Proyecto de Ley N° 4247/2022-CR

CONGRESO de la REPÚBLICA

COMISIÓN ESPECIAL DE SEGUIMIENTO PARLAMENTARIO AL ACUERDO DE LA ALIANZA DEL PACÍFICO

CONGRESO DE LA REPUBLICA
AREA DE TRAMITE Y DIGITALIZACIÓN DE DOCUMENTOS
14 FEB. 2023
RECIBIDO
Firma: Hora: 14:50 h.

PROYECTO DE LEY QUE ESTABLECE MEDIDAS PARA PROTEGER A LA CIUDADANÍA DE LOS RIESGOS DE SEGURIDAD DIGITAL QUE ORIGINAN LA SUSTRACCIÓN DE EQUIPOS MOVILES

El señor Congresista de la República, **ALFREDO PARIONA SINCHE, Presidente de la Comisión Especial de Seguimiento Parlamentario a la Alianza del Pacífico y sus miembros**, en ejercicio del Derecho de iniciativa legislativa que les confiere el artículo 107° de la Constitución Política del Perú y los artículos 22° literal c) y 75° del Reglamento del Congreso de la República; presentan a consideración del Congreso de la República el siguiente proyecto de Ley:

FORMULA LEGAL

Artículo 1. Objeto de la Ley

La presente Ley tiene como objeto establecer medidas que garanticen la protección de la ciudadanía de los riesgos de seguridad digital que originan la sustracción de equipos móviles, y que promuevan la confianza digital en el país.

Artículo 2. Finalidad de la Ley

La finalidad de la Ley es disponer medidas sobre el uso de servicios, plataformas, tecnologías digitales y emergentes para la mitigación de los riesgos en y a través del entorno digital originados por la sustracción de equipos móviles, así como la prevención del uso de las tecnologías de la información y comunicaciones con fines delictivos o que atenten contra la intimidad y seguridad de las personas.

Artículo 3. Intercambio de información entre entidades públicas y privadas

3.1 El Ministerio Público, el Poder Judicial y la Policía Nacional del Perú, en el ejercicio de sus funciones de investigación y represión del delito, acceden a través de mecanismos de interoperabilidad a datos de identificación personal contenidos en bases de datos de entidades públicas y privadas, para permitir una respuesta oportuna contra los delitos que atenten contra la seguridad digital y la intimidad de las personas ante situaciones de sustracción de equipos móviles o similares.

3.2 Las entidades públicas titulares de bancos de datos personales y responsables de su tratamiento establecen medidas técnicas y organizativas para que dicho acceso se realice respetando la normativa que regula las respectivas materias y aplicando el principio de razonabilidad. Así mismo, se establecen mecanismos que permitan la trazabilidad en el proceso de acceso e intercambio de dicha información.

3.3 Las organizaciones del sector privado realizan intercambios seguros de información cuando sea necesario para garantizar la lucha contra la ciberdelincuencia.

3.4 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital en coordinación con las entidades correspondientes dicta las normas reglamentarias que establezcan los supuestos y criterios para la aplicación del presente artículo. Asimismo, implementa y gestiona la Plataforma Nacional de Gobierno Digital a fin de facilitar los mecanismos de interoperabilidad necesarios.

Artículo 4. Medidas técnicas de seguridad digital en dispositivos móviles
4.1 Las entidades públicas y las organizaciones del sector privado promueven la utilización de tecnologías, software y mecanismos de seguridad digital que permitan el bloqueo de dispositivos móviles de forma remota para combatir la sustracción de equipos terminales móviles, así como su posterior comercialización.

4.2 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital, aprueba las normas reglamentarias que establezcan las acciones y medidas para implementar esta disposición en el marco de lo dispuesto en el Decreto de Urgencia N° 007-2020.

Artículo 5. Financiamiento
La implementación de la presente Ley se financia con cargo al presupuesto institucional de las entidades públicas involucradas, sin demandar recursos adicionales al Tesoro Público.

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA. Norma reglamentaria
La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital en coordinación con las entidades competentes aprueba el reglamento de la presente Ley y las disposiciones complementarias necesarias para su aplicación, en el plazo de noventa (90) días hábiles.

