A	**:**	SERGIO ENRIQUE CIFUENTES CASTAÑEDA **GERENTE GENERAL**
CC	**:**	CARMEN DEL ROSARIO CARDENAS DIAZ **DIRECTORA DE LA OFICINA DE COMUNICACIONES Y RELACIONES INSTITUCIONALES** RAFAEL EDUARDO MUENTE SCHWARZ **PRESIDENTE EJECUTIVO**
ASUNTO	**:**	COMENTARIOS AL PROYECTO DE LEY 4247-2022-CR ¿ LEY QUE ESTABLECE MEDIDAS PARA PROTEGER A LA CIUDADANIA DE LOS RIESGOS DE SEGURIDAD DIGITAL QUE ORIGINAN LA SUSTRACCION DE EQUIPOS MOVILES
FECHA	**:**	**10 de marzo de 2023**

	CARGO	**NOMBRE**
ELABORADO POR	COORDINADOR DE COSTOS E INTERCONEXIÓN (E)	RAUL ESPINOZA CHAVEZ
REVISADO POR	SUB DIRECTOR DE ANÁLISIS REGULATORIO (E)	DANIEL ARGANDOÑA MARTINEZ
	DIRECTOR DE LA OFICINA DE ASESORIA JURÍDICA	ALBERTO AREQUIPEÑO TAMARA
APROBADO POR	DIRECTOR DE POLITICAS REGULATORIAS Y COMPETENCIA (E)	MARCO VILCHEZ ROMAN

I. OBJETO

El presente informe tiene por objeto analizar las disposiciones propuestas en el Proyecto de Ley Nº 4247/2022-CR, Ley que establece medidas para proteger a la ciudadanía de los riesgos de seguridad digital que originan la sustracción de equipos móviles, presentado por la Comisión Especial de Seguimiento Parlamentario a la Alianza del Pacífico y sus miembros.

II. ANTECEDENTES

Mediante el Oficio N° D001322-2023-PCM-SC, del 27 de febrero de 2023, la Presidencia de la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha contra las Drogas del Congreso de la República, solicita opinión sobre el Proyecto de Ley Nro. 4247/2022-CR, Ley que establece medidas para proteger a la ciudadanía de los riesgos de seguridad digital que originan la sustracción de equipos móviles.

III. ANÁLISIS

3.1. Sobre el Artículo 1 y Artículo 2, Objeto de la Ley y la Finalidad de la Ley

De la revisión del objeto y la finalidad de la ley, se advierte que en ambos casos se informa sobre la materia legislable o la materia que se regula (objeto) y se señala un propósito que se busca lograr (finalidad).

En efecto, en el artículo 1 se puede observar lo siguiente:

> *Objeto: Establecer medidas que garanticen la protección de la ciudadanía de los riesgos de seguridad digital que originan la sustracción de equipos móviles.*
>
> *Finalidad: Promover la confianza digital en el país.*

Asimismo, en el artículo 2 se identifica:

> *Objeto: Disponer medidas sobre el uso de servicios, plataformas, tecnologías digitales y emergentes.*
>
> *Finalidad: 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.*

Cabe indicar que, si bien el artículo segundo cuenta con mayor detalle, sugerimos acotar adecuadamente ambos artículos, respecto al objeto y la finalidad de la Ley, conforme a lo dispuesto en el Manual de Técnica Legislativa del Congreso de la República.

3.2. Sobre el Articulo 3 - Intercambio de información entre entidades públicas y privadas

En principio, con relación al alcance de la propuesta normativa se advierte que, sería muy amplia considerando que, de manera general, se hace mención a "entidades privadas" o "sector privado", conforme se aprecia en los numerales 3.1, 3.3 del artículo 3 y numeral 4.1 del artículo 4. Lo señalado resulta relevante toda vez que, la obligación a cargo de dichos sujetos podría ser considerada muy onerosa y compleja, en la medida que deberán contar con mecanismos de interoperabilidad.

En tal sentido, y en línea con los fines de la propuesta normativa, recomendamos se delimite su alcance, y se determine qué tipos de entidades del sector privado estarían dentro de su alcance; y, por tanto, les resultará exigible el cumplimiento de las diversas obligaciones que contempla.

En relación al numeral 3.1., en la propuesta normativa se refiere "*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*". Al respecto, es importante clarificar a lo que se entiende por "similares", ¿serían considerados las tabletas, laptop, PCs, etc.?

