Consulta ciudadana Norma técnica que regula el sistema de bloqueo efectivo de los dispositivos robados, hurtados o extraviados	
Nombre completo	Christian Feliu
Empresa (si aplica)	Telefónica Móviles Chile S.A.
Cargo (si aplica)	Gerente de Regulación
Artículo N°1	
Artículo N°2	Respecto de la obligación de remitir todo el tráfico de voz-datos-sms, debemos hacer presente que, para el caso de Telefónica, esto involucraría un volumen de varios miles de millones de registros diarios asociados al tráfico cursado por nuestra red. El tamaño y frecuencia de intercambio de información que se propone, así como el manejo del dígito verificador, tendrá impacto en el rendimiento del EIR y, en el breve plazo otorgado para esta consulta pública, no es posible llegar a dimensionar el nivel de inversión que se requerirá para los nuevos desarrollos sistémicos y las plataformas que permitan soportar esta nueva lógica de funcionamiento del EIR. En consecuencia, es necesario dejar constancia de las enormes complejidades y dificultades técnicas que dicha exigencia conlleva para su implementación en las condiciones requeridas y la nueva e importante carga económica que se le suma a una industria sumida en una grave crisis de sostenibilidad financiera. Desde el punto de vista operativo, debemos señalar que, de acuerdo con nuestras estimaciones preliminares, el tiempo de procesamiento necesario para la mera lectura de dichos registros alcanzaría un promedio de doce (12) horas continuas, considerando la volumetría indicada. A ello debe añadirse que nuestra infraestructura de red, por diseño técnico, no entrega el número de IMEI con dígito verificador, circunstancia que obligaría a efectuar un cálculo adicional de verificación sobre cada uno de los registros. Este proceso complementario, aplicado a la totalidad de los datos exigidos se estima que insumirá aproximadamente diez (10) horas adicionales continuas de cómputo y validación. De esta forma, el cumplimiento íntegro de la normativa, en las condiciones propuesta por esta consulta pública, implicaría un ciclo total de procesamiento y entrega de más de veinte (20) horas, lo cual excede la razonabilidad de un proceso operativo diario y pone de manifiesto la complejidad técnica y la imposibilidad práctica de implementación sin mediar previamente las adecuaciones tecnológicas pertinentes. Por otro lado, esta propuesta normativa no es precisa ni clara en cuanto a procedimiento y/o tratamiento de una serie de otras situaciones que podrían presentarse, tales como: •el tráfico de roaming out nacional, en donde no se dispone de la información de localización (coordenadas de la estación base); •el tráfico de roaming in nacional, donde un suscriptor que origine tráfico en la red de un tercero no tendrá cómo ser localizado por el operador dueño de la IMSI. •El método actual para identificar e ingresar IMEIs en la lista de observación no contempla casos en los que el IMEI ha sido modificado por uno nuevo, único y que cumple con el formato de la GSMA, pero que no ha sido utilizado previamente. Esta omisión permite que dispositivos robados continúen operando sin ser detectados, eludiendo el bloqueo efectivo. El mecanismo de detección se basa en identificar comunicaciones generadas por un mismo IMEI asociado a distintas IMSIs en ubicaciones cuya distancia excede los umbrales definidos en la tabla. Sin embargo, si el IMEI modificado no presenta coincidencias previas, no se activa la alerta, lo que representa una vulnerabilidad en el sistema de detección propuesto. •Las sesiones de datos usualmente duran más de 60 minutos, por lo que no aplicaría la Tabla tiempo/distancia. •No se aclara la relación, entre estas nuevas listas y las existentes. Finalmente, hacemos presente que administrar un volumen de información de la magnitud involucrada en esta propuesta, supondrá desafíos de gestión y operación extraordinarios, pues requiere procesar, validar y consolidar cifras enormes de pares de datos históricos. Dicha operación no solo exige una infraestructura tecnológica de altísima capacidad y sofisticación, sino también sistemas avanzados de interoperabilidad entre concesionarias y organismos técnicos, asegurando la unicidad, trazabilidad y seguridad de todas las transacciones registradas. Esta magnitud de datos implica también riesgos de errores, inconsistencias y costos considerables tanto en recursos humanos como técnicos, incrementando la posibilidad de impactos colaterales en la calidad del servicio y la fiabilidad del sistema centralizado, pudiendo mencionarse, entre otros: •Sobrecarga operativa y de red: La generación y envío de archivos diarios de muy elevado volumen de información requeriría recursos de TI y de red considerables, pudiendo comprometer la estabilidad de sistemas productivos y de reportes críticos. •Ineficiencia en el tratamiento de datos: La mayoría de los registros transmitidos no presentan irregularidades ni valor analítico para la detección de fraudes, lo que implica procesar masivamente información irrelevante para el fin buscado.