DISPOSICIONES COMPLEMENTARIAS MODIFICATORIAS

PRIMERA. Modificación de los artículos 6 y 8 del Decreto Legislativo N° 1338
Modificase los artículos 6 y 8 del Decreto Legislativo N° 1338, Decreto Legislativo que crea el Registro Nacional de Equipos Terminales Móviles para la Seguridad, orientado a la prevención y combate del comercio ilegal de equipos terminales móviles y al fortalecimiento de la seguridad ciudadana, en los siguientes términos:

> Artículo 6.- Autoridades competentes
> (...)
> **6.3 *El Ministerio Público, la Policía Nacional del Perú y el Poder Judicial en el marco de la investigación de un delito, y actuando en el ámbito de sus competencias, acceden a la información contenida en el Registro Nacional de Equipos Terminales Móviles para la Seguridad* - RENTESEG mediante mecanismos de interoperabilidad conforme a la regulación vigente en materia de gobierno digital.**
>
> Artículo 8.- Empresas operadoras de servicios públicos móviles de telecomunicaciones
> 8.1 Las empresas operadoras de servicios públicos móviles de telecomunicaciones tienen las siguientes obligaciones:
> (...)

a) Verificar plenamente la identidad de quien contrata el servicio de servicios públicos móviles de telecomunicaciones mediante el sistema de verificación biométrica de huella dactilar ***u otras tecnologías que permitan niveles similares de seguridad. Las excepciones a dicha verificación son establecidas en el reglamento de la presente Ley.***

DISPOSICIONES COMPLEMNETARIAS DEROGATORIAS

ÚNICA. - Derogación del artículo 5 del Decreto Legislativo Nº 1338

Deróguese el artículo 5 del Decreto Legislativo N° 1338, Decreto Legislativo que crea el Registro Nacional de Equipos Terminales Móviles para la Seguridad, orientado a la prevención y combate del comercio ilegal de equipos terminales móviles y al fortalecimiento de la seguridad ciudadana.

FIRMA DIGITAL
Firmado digitalmente por: CRUZ MAMANI Flavio FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 14/02/2023 12:42:18-0500

FIRMA DIGITAL
Firmado digitalmente por: PARIONA SINCHE Alfredo FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 09/02/2023 12:52:09-0500

FIRMA DIGITAL
Firmado digitalmente por: SAAVEDRA CASTERNOQUE Hitler FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 10/02/2023 14:16:52-0500

FIRMA DIGITAL
Firmado digitalmente por: ZEBALLOS APONTE Jorge Arturo FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 10/02/2023 15:29:44-0500

FIRMA DIGITAL
Firmado digitalmente por: VERGARA MENDOZA Elvis Heman FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 13/02/2023 10:13:30-0500

FIRMA DIGITAL
Firmado digitalmente por: WONG PUJADA Enrique FIR 10621936 hard
Motivo: Soy el autor del documento
Fecha: 13/02/2023 12:33:37-0500

FIRMA DIGITAL
Firmado digitalmente por: CORDERO JON TAY Maria Del Pilar FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 14/02/2023 09:07:58-0500

FIRMA DIGITAL
Firmado digitalmente por: REYMUNDO MERCADO Edgard Cornelio FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 13/02/2023 15:31:24-0500

CONGRESO DE LA REPÚBLICA

Lima, **17** de **febrero** de **2023**

Según la consulta realizada, de conformidad con el Artículo 77° del Reglamento del Congreso de la República: pase la Proposición N° **4247/2022-CR** para su estudio y dictamen, a la (s) Comisión (es) de:

1. **DEFENSA NACIONAL, ORDEN INTERNO, DESARROLLO ALTERNATIVO Y LUCHA CONTRA LAS DROGAS.**

JOSÉ F. CEVASCO PIEDRA
Oficial Mayor
CONGRESO DE LA REPÚBLICA

EXPOSICIÓN DE MOTIVOS

CONTEXTO Y PROBLEMÁTICA

ROBO DE CELULARES

El problema del robo de celulares, en el Perú y el mundo, tiene una serie de causas de diversa índole, entre ellas, la existencia de mercados informales en los que se comercializan los equipos robados, lo que implica la existencia de una oferta que responde a una demanda cada vez más creciente, no solo de equipos, sino también de partes o piezas de dichos equipos.

Asimismo, también contribuyen al problema el desconocimiento, desinformación y/o falta de diligencia de la ciudadanía para protegerse, hacer valer sus derechos y/o denunciar cuando son víctimas de este delito. Esto se debe a que los mecanismos que se ponen a disposición de la ciudadanía son engorrosos, de difícil acceso y poco efectivos.

De acuerdo con lo informado por el Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL), en el año 2021, se contabilizaron 1 350 257 equipos celulares robados en el país, cifra que supera en un 26% lo contabilizado en el año 2020[1];

Según el Instituto Nacional de Estadística e Informática (INEI)[2] durante los años 2013, 2014, 2015, 2016, 2017, 2018 y 2019, la tasa de robo de dinero, cartera, celular a nivel nacional fue de 17.1%, 16.4% 15.9%, 14.2%, 13.4%, 12.6% y 14.3%, respectivamente. Asimismo, durante los mismos años, la tasa de intento de robo de dinero, cartera celular fue de 7.3%, 3.6%, 5.3%, 5.2%, 5.2%, 5.4% y 5.3%, respectivamente.

