamente cada uno busca abordar lo que formuladores de políticas y entes reguladores consideran que son soluciones adaptadas a las necesidades de cada país, el resultado es una colcha de retazos de políticas y enfoques variados, que generan dificultades para la armonización y para el intercambio de datos.

Por ejemplo, Perú no sólo requiere registrar los equipos nuevos en la lista positiva nacional, sino además asociar a cada dispositivo el correspondiente registro del usuario en la Registraduría Nacional del Estado Civil.[59] Esto aumenta dramáticamente el nivel de precisión requerido para el correcto funcionamiento de la lista positiva y le impone cargas significativas al consumidor. Cualquier error en las bases de datos de la lista positiva o del registro civil puede fácilmente redundar en una situación en que los consumidores no puedan usar sus teléfonos. Además, cada ciudadano está sujeto a restricciones en cuanto al número de equipos que puede adquirir en el exterior por cada año calendario. Estos requerimientos estrictos y limitaciones en cuanto al número de equipos extranjeros pueden hacer más difícil cambiar de dispositivos.

Este enfoque no se limita al Perú. Aunque Argentina no ha aplicado la lista positiva, actualmente el Ente Nacional de Comunicaciones (ENACOM) requiere que cada equipo esté asociado al número de identidad nacional de su propietario.[60] Los usuarios con un número excesivo de IMEI registrados serán considerados candidatos para ser bloqueados de la red. Estas políticas dificultan el libre flujo de dispositivos y son inconvenientes para los consumidores que viajan a otros países con sus equipos y hacen más difícil intercambiar tarjetas SIM entre dispositivos.

La Tabla 22 presenta una visión general de las políticas y sus implicaciones asociadas para consumidores, operadoras y fabricantes en varios países de la región. Si bien no es exhaustiva, la información que presenta está diseñada para mostrar la diversidad de enfoques que caracteriza a la región, y algunas de las implicaciones de dichas políticas para los operadores, consumidores y gobiernos. Siempre que fue posible hacerlo, se mencionan las resoluciones correspondientes, aunque hay que decir que algunas regulaciones no están incluidas en la tabla y algunas medidas contra el robo de dispositivos han sido autorizadas mediante acuerdos celebrados con la GSMA o con operadores privados y no mediante regulaciones o leyes oficiales. La tabla que se presenta a continuación busca servir de guía al lector sobre el marco jurídico general que regula las políticas en cada uno de los países.

[58] La Nación, “Cómo proteger tus equipos electrónicos con un software de monitoreo”, 24 de febrero de 2015, disponible aquí. Consultado en octubre de 2017.
[59] Decreto Legislativo 1338/2017, disponible aquí. Consultado en octubre de 2017.
[60] Ver ENACOM, Resolución 2459, disponible aquí. Consultada en octubre de 2017.

Tabla 2: Estado general de las políticas por países

	Lista Negativa (o "Lista Negra")					Lista Positiva (o "Lista Blanca")			
País	**Lista Positiva Implementada**	**Obligaciones del Consumidor**	**Obligaciones de los operadoresllos operadores móviles**	**Obligaciones del Fabricante o de Importación y Exportación**	**Acceso por parte de los Organismos de Seguridad**	**Lista Positiva Implementada**	**Obligaciones del Consumidor**	**Obligaciones de los operadoreslos operadores móviles**	**Obligaciones del Fabricante o de Importación y Exportación**
Argentina	Sí, ver la Resolución 2459/2016.	Registrar los detalles personales con el operador, con un tope de 5 líneas por persona. Así mismo, reportar hurto o extravío de equipos.	Compartir datos con otros operadores y con la base de datos de la GSMA.	No se pueden activar en la red las tarjetas SIM que no han sido registradas con los detalles personales del usuario.	Las autoridades judiciales cuentan con acceso a la lista negativa.	Está siendo considerada.	No hay información	No hay información	No hay información
Brasil	Sí, ver la Ley General de Telecomuni-caciones y la Resolución 477/2007	Los usuarios deben reportar el hurto al operador o a la policía para iniciar el proceso de bloqueo del equipo.	Bloquear equipos en cuestión de 72 horas y sincronizar con la base de datos de la GSMA. Los operadores pagan por el mantenimiento de la lista negativa.	No	La policía puede iniciar un reporte para bloquear un equipo.	No	No hay información	No hay información	No hay información

