Bogotá, 10 de marzo del 2016.

Doctor
DAVID LUNA SÁNCHEZ
Ministro TIC
Edificio Murillo Toro
Carrera 8 entre calles 12 y 13
Email: david.luna@mintic.gov.co
Bogotá D.C.

Doctor
GERMÁN DARÍO ARIAS PIMIENTA
Director
Comisión de Regulación de Comunicaciones
Calle 59 A bis #5-53 Piso 9
Email: atencion.cliente@crcom.gov.co
Bogotá D.C

Asunto: Comentarios proyecto regulatorio "Revisión de las condiciones y criterios para la identificación de equipos terminales móviles: etapa de verificación centralizada".

Respetado Doctor Luna, y Doctor Arias,

En atención a la publicación del proyecto de modificación de "Revisión de las condiciones y criterios para la identificación de equipos terminales móviles: etapa de verificación centralizada", publicado por la Comisión de Regulación de Comunicaciones, se presentan a continuación los siguientes comentarios sobre el eventual impacto de dichas medidas respecto de la privacidad de los usuario, así como en la posible manifestación de daños antijurídicos por la decisión de adoptar una alternativa regulatoria que resulta más onerosa que el beneficio que se pretende obtener.

En todo momento TigoUne ha manifestado su compromiso con las medidas adoptadas por el Gobierno Nacional en el marco de la estrategia contra el hurto a equipos terminales, no obstante, se presentan las siguientes reflexiones con el propósito que puedan permitir generar nuevas alternativas que generen el logro idóneo del objetivo regulatorio propuesto, en orden a evitar que:

- Se expida una norma regulatoria que no logre la finalidad de disminuir los hurtos, y por tanto, se desvíen los esfuerzos en los que se deben concentrar las entidades estatales para incrementar la operatividad, no solo de la Fiscalía y Policía, sino también de aquellas a cargo de los Alcaldes e Inspectores de Policía.
- Se conduzca eventuales afectaciones a los usuarios en sus derechos constitucionales a la intimidad, autodeterminación informática, y privacidad, por el tratamiento de datos

personales a cargo de un tercero, debido que con la información transferida se permitirían con su cruce y procesamiento establecer patrones de comportamiento y localización del usuario.

- Se presentaría clara transgresión a los principios de libertad, necesidad y finalidad, al no contemplar el respeto a las garantías en materia de autodeterminación digital, respeto del consentimiento libre, previo, expreso e informado; así como, que la finalidad del tratamiento sea constitucionalmente legítima, y referida a que cualquier uso diverso de los datos deba ser autorizado por su Titular.
- Se expediría una norma en la que la CRC no contaría con atribuciones legales para definir condiciones regulatorias para la creación de un sistema centralizador en el que se efectúe el tratamiento de datos personales de los usuarios.
- No se cuenta con suficiente información y experiencias internacionales para adoptar medidas regulatorias orientadas a la identificación y control de IMEIS duplicados, que guarde coherencia con el modelo del Estado Colombiano, el cual constitucionalmente, es un Estado social de derecho, democrático, participativo y pluralista, fundado en el respeto de la dignidad humana.
- Se hace necesario evaluar previamente la posible ocurrencia o comisión de daños antijurídicos, que podrían conllevar por parte de los usuarios a un alto riesgo de litigios judiciales y tutelas.
- Se observa que en caso que se decida continuar con la implementación del sistema centralizador, el tercero responsable será quién tenga los deberes de diligencia y cuidado al que estaría obligado conforme con la ley.
- El sistema centralizador es de poco impacto y utilidad, debido que es una alternativa regulatoria excesivamente onerosa que no va a permitir lograr la erradicación del problema de los IMEI duplicados en Colombia, puesto que estos, son regrabados presuntamente en establecimientos públicos que actualmente no cuentan con ninguna medida de control o registro previo establecido por las Autoridades.
- Conforme lo contemplado en la propuesta regulatoria, se observa poca la utilidad de la información que arroje la detención, ya que los operadores previamente detectarán los duplicados intra-redes.
- El proceso de detención centralizado con un tercero no es infalible, y podrá arrojar falsas alarmas, así mismo la no se evidencia utilidad de establecer algoritmos o procesos para arrojar datos propios de temáticas de las ciencias físicas, como lo es la determinación lógica o improbable de la velocidad del desplazamiento del equipo. Dicho requerimiento o exigibilidad, transgrede todo tipo de lógica para convertirse en una materia objeto de regulación de las telecomunicaciones.
- No se tiene claridad suficiente sobre la aplicación de algoritmos que estaría a cargo del centralizador, lo cual podría conllevar a múltiples modificaciones regulatorias con un alto costo para los PRSTM.
- La iniciativa regulatoria no ha surtido el proceso real y estricto de verificación de impacto regulatorio **previo** a la decisión, que ha recomendado aplicar la OCDE en sus políticas y recomendaciones sobre Gobernanza Regulatoria, y no se cuenta con la suficiente información de las medidas de control a aplicar, por tanto no se tiene claridad sobre la utilidad final del sistema centralizador.
- El problema de hurto a ETM, no es de responsabilidad de los operadores, no obstante se coadyuva con soluciones al mismo. La responsabilidad por el control y judicialización de los responsables, y quienes cometan dichos delitos recae

exclusivamente por disposición de la ley, en la Policía Judicial, Fiscalía y las Autoridades Locales de Policía (Alcaldes e Inspectores de Policía). Un esquema centralizado en el ciclo inter-redes va más allá de la coadyuvancia referida.