Por otro lado, durante el semestre septiembre 2020 – febrero 2021, el 10.5% de la población de 15 y más años de edad del área urbana a nivel nacional fue víctima de robo de dinero, cartera, celular. Asimismo, en el semestre septiembre 2021 – febrero 2022, la tasa fue de 8.6%, la cual se mantuvo durante los semestres agosto 2021 – enero 2022 y septiembre 2021 – febrero 2022[3].

Según el OSIPTEL, en el primer trimestre del año 2022, se reportaron 390,416 celulares robados a nivel nacional[4]. Esta cifra se construye con la información que proporcionan a las empresas operadoras las personas que solicitan el bloqueo del equipo móvil y la suspensión de la línea cuando han sido víctimas de robo. Refleja que cada día se produjeron 4433 reportes de robo a nivel nacional, que es equivalente a una solicitud de bloqueo cada veinte segundos[5].

En el IV Foro Internacional de Seguridad Ciudadana y Empresarial, de la Cámara de Comercio de Lima (CCL), llevado a cabo el 26 de abril de 2022, el subjefe del Instituto

---

1 https://www.osiptel.gob.pe/portal-del-usuario/noticias/mas-de-823-000-equipos-moviles-con-imei-invalido-fueron-bloqueados-por-las-empresas-operadoras-el-2021/

2 Instituto Nacional de Estadística e Informática, "Principales indicadores de seguridad ciudadana a nivel regional. Semestre móvil noviembre 2019 - abril 2020". Boletín Estadístico N° 03 - Junio 2020, p.2.

3 Instituto Nacional de Estadística e Informática, "Estadísticas de Seguridad Ciudadana. Septiembre 2021 – febrero 2022. Informe Técnico N° 02 - Abril 2022.

4 Esto significa un incremento de 30% en comparación con el mismo periodo del 2021, en el que las empresas operadoras registraron 274,396 equipos sustraídos.

5 https://ojo.pe/actualidad/roban-mas-de-4-mil-celulares-al-dia-en-el-pais-web-ojo-print-noticia/

Nacional de Estadística e Informática (INEI), señaló que "el hecho más dramático es que de ese universo de delitos patrimoniales (aquellos que más se cometen en el Perú), el 82% son robos de celular. Por cada 10 personas afectadas por robos, a 8 se les ha arrebatado su celular y en algunos casos de forma muy violenta"[6].

Además, durante el semestre septiembre 2020 – febrero 2021, a nivel nacional urbano, en las ciudades de 20 mil a más habitantes, y en los centros poblados urbanos entre 2 mil y menos de 20 mil habitantes, el porcentaje de la población víctima de algún hecho delictivo que presentó denuncia fue de 16.5%, 16.6% y 15.8%, respectivamente; a diferencia del semestre septiembre 2021 – febrero 2022 en el que las tasas fueron de 13.1%, 13.2% y 12.5%, respectivamente[7].

Finalmente, durante el semestre septiembre 2021 – febrero 2022, a nivel nacional urbano, la población de 15 y más años de edad que fue víctima de algún hecho delictivo, no denunció el hecho debido a las siguientes razones: a) es una pérdida de tiempo (35,9%); b) desconoce al delincuente (23,7%); c) porque es un delito de poca importancia (14,4%)[8].

En el contexto descrito, debemos tener en cuenta que el robo o pérdida del celular implica no solo perder el dispositivo sino, sobre todo, perder información valiosa: fotos, cuentas financieras, registros de salud, documentos personales, documentos de trabajo, contactos, entre otros. Asimismo, con dicha información, se pueden cometer una serie de delitos y fraudes en perjuicio del titular y de terceros[9], tales como la suplantación de identidad para adquirir obligaciones, efectuar compras, entre otros. En tal sentido, las medidas a adoptarse deben abarcar el problema de manera integral y desde el punto de vista de las diversas aristas que lo componen.
Por otro lado, mediante Resolución Ministerial N° 125-2022-PCM, de fecha 20 de abril de 2022, se creó el Grupo de Trabajo Multisectorial de naturaleza temporal denominado "Mesa Técnica para proponer acciones y medidas para fortalecer la Confianza Digital en el país".
Dicho Grupo de Trabajo tuvo como objetivo: *"analizar, evaluar y proponer acciones y medidas para prevenir y reducir los ciberataques,* ***el robo de teléfonos móviles****, el uso indebido de medios digitales, el contacto no consentido mediante llamadas, mensajes u otros medios para fines fraudulentos u otras modalidades de riesgos en el entorno digital, a fin de fortalecer la confianza digital en el país".*

En su Informe Final, el Grupo de Trabajo presenta un análisis de la situación actual y propone una lista de acciones y propuesta de políticas que no solo están alineadas con el objetivo de fortalecer la confianza digital, tal como está definida en el Decreto de Urgencia N° 007-2020, sino también con los esfuerzos encaminados a implementar el Convenio de Budapest en el país.