	Lista Negativa (o "Lista Negra")					Lista Positiva (o "Lista Blanca")			
Chile	Sí, ver el Decreto 157/2011.	Los usuarios deben reportar el hurto para iniciar el proceso de bloqueo.	Bloquear los IMEI reportados, tener una línea 24/7 para reportar equipos hurtados, registrar datos personales, número telefónico, hora y fecha del robo, indicar si ha sido reportado a las autoridades, para todos los equipos reportados compartir la información reportada con el Organismo Administrador de Portabilidad Numérica (OAP).	No	La OAP mantiene detalles de cada dispositivo reportado como hurtado o extraviado. La policía puede acceder a esta lista.	Sí, para fines de homologación, especialmente para equipos importados. El ente regulador está contemplando internamente medidas adicionales tipo lista positiva, pero no ha divulgado al público su cronograma. Ver la Resolución 1463/2016.	Los usuarios que importan equipos para uso personal deben certificar que el dispositivo cumple.	Agregar los equipos actualmente en uso en el país a la lista positiva, permitir activación en la red únicamente de equipos homologados, mantener lista de equipos certificados.	Para su venta en el país, los equipos deben certificarse como debidamente homologados y rotulados de esta forma.

	Lista Negativa (o "Lista Negra")					Lista Positiva (o "Lista Blanca")			
Colombia	Sí, ver la Ley 1453/2011 y el Decreto 1630/2011[61]	Los usuarios deben reportar los equipos hurtados o extraviados para iniciar el proceso de bloqueo del equipo.	Bloquear los equipos con IMEI reportados e IMEI alterados o indebidos. Asumir los costos que implica mantener la base de datos. Mantener canales para que los usuarios puedan reportar dispositivos hurtados o extraviados. Compartir datos con operadores y con la GSMA.	Registrar los dispositivos importados en la lista positiva.	La policía y los fiscales pueden acceder a las dos listas, la positiva y la negativa.	Sí, ver la columna sobre lista negativa y también el Decreto 2025/2015.	Registrar los dispositivos actuales en la lista positiva o enfrentar la posible desconexión de la red.	Monitorear redes, bloquear equipos no autorizados. Permitir acceso a la red únicamente a los equipos homologados y registrados. Llevar listas con información personal de los usuarios asociada a cada equipo. Bloquear equipos con IMEI duplicado.	Registrar los equipos importados antes de su venta.
Costa Rica	Sí, ver la Regulación de Telecomuni-caciones de Protección al Usuario.	Los usuarios deben reportar el robo para iniciar el proceso de bloqueo del equipo.	Bloquear conexión a la red de los dispositivos con IMEI reportados, compartir la base de datos con otros operadores. Todos los operadores intercambian información con la lista negativa de la GSMA.	No	No	No	N//A	N/A	N/A

[61] Ver también CRC Resolución 3128/2011 (modificada por la Resolución 4868/2016 de la CRC) y la CRC Resolución 4813/2015.

	Lista Negativa (o "Lista Negra")					Lista Positiva (o "Lista Blanca")			
República Dominicana	Sí, ver la Resolución 137-09.	[Los usuarios están] obligados a reportar los equipos robados y extraviados.	Bloquear dispositivos reportados, reportar los IMEI a la lista negativa nacional. Los operadores también comparten información con la base de datos de la GSMA.	Se requiere ver///ificar los equipos contra la lista negativa nacional para poderse conectar a la red.	Recomiendan no bloquear los equipos para poder rastrear los dispositivos robados.	No	No hay información	No hay información	No hay información
Ecuador	Sí, ver la Resolución No. 191-07-CONATEL-2009 (y posteriores enmiendas en las Resoluciones TEL 214-05-CONATEL y TEL 535-18-CONATEL).	Los usuarios deben reportar el robo para iniciar el proceso de bloqueo.	Bloquear equipos con IMEI reportado, compartir información con otros operadores y con la lista negativa que opera el gobierno. Los operadores también intercambian información con la GSMA.	Los equipos en lista negativa o los que comparten IMEI con un equipo en lista negativa no se pueden conectar a la red.	Los reportes sobre negocios y mercados en donde se venden dispositivos robados se le informan a la Fiscalía General.	Sí, ver las resoluciones citadas para la lista negativa y la Resolución 111-2013.	Registrar los equipos actuales en la lista positiva.	Monitorear las redes y bloquear equipos no autorizados, incluyendo los que tienen IMEI duplicados.	Registrar los equipos importados en la lista positiva.