•Riesgo de exposición de datos sensibles: El traslado diario de información de geolocalización masiva contraviene los principios de minimización y proporcionalidad en el tratamiento de datos personales, incrementando la superficie de riesgo frente a accesos no autorizados.
•Latencia: Los tiempos de transferencia (varias horas, dependiendo de la capacidad del enlace) reducen la inmediatez que se busca lograr en los mecanismos de bloqueo y observación.

Cabe hacer presente y tener a la vista algunas experiencias internacionales similares. En efecto, está el caso cercano de Colombia, donde se implementó un sistema para identificar, registrar y gestionar el acceso de los dispositivos a las redes móviles del país y para establecer un proceso de bloqueo de aquellos identificados como robados. Como se indica en un reporte de GSMA (CyberSecurityReport_Spanish_Web_Singles-2.pdf), esta estrategia basada en el IMEI fue pionera en la región al ser implementada por primera vez en 2011. Se dictaron una serie de normativas asociadas que suponían una gran carga regulatoria para su cumplimiento; creaba barreras para la venta o traspaso de equipos y asignaba responsabilidades legales y financieras a los operadores. Lamentablemente, como lo indica GSMA, el esfuerzo no tuvo éxito en resolver el problema social del robo de equipos; no logró marcar una diferencia y terminó imponiendo costosas obligaciones al ecosistema móvil. Casi una década después, en 2020, viendo que los resultados no justificaban los costos, el regulador colombiano decidió incluir la exigencia de registro de equipos dentro de la lista de normativas a eliminar, como parte de una estrategia global de simplificación regulatoria.
Está también un caso más lejano como el de Pakistan con DIRBS (Device Identification Registration and Blocking System). El objetivo de este proyecto fue:
1.- Eliminar equipos falsos, clonados o importados ilegalmente.
2.- Asegurar que cada IMEI en las redes móviles sea único, válido y registrado.
3.- Crear una base de datos nacional de IMEIs (con cruces GSMA + EIR + aduanas).
4.- Bloquear automáticamente los dispositivos no conformes.
Fue desarrollado entre 2016 y 2018, y se encuentra operativo desde 2019.
Los principales inconvenientes estuvieron en lo complejo de la integración técnica:
* Requería sincronizar bases GSMA, Aduanas y EIR de los operadores en un solo sistema nacional.