---

6 https://www.youtube.com/watch?v=xQyTSV_8Kgl

7 Instituto Nacional de Estadística e Informática, "Estadísticas de Seguridad Ciudadana. Septiembre 2021 – febrero 2022. Informe Técnico N° 02 - Abril 2022.

8 Instituto Nacional de Estadística e Informática, "Estadísticas de Seguridad Ciudadana. Septiembre 2021 – febrero 2022. Informe Técnico N° 02 - Abril 2022.

9 https://elcomercio.pe/lima/policiales/los-olivos-odontologa-sufre-el-robo-de-su-celular-y-ladrones-logran-estafar-con-mas-de-s2-mil-a-sus-clientes-video-rmmn-noticia/

Intercambio de información entre entidades públicas y privadas.

De conformidad con el Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, la Gobernanza Digital es el conjunto de procesos, estructuras, herramientas y normas que nos permiten dirigir, evaluar y supervisar el uso y adopción de las tecnologías digitales en la organización. Además, el Marco de Gobernanza y Gestión de Datos del Estado Peruano está constituido por instrumentos técnicos y normativos que establecen los requisitos mínimos que las entidades de la Administración Pública deben implementar conforme a su contexto legal, tecnológico y estratégico para asegurar un nivel básico y aceptable para la recopilación, procesamiento, publicación, almacenamiento y apertura de los datos que administre.

En ese escenario, la interoperabilidad es la capacidad de interactuar que tienen las organizaciones diversas y dispares para alcanzar objetivos que hayan acordado conjuntamente, recurriendo a la puesta en común de información y conocimientos, a través de los procesos y el intercambio de datos entre sus respectivos sistemas de información. El Marco de Interoperabilidad del Estado Peruano está constituido por políticas, lineamientos, especificaciones, estándares e infraestructura de tecnologías digitales, que permiten de manera efectiva la colaboración entre entidades de la Administración Pública para el intercambio de información y conocimiento, para el ejercicio de sus funciones en el ámbito de sus competencias, en la prestación de servicios digitales inter-administrativos de valor para el ciudadano provisto a través de canales digitales.

Por otro lado, según el Decreto Supremo N° 029-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto Legislativo Nº 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo, la gobernanza digital es el conjunto de roles, estructuras, procesos, herramientas y normas para articular, dirigir, evaluar y supervisar el uso y adopción de las tecnologías digitales y datos en el Estado Peruano y el proceso de transformación digital en el país. La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital, es la entidad responsable de ejercer la gobernanza digital del uso transversal y adopción estratégica de las tecnologías digitales y datos en el Estado Peruano.

Adicionalmente, mediante Decreto Legislativo N° 1246, Decreto Legislativo que aprueba diversas medidas de simplificación administrativa, se dispuso que las entidades de la Administración Pública, de manera gratuita, a través de la interoperabilidad, interconecten, pongan a disposición, permitan el acceso o suministren la información o bases de datos actualizadas que administren, recaben, sistematicen, creen o posean respecto de los usuarios o administrados, que las demás entidades requieran necesariamente y de acuerdo a ley, para la tramitación de sus procedimientos administrativos y para sus actos de administración interna. En los casos en los que la información o datos se encuentren protegidos bajo la Ley N° 29733, Ley de Protección de Datos Personales, las entidades de la Administración Pública deben obtener la autorización expresa e indubitable del usuario o administrado para acceder a dicha información o datos.

Siendo así, la posibilidad de compartir información también puede habilitarse para incluir a las entidades privadas, en lo que corresponda y sea razonable, para fines de apoyo a las acciones de lucha contra el delito y cautelando los derechos de los ciudadanos, en especial, el correcto tratamiento de los datos personales.

ACTUAL	PROPUESTA
(Sin regulación previa)	**Artículo 3. Intercambio de información entre entidades públicas y privadas** 3.1 El Ministerio Público, el Poder Judicial y la Policía Nacional del Perú, en el ejercicio de sus funciones de investigación y represión del delito, acceden a través de mecanismos de interoperabilidad a datos de identificación personal contenidos en bases de datos de entidades públicas y privadas, para permitir una respuesta oportuna contra los delitos que atenten contra la seguridad digital y la intimidad de las personas. 3.2 Las entidades públicas titulares de bancos de datos personales y responsables de su tratamiento establecen medidas técnicas y organizativas para que dicho acceso se realice respetando la normativa que regula las respectivas materias y aplicando el principio de razonabilidad. Así mismo, se establecen mecanismos que permitan la trazabilidad en el proceso de acceso e intercambio de dicha información. 3.3 Las organizaciones del sector privado realizan intercambios seguros de información cuando sea necesario para garantizar la lucha contra la ciberdelincuencia. 3.4 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital en coordinación con las entidades correspondientes dicta las normas reglamentarias que establezcan los supuestos y criterios para la aplicación del presente artículo. Asimismo, implementa y gestiona la Plataforma Nacional de Gobierno Digital a fin de facilitar los mecanismos de interoperabilidad necesarios.