	Lista Negativa (o "Lista Negra")					Lista Positiva (o "Lista Blanca")			
Honduras	Sí, ver la Resolución NR009/14.	Los usuarios deben reportar los dispositivos hurtados a los operadores para iniciar el proceso de bloqueo. Para desbloquear un dispositivo recuperado, el usuario debe acudir personalmente ante la empresa operadora.	Los operadores deben pagar el mantenimiento de la lista negativa, intercambiar información diariamente con la GSMA, bloquear los teléfonos en lista negativa para impedir su conexión a la red. Los operadores también deben mantener información sobre el consumidor asociado a cada equipo para facilitar el proceso de bloqueo cuando se reporta un equipo robado. Los operadores deben tener un número telefónico disponible 24/7 con tiempo de respuesta de 20 segundos para aceptar reportes de teléfonos a ser bloqueados.	Los equipos importados del exterior no pueden conectarse a la red si el IMEI aparece en la lista negativa.	Todas las "autoridades judiciales o administrativas competentes" podrán acceder al registro nacional de equipos del país.	Approbada[62] en agosto de 2017, será implementada en el 2018.	El usuario debe registrar la tarjeta SIM y el número IMEI para que el dispositivo se pueda conectar a la red. Ello incluye a las personas que ingresen dispositivos del exterior.	Los operadores le harán monitoreo a las redes y no podrán conectar los dispositivos que figuren en la lista positiva. Deben mantener información personal de los usuarios de dispositivos.	Los equipos Importados deben registrarse en la lista positiva para poderse conectar a la red.
México	Sí, ver la Ley Federal de Telecomuni-caciones y Radiodifu-sión (2014) y la Disposición Técnica IFT-011-2017.	Para dar inicio al proceso de bloqueo, los usuarios deben reportar los dispositivos robados.	Bloquear de inmediato los IMEI reportados, permitir a los usuarios consultar el estado de los IMEI, impedir la conexión a la red de los IMEI duplicados o de los equipos reportados como hurtados o extraviados.	Los equipos cuyo IMEI figura en lista negativa no pueden recibir el certificado de homologación.	No	No	No hay información	No hay información	No hay información

[62] Para el momento de la presente publicación ya habían sido aprobadas las reformas al Decreto 19-2014, pero aún no habían sido publicadas.

	Lista Negativa (o "Lista Negra")					Lista Positiva (o "Lista Blanca")			
Paraguay	Sí, ver el Decreto 6728/17.	Los usuarios deben reportar los dispositivos hurtados y extraviados.	Bloquear los equipos reportados en cuestión de 30 minutos, llevar un registro de los últimos 3 IMEI asociados a cada línea telefónica. Compartir información con otras operadoras y con la GSMA.	No	La policía y la Fiscalía General disponen de acceso a la base de datos.	Está siendo considerada.	No hay información	No hay información	No hay información
Perú	Sí, ver la Resolución 138/2012 y el Decreto Legislativo 1338/2017.	Los usuarios deben reportar los dispositivos hurtados, extraviados o inoperantes.	Bloquear los dispositivos reportados para impedir su conexión a la red, compartir datos sobre equipos reportados con administradores de la base de datos del gobierno. Bloquear los dispositivos que el Gobierno les pida bloquear.	Ver las obligaciones de lista positiva para importadores y exportadores.	La policía puede solicitar acceso a la base de datos al hacer sus investigaciones.	Sí, ver las resoluciones citadas en la columna de lista negativa.	Registrar la información personal de los usuarios asociados a cada equipo no autorizado para impedir su conexión a la red, incluyendo los que tienen IMEI duplicado.	Bloquear todos los equipos que no estén en la lista positiva.	Los equipos importados se deben agregar a la lista positiva antes de su venta. Los exportados también deben reportarse para asegurar su retiro de la lista positiva.

Fuente: TMG

3.5 Efectividad del enfoque actual

El éxito de una lista negativa depende de que existan prácticas de reporte robustas y precisas, lo cual se dificulta en regiones en donde la mayoría de los crímenes con frecuencia no son denunciados. En Colombia, por ejemplo, tan sólo un 4% de los hurtos de teléfonos fueron reportados a la policía durante la primera mitad del año 2017.[63] En Brasil, una encuesta reciente encontró que tan sólo el 51% de las víctimas de hurtos de teléfonos celulares notificaron a la policía.[64]