* Se enfrentaron inconsistencias de datos, IMEIs duplicados o inválidos, y falta de estándares en los dumps de operadores

	También se produjo una resistencia gigante de mercado gris y del mercado formal comercial, y por último se vieron afectados los usuarios por bloqueos masivos errados. Otra falla fue por el lado de escalamiento y capacidad operativa ya que el sistema procesaba millones de registros: más de 100 millones de IMEIs pareados y 53 millones bloqueados, lo que exigió automatización y capacidad de cómputo no habitual para un regulador y finalmente el regulador debió transformar su modelo de fiscalización y pasar de decisiones legales a decisiones solventadas en análisis de datos (millones) e informáticas (capacidad e hardware para poder administrar este proyecto). En razón de todo lo expuesto anteriormente, resulta imperioso replantearse el modelo propuesto en el borrador de norma técnica en consulta, de manera de simplificarlo de forma relevante, sin perder de vista los objetivos de eficiencia y de resguardo a la privacidad de la información. Para ello, se propone analizar un modelo por fases, que contemple lo siguiente: Fase 1: Dataset Diario Compacto Cada operador enviará una vez al día un dataset consolidado que contenga: •Pares únicos IMEI–IMSI activos del día. •IMEI completo de 15 dígitos y fecha de referencia. Este dataset no incluirá coordenadas geográficas ni registros por evento, reduciendo drásticamente el volumen y el riesgo de exposición. Fase 2: Requerimiento de Detalle La plataforma central será la encargada de consolidar la información de todas las operadoras y detectar patrones sospechosos (por ejemplo, IMEI con múltiples IMSI; IMEI activos en más de un operador o simultaneidad incompatible). Ante la detección de este tipo de casos, la plataforma emitirá un Requerimiento de Detalle (RD) a los operadores involucrados, solicitando únicamente: •Los registros detallados del par IMEI-IMSI o conjunto de IMEI observados. El operador responderá con un Dataset Enriquecido Acotado, que incluirá los campos exigidos (timestamp, cell_id, latitud/longitud, tipo de evento) solo para esos casos específicos. Todo esto ya sea para sesiones de voz, SMS o datos.
Artículo N°3	La normativa propuesta no es clara ni precisa en cuanto a qué va a pasar con los IMEI's repetidos que existen en el parque actual. ¿deberán todos ingresar a una lista de excepción? Respecto a la utilización de la declaración jurada como medio de acreditación, ¿qué sucederá en el caso que dos clientes de dos concesionarios diferentes acrediten por esta vía que cuentan con el justo título exigido? ¿quién resuelve una situación de este tipo? Se plantea además que el medio de acreditación de justo título no sea únicamente una declaración jurada notarial, dejando abierta la opción de usar algún otro medio, como la boleta, para este fin.
Artículo N°4	
Artículo N°5	Actualizar la lista negativa de IMEI’s en los EIR cada 15 minutos, conforme a lo exigido por el artículo 5°, expone al sistema a una sobrecarga operacional significativa, puesto que el EIR es un componente crítico del registro y validación de cada dispositivo en la red móvil. El EIR debe verificar el estado del IMEI en tiempo real cada vez que un smartphone intenta acceder a la red, procesando millones de transacciones por hora. Si la lista negativa aumenta considerablemente por actualizaciones frecuentes y masivas, el rendimiento del EIR puede verse comprometido, generando latencias, posibles bloqueos, e incluso fallos en la gestión de acceso de los equipos, afectando la disponibilidad del servicio para todos los clientes, y por tanto la calidad de experiencia que hoy se entrega a los usuarios de toda la industria de telecomunicaciones nacional. Además, incorporar los 15 dígitos con chequeo constante implica que cualquier error en sincronización o actualización puede provocar bloqueos masivos injustificados o permitir la entrada de equipos no autorizados, complicando enormemente el control efectivo de la red móvil y su seguridad.

Artículo primero transitorio	Dada la magnitud de las afectaciones sistémicas y los impactos operacionales que esta normativa puede llegar a tener, así como también la necesidad de definir la mejor opción para crear la plataforma de centralización de datos; fijar términos de referencia; eventualmente abrir proceso de licitación y/o negociar dichos términos; adjudicar y, finalmente, implementar la entrada en operación del sistema, se estima que, a lo menos, se requerirá un plazo de 24 meses para poner en operación la nueva normativa, contados desde que está se publique en el diario oficial. Sin perjuicio de lo anterior, insistimos en la necesidad de ajustar y simplificar la propuesta para esta norma técnica, y aterrizarla a un escenario que resulte viable y realizable, tanto desde el punto de vista del impacto operativo / técnico como desde el punto de vista de la racionabilidad de costos.
Artículo segundo transitorio	
Artículo tercero transitorio	En línea con el objetivo de simplificar y reducir carga regulatoria asociada a esta normativa, se propone que la base histórica de pares IMEI-IMSI a incluir en el Sistema se reduzca a 6 meses.
Anexo	
¿Tiene algún otro comentario que quiera agregar?	