IMPLEMENTACIÓN DE MEDIDAS TÉCNICAS DE SEGURIDAD DIGITAL PARA DISPOSITIVOS MÓVILES

Habiendo identificado como un problema grave el incremento del robo de dispositivos móviles, los cuales posteriormente son utilizados para cometer diferentes delitos, algunos de ellos delitos informáticos, se propone promover la adopción de mecanismos de prevención por parte de los ciudadanos y otros actores del sector privado. Con el fin de que estas medidas puedan ser efectivas y respondan al estado actual de la tecnología, se señala que la implementación estará a cargo del Poder Ejecutivo a través de la expedición de procedimientos reglamentarios.

ACTUAL	PROPUESTA
(Sin regulación previa)	**Artículo 4. Medidas técnicas de seguridad digital en dispositivos móviles** 4.1 Las entidades públicas y las organizaciones del sector privado promueven la utilización de tecnologías, software y mecanismos de seguridad digital que permitan el bloqueo de dispositivos móviles de forma remota para combatir la sustracción y robo de equipos terminales móviles, así como su posterior comercialización. 4.2 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital, aprueba las normas reglamentarias que establezcan las acciones y medidas para implementar esta disposición en el marco de lo dispuesto en el Decreto de Urgencia N° 007-2020.

DECRETO LEGISLATIVO Nº 1338, DECRETO LEGISLATIVO QUE CREA EL REGISTRO NACIONAL DE EQUIPOS TERMINALES MÓVILES PARA LA SEGURIDAD (RENTESEG)

Mediante el Decreto Legislativo Nº 1338, se creó el Registro Nacional de Equipos Terminales Móviles para la Seguridad (RENTESEG), el cual está a cargo del Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL).

Según el artículo 1 del Decreto Legislativo N° 1338, el RENTESEG tiene por finalidad prevenir y combatir el hurto, robo y comercio ilegal de equipos terminales móviles, dentro del marco del fortalecimiento de la seguridad ciudadana; garantizando la contratación de los servicios públicos móviles de telecomunicaciones.

El artículo 4 del Decreto Legislativo Nº 1338 establece el contenido del RENTESEG en los siguientes términos:

> ***"Artículo 4. Contenido del RENTESEG***
> *4.1 El contenido del RENTESEG* ***tiene carácter permanente y se constituye por la información de la Lista Blanca y la Lista Negra, y otra información pertinente a sus fines*** *establecida en el reglamento del presente decreto legislativo.*

El artículo 3 del Reglamento del Decreto Legislativo N° 1338 define la lista blanca y la lista negra en los siguientes términos:

> ***"Artículo 3.- Definiciones***
> *Para los efectos de aplicación de la Ley y el presente Reglamento, se establecen las siguientes definiciones*
> *(...)*
> ***q) Lista Blanca:*** *Base de datos dinámica y actualizada* ***que contiene información del registro de abonados del servicio público móvil, incluyendo el registro de los equipos terminales móviles utilizados en la prestación de dicho servicio y los equipos terminales móviles importados legalmente****, así como aquellos que de acuerdo con el presente Reglamento deban ser incluidos.*
> *(...)*
> ***r) Lista Negra:*** *Base de datos dinámica y actualizada que* ***contiene información de los equipos terminales móviles que son reportados como perdidos, sustraídos de Perú y que, por lo tanto, deban ser incluidos.***
> *(...)."* (resaltado agregado)

Como puede apreciarse, el RENTESEG contiene información útil y necesaria para combatir la delincuencia; en tal sentido, en la línea de la propuesta anterior, a fin de que, junto con la Policía Nacional del Perú, el Ministerio Público también tenga acceso al RENTESG, toda vez que, según la Constitución Política del Perú es quien ejerce la acción penal. Al igual que en el caso anterior, la finalidad es facilitar el acceso a información relevante y pertinente para fines de investigación de los delitos.

Por otro lado, diferentes medidas de seguridad asociadas al robo de celulares y el fraude digital dependen de contar con un sistema de validación de identidad digital robusto, pero que no impida o dificulte demasiado la interacción entre los actores del mercado. A propósito de ello, el Informe del Grupo de Trabajo propone cambios a los sistemas de verificación de identidad como el uso de la validación biométrica a través de la huella digital y la apertura a un ecosistema mayor y más seguro de aplicaciones de identidad digital que sean más eficaces para cumplir con sus objetivos.