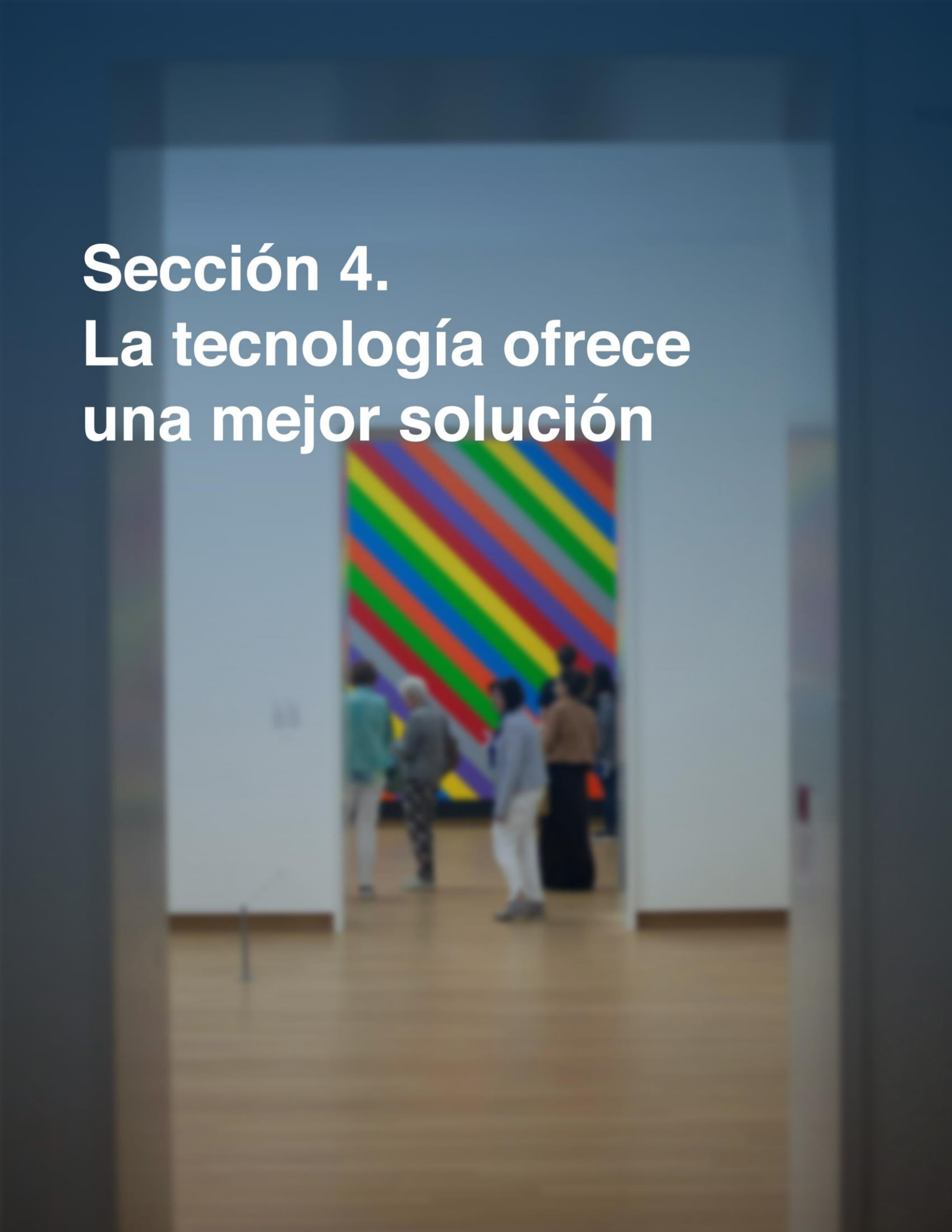
Los hurtos se han venido estabilizado a medida que los ladrones encuentran soluciones temporales alternas para superar las trabas que les ocasiona el sistema de listas negativas, especialmente al manipular los IMEI y/o vender los dispositivos robados en países vecinos. De hecho, en agosto del 2017 la Fiscalía General de Colombia le solicitó al Gobierno producir una nueva estrategia contra el hurto de teléfonos, aduciendo que la estrategia actual de bloquear los números IMEI había fracasado.[65] También, la asociación de operadores móviles en Colombia (Asomovil) ha manifestado que, a pesar de la inversión de los operadores (de aproximadamente USD 20 millones), no hay resultados significativos de la estrategia adoptada por el gobierno y la fuerza pública.[66] Un estudio sobre el hurto de equipos móviles en Colombia demostró que el número de hurtos en el año 2016 fue un 46.7% más grande que en el año 2010, aunque hubo una ligera reducción entre el año 2015 y el 2016.[67] La Fiscalía General de Colombia observó también que el hurto de teléfonos móviles es el delito de más rápido crecimiento en el país, registrando un aumento de un 79% entre los primeros seis meses del 2016 y la primera mitad del 2017. Este aumento se dio pese a la imposición de una regulación específica contra el robo (enfocada en el bloqueo de los números IMEI) en el 2011.