En relación al numeral 3.3, es importante que, respecto a los intercambios de información que se soliciten a las entidades privadas, se precise que los mismos deben efectuarse en el momento y tiempos requeridos, para poder cumplir con el objetivo de lucha contra la delincuencia. Adicionalmente, del texto del proyecto, tampoco queda claro en qué consistiría el intercambio de información a que este hace referencia.

Al respecto, es preciso citar la Exposición de Motivos, la cual señala:

> *"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."*

Del texto antes citado, parecería que se busca que las entidades privadas puedan acceder a información de las entidades públicas a través de la interoperabilidad. Sin embargo, consideramos necesario que, en caso esa sea la finalidad de la disposición bajo comentario, además de lo señalado previamente, se precise expresamente que sería únicamente para el ejercicio de funciones administrativas que estén previstas en normas con rango de ley[1], especialmente, en el caso que se trate de información de datos personales. En su defecto, también podría listarse expresamente el tipo de entidad privada que tendrá dicho acceso.

Sin perjuicio de ello, en caso la finalidad de la propuesta sea solo que las entidades públicas tengan acceso a información de las entidades privadas por interoperabilidad, consideramos preciso especificar expresamente ello, con la finalidad de garantizar su exigencia a dichas entidades, toda vez que de dejar dichas precisiones a una norma de inferior jerarquía podría ser cuestionado por dichas entidades, por ejemplo, a través de un procedimiento de barreras burocráticas ante el INDECOPI.

En relación al numeral 3.4, se debe tomar en cuenta que mediante Decreto Supremo Nº 083-2011-PCM, el Poder Ejecutivo creó la Plataforma de Interoperabilidad del Estado (PIDE), que permite la implementación de servicios públicos por medios electrónicos y el intercambio electrónico de datos entre entidades del Estado a través de Internet, telefonía móvil y otros medios tecnológicos disponibles.

Asimismo, mediante Decreto Supremo Nº 016-2020-PCM, se ampliaron los servicios de información para la implementación progresiva de la interoperabilidad y digitalización de servicios en beneficio del ciudadano, siendo que, en el caso del Osiptel, se estableció que la información del RENTESEG será proporcionada de manera gratuita y permanente a las entidades de la Administración Pública.

En función de lo antes indicado, considerando que la información de la plataforma PIDE ya puede ser consultada por cualquier entidad de la administración pública, no resulta necesario establecer una disposición normativa adicional que facilite mecanismos de interoperabilidad que ya existen, incluyendo el acceso a información del RENTESEG.

Para ello, la entidad solicitante podrá efectuar el consumo de los servicios que se proporcionan a través de la mencionada plataforma siempre que cumpla con lo establecido en el referido artículo 3 del Decreto Supremo N° 016-2020-PCM, esto es, deberá encontrarse sustentado en el cumplimiento de su misión, desarrollo de sus actividades y mejora en la prestación de sus servicios públicos, en estricto cumplimiento de sus funciones, competencias o atribuciones asignadas por norma expresa o Ley, en línea con lo previsto en la Ley N° 29733, Ley de Protección de Datos Personales.

[1] **Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 004-2019-JUS**
*"**Artículo I. Ámbito de aplicación de la ley***
La presente Ley será de aplicación para todas las entidades de la Administración Pública.
Para los fines de la presente Ley, se entenderá por "entidad" o "entidades" de la Administración Pública:
(…)
8. Las personas jurídicas bajo el régimen privado que prestan servicios públicos o ejercen función administrativa, en virtud de concesión, delegación o autorización del Estado, conforme a la normativa de la materia.
Los procedimientos que tramitan las personas jurídicas mencionadas en el párrafo anterior se rigen por lo dispuesto en la presente Ley, en lo que fuera aplicable de acuerdo a su naturaleza privada".

3.3. Sobre el Artículo 4 - Medidas técnicas de seguridad digital en dispositivos móviles

Actualmente, la normativa nacional vigente, en específico, el Decreto Supremo Nº 007-2019-IN – Reglamento del Decreto Legislativo 1338, permite que las empresas operadoras suspendan servicios de telefonía móvil y bloqueen equipos terminales reportados como sustraídos o perdidos por parte del abonado, su representante o usuario, de manera inmediata, previa consulta en línea, a través del sistema automático implementado por las empresas operadoras y el OSIPTEL.

En ese sentido, a la fecha, constituye una obligación normativa para las empresas operadoras del sector de telecomunicaciones, que, frente a un reporte por parte del usuario, aquella proceda con el bloqueo correspondiente.

Siendo así, el incorporar el numeral 4.1 y del articulo 4 no resultaría necesario, considerando la conducta que despliegan los administrados en cumplimiento de las disposiciones vigentes.