ACTUAL	PROPUESTA
Artículo 6. Autoridades competentes (...) 6.3 La Policía Nacional del Perú, en el marco de la investigación de un delito, puede solicitar al OSIPTEL la información contenida en el RENTESEG.	CUARTA. - Modificación del artículo 6 del Decreto Legislativo N° 1338 Modificase el artículo 6 del Decreto Legislativo N° 1338, Decreto Legislativo que crea el Registro Nacional de Equipos Terminales Móviles para la Seguridad,

	orientado a la prevención y combate del comercio ilegal de equipos terminales móviles y al fortalecimiento de la seguridad ciudadana, en los siguientes términos: Artículo 6.- Autoridades competentes (...) ***6.3 El Ministerio Público, la Policía Nacional del Perú y el Poder Judicial en el marco de la investigación de un delito, y actuando en el ámbito de sus competencias, acceden a la información contenida en el RENTESEG mediante mecanismos de interoperabilidad conforme a la regulación vigente en materia de gobierno digital.***
Artículo 8. Empresas operadoras de servicios públicos móviles de telecomunicaciones 8.1 Las empresas operadoras de servicios públicos móviles de telecomunicaciones tienen las siguientes obligaciones: (...) a) Verificar plenamente la identidad de quien contrata el servicio de servicios públicos móviles de telecomunicaciones mediante el sistema de verificación biométrica de huella dactilar. Las excepciones a dicha verificación son establecidas en el reglamento del presente decreto legislativo.	Modificación del artículo 8 del Decreto Legislativo N° 1338 Modificase el artículo 8 del Decreto Legislativo N° 1338, Decreto Legislativo que crea el Registro Nacional de Equipos Terminales Móviles para la Seguridad, orientado a la prevención y combate del comercio ilegal de equipos terminales móviles y al fortalecimiento de la seguridad ciudadana, en los siguientes términos: Artículo 8.- Empresas operadoras de servicios públicos móviles de telecomunicaciones 8.1 Las empresas operadoras de servicios públicos móviles de telecomunicaciones tienen las siguientes obligaciones: (...) a) Verificar plenamente la identidad de quien contrata el servicio de servicios públicos móviles de telecomunicaciones mediante el sistema de verificación biométrica de huella dactilar ***u otra tecnología que permita un nivel similar de seguridad. Las excepciones a dicha verificación son establecidas en el reglamento del presente decreto legislativo.***

DEROGACIÓN DEL ARTÍCULO 5 DEL DECRETO LEGISLATIVO Nº 1338

El artículo 5 del Decreto Legislativo N° 1338 regula el intercambio seguro en los siguientes términos:

> *"Artículo 5. Intercambio seguro*
> ***5.1 Sólo se pueden activar en un equipo terminal móvil los IMSI -código de identidad internacional del abonado a un móvil- cuya identidad del abonado coincida con la identidad del usuario que tenga registrado dicho equipo terminal móvil.*** *Para efectos del RENTESEG, se considera usuario registrado de un equipo terminal móvil al titular de la IMSI que active por primera vez dicho equipo terminal móvil.*
>
> ***5.2 Para activar el IMSI en un equipo terminal móvil que ha sido objeto de transferencia, el usuario registrado se desvincula previamente de la titularidad del IMEI - código de identidad internacional del equipo terminal móvil-,*** *de acuerdo con el procedimiento establecido en el reglamento del presente decreto legislativo.*
>
> ***5.3 No se puede brindar servicio público móvil de telecomunicaciones en dos o más equipos terminales móviles que tengan el mismo IMEI.*** *El procedimiento para la suspensión temporal del servicio público móvil de telecomunicaciones en casos de dos o más equipos terminales móviles que tengan el mismo IMEI es establecido en el reglamento del presente decreto legislativo.*
>
> *5.4 Las disposiciones especiales y excepciones al intercambio seguro son establecidas en el reglamento del presente decreto legislativo."* (resaltado agregado)

Sobre el proceso de desvinculación, el artículo 25 del Reglamento del Decreto Legislativo N° 1338 señala:

> ***"Artículo 25.- Desvinculación del equipo terminal móvil***
> ***25.1. El abonado se desvincula de un equipo terminal móvil del cual es usuario registrado ante la empresa operadora que le presta el servicio público móvil, vía telefónica o de manera presencial, para lo cual proporciona la siguiente información:***
> ***a) Identificación completa del usuario registrado del equipo terminal móvil, ya sea persona natural o jurídica.***
> ***b) Tipo y número del documento legal de identidad del usuario registrado del equipo terminal móvil.***
> ***c) Información que valide los datos del usuario registrado del equipo terminal móvil que la empresa operadora considere necesaria, previa conformidad emitida por el OSIPTEL. La validación de datos puede realizarse a través de la contraseña a la que hace referencia el numeral 37.3 del artículo 37 del presente Reglamento.***
>
> *25.2. Una vez desvinculado el equipo terminal móvil, dicho equipo puede ser utilizado en otro servicio público móvil vinculándose automáticamente a su abonado, a través de un IMSI o MSISDN registrado a su nombre.*

25.3. La persona jurídica puede desvincular el equipo terminal móvil acreditando su condición de representante de acuerdo a lo establecido en las Condiciones de Uso.