Mientras que en el 2000 Brasil creó una base de datos nacional de dispositivos robados que luego se conectó con la base de datos de la GSMA en 2014, los niveles de hurto no se han reducido significativamente. De hecho en Río de Janeiro, según datos del Instituto de Seguridad Pública de julio de 2017, hubo un aumento del 47.1% en el robo de equipos celulares en comparación con el mismo mes del año anterior.[68] Si bien no siempre hay información integral disponible sobre los niveles de hurto de los equipos móviles, reportes como éste indican que el hurto de dispositivos móviles sigue siendo un problema importante en América Latina y que las medidas que bloquean los números IMEI han resultado ineficaces para tratar el problema.

En Perú, a pesar de la implementación de las listas positivas y negativas, aproximadamente 6.000 teléfonos móviles son robados cada día (cerca de 250 móviles por hora). El ministerio del

[63] El Tiempo, “Colombia es el país de la región con mayor robo de celulares”, 8 de agosto de 2017, disponible aquí. Consultado en octubre de 2017.
[64] Panorama Mobile Time/Opinion Box, “Roubo de celulares no Brasil”, julio de 2017. Disponible para descargar aquí. Consultado en octubre de 2017.
[65] Fiscalía General, “Comunicado de prensa: El bloqueo de los Imei de los celulares no está funcionando”, 4 de agosto de 2017, disponible aquí. Consultado en octubre de 2017.
[66] Caracol Radio Colombia, “En Colombia cada hora se roban 153 celulares,” Enero, 2018, Disponible aquí. Recuperado en febrero de 2018
[67] Claudia Rodriguez, Juan Sebastian Moreno y Juan Felipe Godoy (Universidad de los Andes), “Informe seguridad 2016”, julio de 2017, p. 6, disponible aquí. Consultado en octubre de 2017.
[68] Instituto de Seguranca Publica, “Comparativo das Incidências Publicadas No Diário Oficial Do Estado Do Rio De Janeiro”, 24 de agosto de 2017, disponible aquí. Consultado en octubre de 2017.

Sección 4.
La tecnología ofrece una mejor solución



4 La tecnología ofrece una mejor solución

Está ampliamente aceptado, incluso por la misma GSMA, que el bloqueo de equipos por número IMEI tiene escasa probabilidad de ser eficaz como una solución en sí misma.[71] Como se anotó arriba, ni las listas negativas ni las positivas, incluso empleadas conjuntamente, resuelven el problema del hurto de equipos, y las dos soluciones implican costos que debe asumir alguna combinación de reguladores, operadoras y usuarios. Dadas estas limitaciones, le convendría mucho más a la América Latina adoptar un enfoque que incremente dramáticamente la visibilidad y el uso de las soluciones tecnológicas, con el apoyo de listas negativas así como de un sistema jurídico actualizado que penalice las actividades de recolección, modificación y distribución de equipos robados.

4.1 Beneficios para América Latina

Tal como se observó en las Secciones 2.2 y 2.3, las soluciones tecnológicas para el hurto de dispositivos producen beneficios significativos que no se pueden dar con el bloqueo de IMEI, especialmente comparados con las listas positivas.

- **Éxito.** Más importante aún, las soluciones basadas en mecanismos de desactivación o "killswitch" han demostrado ser capaces de reducir el hurto de teléfonos inteligentes, en contraste con las soluciones de listas negativas y positivas que prefieren muchos gobiernos latinoamericanos. Todas las partes interesadas deben promover una solución que permita éxitos medibles.
- **No implican costos para gobiernos, operadores ni consumidores.** Hasta la fecha, las soluciones tecnológicas son habilitadas por los fabricantes y los usuarios, y no requieren inversión de recursos ni tiempo para crear o mantener bases de datos, por ejemplo, ni para crear mecanismos de coordinación transfronteriza.
- **Permiten reubicar recursos de los organismos de seguridad.** Como se observó en la Sección 2.3, las soluciones tecnológicas permiten a los organismos de seguridad enfocarse más bien en los problemas subyacentes y las partes responsables, y reducir el tiempo requerido para registrar el hurto de equipos y rastrear equipos individuales.
- **Solución liderada por la industria y controlada por los usuarios.** Las soluciones tecnológicas se pueden implementar sin necesidad de nuevas regulaciones o leyes. Más bien los fabricantes desarrollan enfoques que pueden controlar los usuarios y la facilidad de uso o la nueva funcionalidad pueden incluso convertirse en punto de diferenciación y competencia entre fabricantes. Este enfoque deberá evitar agregarle complejidad al marco jurídico y regulatorio.
- **Está disponible hoy.** Los fabricantes y proveedores de sistemas operativos, incluyendo los ecosistemas Android e iOS, ya ofrecen soluciones tecnológicas que hacen menos rentable el hurto de equipos. No se trata de una tecnología del futuro, sino de una que se puede activar fácilmente hoy. Al crecer la adopción de teléfonos inteligentes, una mayor proporción de los equipos en circulación incluirá la tecnología del mecanismo de