Con relación a ello, cabe agregar además que la utilización de dichas tecnologías, estarían a cargo, principalmente, de los fabricantes de equipos terminales, los cuales, se encuentran fuera del ámbito de competencia del Osiptel, por lo que debería quedar claro, a qué entidades públicas se estaría refiriendo el texto propuesto.

Asimismo, de mantener la propuesta, se podría especificar que el bloqueo del dispositivo móvil puede ser de forma temporal o definitivo, incorporando opciones tecnológicas que permitan la inutilización del equipo terminal, y de esta forma no sea posible vulnerar de alguna forma la información que posee, y de esta forma cumpla con el objetivo de lucha contra la delincuencia.

3.4. Modificación del artículo 5 del Decreto Legislativo N° 1338

Con relación a la propuesta derogatoria de la institución jurídica del intercambio seguro, regulado actualmente en el artículo 5° del Reglamento del Decreto Legislativo N° 1338, debemos señalar que no tenemos observación alguna, ya que se trata de una propuesta derogatoria que recoge nuestra postura; en ese sentido, no tenemos acotación que hacer al respecto.

3.5. Modificación del artículo 6 del Decreto Legislativo N° 1338

Respecto de la modificación del artículo 6 del Decreto Legislativo N°1338, es de tenerse en cuenta que en la Tercera Fase del RENTESEG, y en cumplimiento de lo establecido en el artículo 18° del Reglamento del Decreto Legislativo N° 1338, el RENTESEG ya contará con un Módulo de Consulta Especializado para atender las solicitudes de información del Ministerio del Interior, Ministerio Público, Poder Judicial y de otras entidades del Estado, conforme al procedimiento establecido por el OSIPTEL; por lo que la modificatoria en el artículo 6.3 no tendría un impacto. Incluso, además de dicho módulo, cualquier entidad puede solicitar el acceso a información del RENTESEG a través de la plataforma PIDE.

3.6. Modificación del artículo 8 del Decreto Legislativo N° 1338

Se advierte que la propuesta normativa propone modificar el referido artículo, que –originalmente- estableció la obligatoriedad, para las empresas operadoras, de identificar al solicitante del servicio público mediante el sistema de verificación biométrica de huella dactilar.

Dicha obligación se estableció en atención a la relevancia de que se identifique correctamente a la persona contratante del servicio público toda vez que la falta de identificación del abonado o titular del servicio móvil genera problemas que inciden en la seguridad ciudadana, por cuanto facilita las usurpaciones de identidad, imposibilita la identificación del autor o partícipe de delitos cometidos con el empleo de dispositivos móviles, entorpece las acciones destinadas a combatir el comercio ilegal de terminales robados o hurtados, y facilita los fraudes financieros por banca móvil.

En tal contexto, el OSIPTEL ha venido desplegando diferentes esfuerzos a fin resguardar que las contrataciones de los abonados se enmarquen en un ámbito de seguridad. Negar dicho aspecto, implicaría serias repercusiones en la esfera de los referidos usuarios, pues considerando que el TUO del Reglamento de la Ley de Telecomunicaciones establece que el titular del servicio es responsable por el uso que se haga del mismo[2], cualquier tipo de responsabilidad que se desprenda de un uso ilícito del mismo le podría ser atribuido.

Tanto es así que, la persona cuya identidad haya sido usurpada y registra líneas móviles sin consentimiento, se vea afectada por cuanto la empresa operadora posteriormente le exige el pago por los consumos realizados desde dichas líneas, así como por el costo del equipo adquirido bajo financiamiento. Del mismo modo, en caso se hayan cometido hechos ilícitos empleando dicha línea y/o equipo, la persona que figura como titular del servicio se verá vinculada a tales ilícitos ante las autoridades respectivas (Policía Nacional del Perú, Ministerio Público y/o Poder Judicial), con el consecuente perjuicio que ello implica.

A modo de ejemplo, cabe mencionar los casos de las señoras Guicela Taboada Campos y Eliana Ramos quienes fueron vinculadas con procesos judiciales, dado que desde algunas de las líneas que se registraron bajo su titularidad, sin su consentimiento, se cometieron determinados delitos. En el caso de la Sra. Taboada Campos, se registraron indebidamente más de 21 mil líneas móviles bajo su titularidad. Tales hechos fueron de conocimiento de toda la ciudadanía conforme se observa de las siguientes noticias publicadas en internet.