25.4. La empresa operadora puede implementar otros mecanismos no presenciales para facilitar el proceso de desvinculación del equipo terminal móvil ***siempre que se cumpla con la entrega de la información a que hace referencia el numeral 25.1 del presente artículo*** *y previa aprobación del OSIPTEL."* (resaltado agregado)

El SIM card, que es un chip que contiene el número de teléfono y las claves de servicio del suscriptor usadas para identificarse ante la red, es diferente e independiente al equipo terminal móvil, el cual es identificado por el código IMEI. Por tal razón, técnicamente es posible extraer el SIM card del equipo terminal móvil y colocarlo en otro diferente, de manera permanente o temporal.

No obstante, la normativa vigente establece que el titular del equipo terminal móvil debe registrarlo ante la empresa operadora y, para poder venderlo, prestarlo o alquilarlo; es decir, para que pueda ser utilizado en otro servicio público móvil, debe desvincularse del mismo a través de un protocolo formal, lo que incluye identificarse ante la empresa operadora y registrar una serie de datos personales.

Al respecto, el intercambio seguro se aplicará cuando entre en vigencia la tercera fase del RENTESEG (abril de 2023); implica la obligación del titular del equipo de realizar un trámite previo para desvincularse de su equipo terminal, lo cual restringe el ejercicio del derecho de propiedad (uso y disfrute). Además, desconoce la naturaleza de la tecnología GSM que está actualmente en uso, en virtud de la cual, el número telefónico (contenido en un SIM card) y el equipo celular (identificado por el código IMEI) son dos conceptos totalmente independientes entre sí, de modo tal que, es técnicamente posible que una persona pueda contratar un servicio con un equipo terminal determinado y cambiar dicho terminal por otro diferente, sea de manera permanente (adquisición de un nuevo terminal) o temporal (cuando se termina la batería del celular y se saca el SIM card temporalmente para ingresarlo en otro terminal para hacer una llamada telefónica puntual). En tal sentido, resulta pertinente eliminar el intercambio seguro.

ACTUAL	PROPUESTA
(Sin regulación previa)	**DISPOSICIONES COMPLEMENTARIAS DEROGATORIAS** **ÚNICA. - Derogación del artículo 5 del Decreto Legislativo N° 1338** Deróguese el artículo 5 del Decreto Legislativo N° 1338, Decreto Legislativo que crea el Registro Nacional de Equipos Terminales Móviles para la Seguridad, orientado a la prevención y combate del comercio ilegal de equipos terminales móviles y al fortalecimiento de la seguridad ciudadana.

ALIANZA DEL PACIFICIO

El 11 de diciembre de 2020, con motivo de la XV Cumbre Presidencial de la Alianza del Pacifico, se suscribió una **Declaración Presidencial sobre el desarrollo del Mercado Digital Regional** y el impulso hacia la transformación digital de la región, que tiene como segundo pilar: crear un entorno habilitador para promover el intercambio de bienes y servicios digitales.

El objetivo de este pilar es crear un entorno propicio para promover el intercambio de bienes, productos y servicios por medios digitales en la Alianza del Pacifico, que tenga por objeto: reducir las barreras al comercio electrónico, mejorar la interoperabilidad técnica y legal, promover la confianza en línea, la privacidad, la protección de datos y la ciberseguridad, así como analizar la importancia de la propiedad intelectual y la facilitación del comercio en el entorno digital.

EFECTOS DE LA VIGENCIA DE LA NORMA SOBRE LA LEGISLACIÓN NACIONAL

De acuerdo con lo señalado en el artículo 79° de la Constitución Política del Perú, en concordancia con lo establecido en el artículo 76° del Reglamento del Congreso de la República, la iniciativa legislativa no puede contener propuesta de creación ni aumento de gasto público, por lo que la iniciativa materia de estudio cumple con lo señalado en las normas legales antes citadas y no contraviene la Constitución Política del Perú, ni ninguna norma legal.

ANÁLISIS COSTO- BENEFICIO

La aplicación de la presente norma en las instituciones del sector público se financia con cargo a su presupuesto institucional aprobado y sin demandar recursos adicionales al tesoro público.

VINCULACIÓN CON EL ACUERDO NACIONAL Y LAS POLÍTICAS NACIONALES

La propuesta legislativa tiene vinculación directa con las siguientes Políticas de Estado del Acuerdo Nacional:

Política 7 del Acuerdo Nacional: Erradicación de la violencia y fortalecimiento del civismo y *de la seguridad ciudadana*, con este objetivo el Estado consolidará políticas orientadas a prevenir, disuadir, sancionar y eliminar aquellas conductas y prácticas sociales que pongan en peligro la tranquilidad, integridad o libertad de las personas.