[71] CITEL, PCC.I/Doc. 2311 (XVII-11) "GSMA Resources and Position to Support Regional Front to Combat the Theft of Mobile Terminal Equipment," septiembre de 2011 y CITEL, PCC.I Doc 4303p1 (XXX-17) "Avances del Sistema de Control de IMEI en Colombia", diapositiva 9, abril de 2017.

desactivación o "killswitch". Esto marca un contraste importante con los enfoques basados en listas, cuya completa implementación puede tomar años.[72]

- **La característica antirrobo puede usarse como argumento de ventas de teléfonos inteligentes.** La inclusión o la fácil disponibilidad de las soluciones antirrobo tecnológicas puede convertirse en característica atractiva de los teléfonos inteligentes y aumentar así la probabilidad de que los consumidores informados los adquieran y usen --y ese objetivo concuerda con las preferencias de los operadores y otras partes interesadas--.
- **Fácilmente reversible.** En el caso de que se recupere un dispositivo extraviado o hurtado, los usuarios pueden desbloquear el dispositivo con facilidad, sin tener que radicar un nuevo informe con la empresa operadora. Esto constituye un proceso mucho más simple, que libera los recursos de los operadores y del gobierno para enfocarse en otras prioridades y que puede ayudar a reducir los costos de mantenimiento de los enfoques basados en listas.

4.2 Mejores listas negativas como complemento a la tecnología

Si bien las soluciones tecnológicas se habrán de convertir en herramientas clave para reducir el hurto de equipos, las listas negativas también prometen, dándoles un mejor uso, como solución complementaria. Las listas negativas pueden ayudar a asegurar que los dispositivos robados no puedan conectarse a las redes, y pueden emplearse con todo tipo de equipos capaces de conectarse a una red móvil, incluyendo los teléfonos móviles convencionales.

Adicionalmente es posible revisar la implementación y empleo de las listas negativas para mejorar significativamente su efectividad:

- **Mayor armonización y adopción.** Una importante debilidad de las listas negativas es la falta de armonización y de una adopción uniforme. Estas listas serían más eficaces si todos los participantes, incluso los de países distintos, adoptaran un enfoque uniforme capaz de simplificar la información que se comparte y así reducir costos.
- **Alcance global.** Las listas negativas sólo son útiles en tanto su uso sea generalizado. Una mayor adopción global eliminaría los mercados en los que los equipos robados tienen mayor probabilidad de venta y reduciría así la demanda de estos equipos. Un enfoque regional no impide el movimiento de equipos robados hacia otras regiones en las que esos equipos no figuran en ninguna lista negativa.
- **Mayor precisión en los datos.** Las listas negativas sólo son eficaces según el grado de precisión de sus datos. Los operadores y los administradores de bases de datos deben redoblar esfuerzos para asegurar que se incluya información precisa de números IMEI y poder así enfocarse únicamente a los equipos que han robados legítimamente.

Sin embargo, es importante observar que las listas negativas mejoradas únicamente podrán ser eficaces si se emplean como uno de varios componentes en una solución integral que aprovecha el enfoque que construye sobre los éxitos alcanzados con las soluciones tecnológicas, incluyendo a los organismos de seguridad, mejores sistemas administrativos para aumentar la precisión de las bases de datos, y educación de los consumidores. Incluso con estas mejoras, las bases de datos de las listas negativas siguen siendo un punto de falla potencial del enfoque que adopte cualquier país para reducir el hurto de equipos, debido a que cualquier falla o

[72] La lista positiva colombiana se introdujo de manera escalonada durante cuatro años entre mayo de 2013 y julio de 2017. Ver CITEL, PCC.I Doc 4303p1 (XXX-17) "Avances del Sistema de Control de IMEI en Colombia", diapositiva 5, abril de 2017.

corrupción de los datos reduce su valor como herramienta en la lucha contra el hurto de dispositivos.