[2] ***"Artículo 15.- Responsabilidad del abonado***
El abonado titular de un servicio público de telecomunicaciones, es responsable del uso que se haga del mismo."

Fuente: https://panamericana.pe/24horas/locales/207855-delincuentes-sacan-21-000-lineas-nombre-mujer-policia

Fuente: https://larepublica.pe/sociedad/947539-mafia-la-suplanta-para-obtener-chips-y-ahora-ella-puede-ir-a-prision

Cabe indicar que, los casos antes descritos no fueron los únicos casos públicos de suplantación de identidad en la contratación de servicios móviles, sino que se trata de una problemática que ha sido advertida, en diversas ocasiones, por los medios de comunicaciones y con mayor auge en el periodo en el cual no se empleaba el sistema de verificación biométrica de huella dactilar (años 2015-2018).

En virtud de lo anterior, genera mucha preocupación la propuesta de modificación del artículo en cuestión, toda vez que, de manera muy amplia, contempla permitir que la identificación del solicitante del servicio se realice mediante tecnologías de “similar seguridad”, tal como se advierte:

> *"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". El resaltado y subrayado es nuestro.*

En tal sentido, consideramos que, en virtud de la generalidad del referido texto, las empresas operadoras podrían tener mayor libertad y discreción para emplear cualquier otro tipo de tecnología argumentando que tiene un nivel de seguridad similar a la biometría de huella dactilar, tendiendo a elegir aquella que le genere los menores costos. Con ello, consideramos que se desvirtuaría el objetivo que busca la norma, esto es, identificar plenamente al contratante del servicio a efectos de evitar que se produzcan casos de suplantación de identidad que -como se ha mencionado anteriormente- generan graves afectaciones a los ciudadanos y diversas consecuencias negativas para los abonados afectados.

Asimismo, se ha de tener en cuenta que antes de introducir otros métodos de verificación de la identidad del abonado y/o usuario – distintos al sistema de verificación biométrica – es necesario, conocer los alcances de lo manipulable que puede ser la tecnología. Del mismo modo, que, a la fecha, no se tiene conocimiento de la existencia de un mecanismo igual de idóneo que el de verificación biométrica y, que otorgue el mismo nivel de precisión que este.

Sin perjuicio de lo señalado, de presentarse un mecanismo adicional, consideramos que este no debería ser utilizado en defecto del sistema de verificación biométrica, sino solo cuando se presenten escenarios excepcionales, no debiendo establecerse de manera normativa como de uso alternativo a discrecionalidad de la empresa operadora. Asimismo, siempre que estos mecanismos a implementarse hayan sido aprobados previamente por la autoridad administrativa competente la cual debe indicar mediante una norma o disposición complementaria la aprobación y los lineamientos de un nuevo sistema de identificación de abonados para los servicios públicos de telecomunicaciones.

De otro lado, de no realizarse una adecuada identificación de los contratantes de las líneas móviles no sería posible contar con un registro de abonados con información cierta y confiable sobre la identidad de los titulares de los servicios. Con ello, las acciones adoptadas por el Estado dirigidas a combatir el comercio ilegal de equipos terminales hurtados o robados, resultarían ineficaces.

Si bien es cierto, con el desarrollo de nuevas tecnologías podría garantizarse el cumplimiento del objetivo planteado, consideramos que ello debería encontrarse respaldado y/o garantizado y no dejarse a discreción de las empresas operadoras; por lo que sugerimos un ajuste en la redacción del artículo a fin de que las tecnologías alternativas que puedan ser empleadas sean validadas por una entidad técnica especializada; y contar con aprobación del Osiptel.

En ese sentido, la propuesta modificatoria sería la siguiente:

> ***"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 público móvil mediante el sistema de verificación biométrica de huella dactilar. De manera excepcional y cuando no sea posible identificar la identidad de quien contrata el servicio a través del sistema de verificación biométrica, se podrá utilizar los mecanismos tecnológicos alternativos que hayan sido implementados para tales efectos. Las excepciones a dicha verificación son establecidas en el reglamento del presente decreto legislativo".*
>
> *Los mecanismos tecnológicos alternativos al sistema de verificación biométrica, deberán ser aprobados previamente antes de su utilización por el OSIPTEL, debiendo la empresa operadora resguardar la información que sustente haber estado inmerso en las excepciones establecidas en la utilización de dicho mecanismo."*

3.7. Referente a la exposición de motivos

Con relación al análisis costo–beneficio de la propuesta.