Política 35 del Acuerdo Nacional: Sociedad de la información y sociedad del conocimiento, con este objetivo nos comprometemos a impulsar una sociedad de la información hacia una sociedad del conocimiento orientada al desarrollo humano integral y sostenible, en base al ejercicio pleno de las libertades y derechos de las personas, y capaz de identificar, producir, transformar, utilizar y difundir información en todas las dimensiones humanas incluyendo la dimensión ambiental.

Promoveremos el acceso universal al conocimiento a través de las Tecnologías de la Información y Comunicación (TIC), acompañado de la generación de contenidos, servicios y

bienes digitales; así como del desarrollo de capacidades para que todos los peruanos puedan desempeñarse plenamente y de manera segura en el entorno digital, y de igual manera promoveremos mecanismos que fortalezcan el acceso, conectividad y su uso en las regiones del país.

Promoveremos las TIC como medios para fortalecer la gobernabilidad democrática y el desarrollo sostenible, a través de un servicio moderno, transparente, eficiente, eficaz, efectivo y descentralizado al ciudadano.

Con este objetivo el Estado: (a) generará una institucionalidad multiestamentaria, con participación del gobierno, sociedad civil, academia y sector privado, con la finalidad de garantizar principios como los de la Cumbre Mundial de la Sociedad de la Información: acceso universal a la información, libertad de expresión, diversidad cultural y lingüística, y educación para todos; (b) fomentará el pleno ejercicio y respeto de los Derechos Humanos en todo entorno digital; (c) promoverá, a través de la educación, la inclusión y alfabetización digital para reducir las brechas existentes y generar igualdad de oportunidades, de modo tal que ninguna persona en el Perú quede fuera de la sociedad de la información y del conocimiento; (d) fomentará la ampliación y modernización de la infraestructura como soporte de la reducción de los aspectos digitales de la brecha social, e impulsará las ciudades inteligentes; (e) fomentará la modernización del Estado, mediante el uso de las TIC, con un enfoque descentraliza, planificador e integral; (f) promoverá las TIC como factor de generación de empleo digno y no de exclusión, y establecerá lineamientos para la reconversión laboral en casos que las TIC generen pérdidas de empleo; (g) promoverá la productividad y competitividad del país mediante el uso de las TIC en los sectores productivos, e impulsará una industria de las TIC; (h) fomentará el uso transversal de las TIC en ámbitos tales como educación, salud, conservación del ambiente, seguridad ciudadana, prevención de riesgo de desastres, gobierno abierto, defensa nacional, innovación, investigación, transferencia de conocimiento y sectores productivos y sociales; (i) diseñará las políticas y la regulación en materia de sociedad de la información y del conocimiento teniendo como base los principios de internet libre, abierto, neutro y para todos, así como el adecuado resguardo de la seguridad de la información; (j) establecerá un observatorio permanente y prospecto en materia de la sociedad de la información y del conocimiento.

PLAN ESTRATÉGICO DE DESARROLLO NACIONAL

Eje 2 Oportunidades y Acceso a los servicios: Seguridad Ciudadana

Objetivo Nacional 3: Elevar los niveles de competitividad y productividad con empleo decente y en base al aprovechamiento sostenible de los recursos, el capital humano, el uso intensivo de la ciencia y tecnología, y la transformación digital del país.

POLÍTICA GENERAL DEL GOBIERNO 2021-2026

Decreto Supremo N°164-2021-PCM publicado el 16 de octubre de 2021.

Eje 6: Fortalecimiento del Sistema Democrático, *Seguridad Ciudadana* y Lucha contra la corrupción, narcotráfico y terrorismo.

Lineamiento 6.2.- Fortalecer la articulación e interoperabilidad para el combate del crimen organizado.

Eje 8: Gobierno y transformación digital con equidad.

8.1 Garantizar el acceso inclusivo, seguro y de calidad al entorno digital y el aprovechamiento de las tecnologías digitales en todas las regiones del país para consolidar la ciudadanía digital considerando sus condiciones de vulnerabilidad y diversidad cultural.

Líneas de intervención

8.1.1 Consolidar el ejercicio de la ciudadanía digital para todas las personas a través de su identidad digital incluyendo lenguas originarias a nivel nacional.

8.1.2 Impulsar la economía digital, el comercio electrónico, el emprendimiento digital, la innovación, los datos abiertos, la digitalización y resiliencia de las pymes y los procesos productivos del país.

8.1.3 Acelerar el gobierno y transformación digital del sector público impulsando el ecosistema de tecnología y fortaleciendo la gobernanza digital en el país.

8.1.4 Fortalecer la educación, el acceso al entorno digital, la inclusión y el talento digital en todas las personas promoviendo alianzas con el sector privado.

8.1.5 Consolidar las acciones de seguridad y confianza digital para la protección de la ciudadanía frente a los riesgos y amenazas en el entorno digital.

8.1.6 Impulsar el uso ético y el aprovechamiento de las tecnologías exponenciales y los datos en favor de la ciudadanía.