En últimas, sin embargo, los encargados de formular políticas deben evaluar la importancia que tiene invertir en listas negativas cuando el mercado se dirige más hacia los teléfonos inteligentes, que pueden emplear soluciones tecnológicas. Comprometer recursos para listas negativas constituye una inversión bajo un enfoque que será cada vez menos relevante, a medida que el mercado evoluciona en esa dirección. Los entes reguladores deben comenzar a considerar si los dineros que actualmente se están invirtiendo en los enfoques basados en listas podrían invertirse más bien y mejor en otras alternativas, como por ejemplo para promover y educar al público sobre las herramientas antirrobo que se basan en tecnología.

4.3 Educación del consumidor

La participación del consumidor es clave para el éxito de cualquier medida dirigida a combatir el hurto de equipos. Tanto las medidas que bloquean los IMEI como las listas negativas y las soluciones técnicas tales como el mecanismo de desactivación o "killswitch" requieren participación de los usuarios para poder ser eficaces. La tecnología antirrobo de los teléfonos inteligentes con a menudo se ofrece para selección expresa del usuario y ello implica que la educación del consumidor es crítica para poder aprovechar al máximo las tecnologías antirrobo. Si los usuarios desconocen una característica o no saben cómo emplearla, la eficacia de la misma será reducida. Además, las políticas que buscan hacer menos incómodo reportar los IMEI de equipos robados pueden ayudar a mejorar la efectividad de las medidas dirigidas a contrarrestar el hurto de dispositivos.

No son frecuentes en América Latina las iniciativas relacionadas con el hurto de dispositivos, especialmente a nivel regional. Sin embargo, la GSMA ha promovido activamente iniciativas para generar conciencia entre los consumidores, especialmente con la "Campaña Nos Importa" ["We Care Campaign"], una campaña conjunta de la GSMA y los proveedores móviles de la región.[73] Dicha campaña incluye medidas para facilitarle al consumidor verificar el estado de un IMEI en tiempo real. Este mecanismo, denominado IMEI Device Check o verificación del IMEI de equipos, permite a los usuarios comprobar la historia del IMEI de un dispositivo de su propiedad o que están considerando adquirir, contra la lista negativa de la GSMA.[74] Desde su introducción en el año 2014, la campaña ha producido tres lanzamientos en la región y 18 anuncios públicos sobre iniciativas lideradas por la industria.[75] Esta campaña le otorga poder a los usuarios para que puedan tomar decisiones informadas al comprar nuevos dispositivos y les permite un rol constructivo en la lucha contra el hurto de equipos.

Las iniciativas dirigidas a educar consumidores en América Latina, como la campaña de la GSMA, se han enfocado más en el registro y reporte de números IMEI y no tanto en cómo aprovechar los beneficios de la tecnología antirrobo. Esto no quiere decir que estas iniciativas no puedan jugar un papel constructivo. En el caso de las listas negativas y positivas, la base de datos es mucho más confiable cuando se reportan los números IMEI de los dispositivos robados, y cuando los usuarios tienen la posibilidad de verificar el estado de los equipos de su propiedad o que están pensando adquirir. En los dos casos la educación del consumidor es clave para que

[73] GSMA, sitio web oficial de "We Care Campaign" ["Campaña Nos Importa"], disponible aquí. Consultado en octubre de 2017.
[74] GSMA, sitio web oficial de "GSMA Device Check" ["Verificación de equipo"], disponible aquí. Consultado en octubre de 2017.
[75] GSMA, sitio web oficial de "We Care Campaign", disponible aquí. Consultado en octubre de 2017.

estas iniciativas puedan alcanzar su pleno potencial. Brasil creó un sitio web que permite a los consumidores verificar el estado de un IMEI específico antes de hacer una compra.[76] Los portales de internet operados por entes reguladores u operadores en que los usuarios pueden verificar el estado de su IMEI están generalizados en la región.[77] En los países en donde se programa la desconexión de los dispositivos que existen en el mercado a menos que los consumidores actúen al respecto para remediarlo, como por ejemplo registrando el dispositivo, se envían mensajes de texto directamente a los consumidores para informarles sobres sus obligaciones. Estos procedimientos envían información directamente a los afectados, en lugar proceder como las campañas que no tienen un público objetivo concreto, tales como las de la publicidad en medios impresos o en televisión.