Un aspecto de suma relevancia es el análisis costo-beneficio que sustenta la medida, en la exposición de motivos, de manera bastante sucinta, enunciativa y general se indica que el financiamiento se realizaría con el presupuesto institucional aprobado de las instituciones públicas, no demandando recursos adicionales del tesoro público; sin embargo, considerando que, la propuesta normativa contempla, entre otros, el empleo de mecanismos de interoperabilidad para el intercambio de información entre instituciones públicas y privadas, cuya implementación puede ser muy compleja y costosa, es importante se cuente con un análisis costo beneficio que incorpore y detalle los costos regulatorios que representa y si estos resultan menores al beneficio social que podría obtenerse.

IV. CONCLUSIONES

4.1 Este organismo emite **opinión favorable con observaciones** respecto al Proyecto de Ley Nº 4247/2022-CR; en específico nos encontramos conforme con la eliminación del intercambio seguro, y respecto a las otras disposiciones se sugiere tener en consideración las observaciones planteadas.

.

4.2 El resumen de los principales comentarios se citan a continuación:

Referente al alcance:

- Se sugiere acotar adecuadamente los artículos 1 y 2, respecto al objeto y la finalidad de la Ley, conforme a lo dispuesto en el Manual de Técnica Legislativa del Congreso de la República.

- Se recomienda delimitar el alcance, y se determine qué tipos de entidades del sector privado estarían dentro de su alcance; y, por tanto, les resultará exigible el cumplimiento de las diversas obligaciones que contempla.

Referente al intercambio de información:

- Se debe precisar expresamente que sería únicamente para el ejercicio de funciones administrativas que estén previstas en normas con rango de Ley, especialmente, en el caso que se trate de información de datos personales.

- En caso la finalidad de la propuesta sea que las entidades públicas tengan acceso a información de las entidades privadas por interoperabilidad, consideramos preciso especificar expresamente ello, con la finalidad de garantizar su exigencia a dichas entidades.

Referente a las medidas técnicas de seguridad digital en dispositivos móviles:

- La incorporación del numeral 4.1 y del articulo 4 no resultaría necesario, considerando la conducta que despliegan los administrados en cumplimiento de las disposiciones vigentes.

Referente a la modificación del artículo 5 del Decreto Legislativo N° 1338

- Con relación a la propuesta derogatoria de la institución jurídica del intercambio seguro, regulado actualmente en el artículo 5° del Reglamento del Decreto Legislativo N° 1338, debemos señalar que no tenemos observación alguna, ya que se trata de una propuesta derogatoria que recoge nuestra postura; en ese sentido, no tenemos acotación que hacer al respecto.

Referente a la modificación del artículo 6 el Decreto Legislativo N° 1338

- Respecto de la modificación del artículo 6 del Decreto Legislativo 1338, es preciso reiterar lo señalado para el articulo 3 del Proyecto Normativo propuesto. En ese sentido, considerando que, a la fecha, tanto el Ministerio Público como el Poder Judicial pueden acceder a la información del RENTESEG a través de la plataforma PIDE, resulta innecesario impulsar su acceso a la misma información a través de otro canal digital.

Referente a la modificación del artículo 8 del Decreto Legislativo N° 1338

- Genera mucha preocupación la propuesta de modificación del artículo en cuestión, toda vez que, de manera muy amplia, contempla permitir que la identificación del solicitante del servicio se realice mediante tecnologías de “similar seguridad”.

- Si bien es cierto, con el desarrollo de nuevas tecnologías podría garantizarse el cumplimiento del objetivo planteado, consideramos que ello debería encontrarse respaldado y/o garantizado y no dejarse a discreción de las empresas operadoras; por lo que sugerimos un ajuste en la redacción del artículo a fin de que las tecnologías alternativas que puedan ser empleadas sean validadas por una entidad técnica especializada; y contar con aprobación del OSIPTEL.

4.4 En caso se insista con la aprobación de la totalidad de las disposiciones del Proyecto de Ley, se requiere que esta sea modificada a fin de incluir los comentarios expuestos en el presente informe.

V. RECOMENDACIÓN

Conforme a lo expuesto, se recomienda remitir el presente informe a la Presidencia del Consejo de Ministros y al Congreso de la República, para los fines correspondientes.

Atentamente,

Firmado digitalmente por:VILCHEZ ROMAN Marco Antonio FAU 20216072155 soft

OSIPTEL OAJ A. Arequipeño

OSIPTEL OAJ C. CÁMARA

OSIPTEL DPRC R.ALANIA

OSIPTEL DPRC D.ARGANDOÑA

OSIPTEL DPRC R.ESPINOZA