Sin embargo, estas iniciativas latinoamericanas no tratan el papel que pueden tener las soluciones técnicas para prevenir el hurto de equipos, como se mencionó en la Sección 3.3. Las estrategias dirigidas a prevenir el hurto de dispositivos podrían mejorar mucho si se desarrolla amplia conciencia sobre las ventajas de seguridad de los teléfonos inteligentes. Si los usuarios se enteran que hay fácilmente disponibles equipos con tecnología antirrobo en su mercado, capaces de disuadir el hurto, habrá mayores incentivos para adquirir teléfonos inteligentes.

Se pueden mejorar mucho las medidas dirigidas a contrarrestar el hurto de equipos móviles en América Latina, y consisten en promover los beneficios de la tecnología antirrobo y educar a los consumidores sobre los beneficios de los teléfonos inteligentes que tienen habilitada esta tecnología. En Estados Unidos, los esfuerzos liderados por los fiscales generales en las ciudades de Nueva York y San Francisco, al igual que la legislación de los estados de Minnesota y California, promovieron un amplio cubrimiento en los medios sobre el tema del hurto de equipos y ayudaron a generar conciencia sobre los potenciales beneficios de las herramientas antirrobo de tipo tecnológico. A esto se sumó el compromiso público de los fabricantes miembros de la CTIA para abordar el tema, lo cual le sumó visibilidad al problema. Estos enfoques adoptados en nombre tanto del gobierno como de la industria pueden servir de modelo en América Latina para elevar el nivel de conciencia sobre las soluciones antirrobo de tipo tecnológico.

[76] Portal Brasil, “Anatel aprimora regras para coibir roubos e furtos de celulares”, 9 de marzo de 2016, disponible aquí.
[77] Ver por ejemplo: ENACOM, “Consulta de IMEI”, disponible aquí; Entel, “Quieres saber si tu equipo está bloqueado”, disponible aquí; CRC, “Cómo registrar tu celular”, disponible aquí. Consultados en octubre de 2017.

Sección 5. Conclusiones

5 Conclusiones

Se han adoptado políticas para enfrentar el hurto de dispositivos móviles en la América Latina. Las listas negativas de dispositivos hurtados fueron adoptadas ampliamente en la región como parte del enfoque inicial adoptado para enfrentar el hurto. Sin embargo, la efectividad de las mismas se ha visto menoscabada por las debilidades implícitas del enfoque de listas negativas, así como por la falta de uniformidad y armonización, al igual que por el éxito de los delincuentes al explotar las debilidades y desarrollar contramedidas.

Las listas negativas han sido complementadas por otros enfoques basados en el número IMEI para ser más eficaces contra el robo de dispositivos. Las listas positivas refuerzan políticas que tratan de combatir el hurto de dispositivos como uno de varios problemas, incluyendo el de los equipos falsos y fraudulentos. Sin embargo, las listas positivas tienen también varias desventajas que han impactado en sus beneficios particularmente porque aún carecen de armonización regional y crean tanto incomodidad a los consumidores como cargas a la industria. La implementación de las dos listas, negativas y positivas es costosa y requiere tiempo y sus beneficios no han sido enteramente demostrados.

A pesar de la implementación de tanto las listas negras como las listas blancas, el robo de terminales sigue siendo un problema muy serio en América Latina.

Aunque los gobiernos latinoamericanos han apoyado firmemente las listas negativas y otras herramientas basadas en bloquear los IMEI, ha habido poca discusión pública sobre las soluciones antirrobo de índole tecnológica que puede probar ser más efectivas, menos costosas y requieren menos participación del gobierno. Son promisorios los enfoques tales como los mecanismos de desactivación o “killswitch” que han implementado los principales fabricantes, pueden hacen menos rentable el hurto de equipos y no requieren más fondos públicos ni otros recursos, o la necesidad de imponer cargas costosas a los consumidores y empresas. Con el apoyo de listas negativas mejoradas e iniciativas que educan al consumidor sobre el uso de las medidas antirrobo disponibles, las soluciones tecnológicas ofrecen mucho potencial para reducir el hurto de dispositivos móviles en América Latina.

Además, implementar una solución tecnológica tiene los beneficios adicionales de permitirle a los organismos de seguridad dedicar sus esfuerzos a los elementos y comportamientos que habilitan el hurto de equipos, e incluso de estimular una mayor adopción de los teléfonos inteligentes.