1. LA REGULACIÓN NO HA SIDO IDÓNEA PARA REDUCIR EL HURTO A ETM.

Desde el 2011 se han expedido por la Presidencia y la Comisión de Regulación de Comunicaciones, doce (12) normas estableciendo obligaciones en materia de hurto a ETM, que a la fecha que no han logrado su objetivo de disminuir el problema. A continuación se listan dichas normas:

RESOLUCIONES	PUNTOS CLAVE
Decreto 1630 del 2011	▪ Adopta medidas para determinar personas autorizadas venta ETM ▪ Crea obligaciones de implementación bases de datos positiva y negativa ▪ Establece medidas para activación de terminales móviles [verificación previa en base de datos negativa]
Resolución 3128 del 2011	▪ Creó bases de datos positiva y negativa ▪ Determinó obligaciones a los operadores para crear dichas bases de datos, y contratar a un tercero el diseño, puesta en marcha y operación de las mismas ▪ Facultó a los operadores para bloquear los IMEI que se encuentren en base de datos negativa
Decreto 2365 del 2012 [Derogado]	▪ Establece controles exportación equipos terminales móviles ▪ Define nuevos procedimientos para exportación ETM.
Resolución 3667 del 2012	▪ Crea nuevas obligaciones operadores para verificar datos personales de los usuarios para registrarlos o actualizar las bases de datos positivas ▪ Se modifica el procedimiento registro de IMEI ▪ Modifica contenidos de las bases de datos positivas y sus procedimientos asociados
Resolución 3854 del 2012	▪ Modifica tiempos de implementación
Resolución 3947 del 2012	▪ Modifica obligaciones a cargo de los operadores y los contenidos de las bases de datos positivas, y sus procedimientos asociados ▪ Modifica procedimiento registro de IMEI ▪ Establece plazos para que los usuarios registren sus ETM
Resolución 4107 del 2012	▪ Establece nuevas obligaciones a los PRSTM.
Resolución 4585 del 2014	▪ Crea el Registro de Personas Autorizadas para la venta de ETM [excluye operadores]:

	- Solo puede vender ETM quién esté autorizado por el registro de MinTIC - Vigencia 3 años - Obliga a exhibir en un lugar visible la Decisión de Autorización que acredita su calidad de autorizado para la venta al público de ETM [Art. 15.2]
Resolución 4119 del 2013	▪ Crea nuevas obligaciones a los PRSTM ▪ Modifica bases de datos negativas y procedimientos asociados ▪ Crea el formato de declaración de adquisición legal, para cuando el usuario no posea la factura que demuestre la compra del ETM
Resolución 4813 del 2015	▪ Crea nuevas obligaciones a los PRSTM ▪ Obliga a la creación de un nuevo sistema centralizado para verificación de IMEIS duplicados, inválidos, no homologados y no registrados. ▪ Establece nuevas medidas de control en el registro de IMEI.
Decreto 2025 del 2015	▪ Medidas para controlar importación y exportación de teléfonos móviles y sus partes ▪ Crea procedimiento previo a la exportación e importación para verificación de los IMEIS que entrarán al país (solo entran los que no estén en BD negativa) ▪ Los viajeros solo podrán traer hasta 3 equipos. [importación modalidad viajero]
Resolución 4868 del 2016	▪ Crea el procedimiento de diagnóstico y notificación a los usuarios que tengan IMEI alterados [no correspondencia con BD homologados de la GSMA y CRC] ▪ Define medidas de control para bloquear los IMEI de los usuarios que no registren a tiempo sus equipos [desde marzo hasta junio del 2016]

De la enunciación anterior faltaría por adicionar dos resoluciones adicionales que se estiman podrían ser expedidas por la CRC en materia de modificación de plazos y procedimientos para el sistema centralizado de IMEIS, así como las medidas de control de IMEIS duplicados.

La enunciación anterior, refleja cómo la expedición de normas relacionadas con la estrategia de hurto contra equipos terminales, no ha logrado el objetivo de disminuir o erradicar las causas de los hurtos a los ETM.

De acuerdo con datos de la Presidencia de la República[1], sólo a partir del 20 de agosto del 2015, se logró una considerable disminución, a partir de las acciones desplegadas por la Policía Nacional y con la Fiscalía General de la Nación, de acuerdo con las medidas coordinadas directamente desde la Presidencia de la República.

Dicha situación, antes que incrementar las obligaciones regulatorias, los esfuerzos estatales deben concentrarse en incrementar la operatividad no solo de la Fiscalía y Policía, sino también de aquellas medidas de Policía a cargo de los Alcaldes e Inspectores de Policía, de manera que se asegure el debido control estatal a uno de los eslabones de la cadenas de hurto contra ETM que faltaría por atender, esto es controlar los establecimientos de venta de ETM para verificar que cuenten con el Registro de Venta vigente, así mismo, adoptar medidas de control para los establecimientos dedicados al mantenimiento y venta de partes de ETM.

Por lo tanto, las últimas modificaciones que incluyen obligaciones sobre la implementación de un ciclo inter-redes centralizado, van más allá del objetivo de la estrategia, que no es otro que concentrar los esfuerzos en incrementar la operatividad referida. Se hace por tanto un llamado a dirigir las medidas, al control de dichos establecimientos, así como los responsables del tráfico de partes de ETM, y asegurar la continuidad de la operatividad de policía judicial para el desmantelamiento y judicialización de las bandas dedicadas al hurto de ETM.

2. EL SISTEMA CENTRALIZADO PUEDE TRANSGREDIR LA PRIVACIDAD DE LOS USUARIOS.

La Constitución Política establece en el artículo 15 que en toda "recolección, tratamiento y circulación de datos **se respetarán la libertad y demás garantías**

---

[1] Comunicado de prensa Presidencia. Noviembre 25 del 2015:
"Indicó, que en los últimos tres meses "se han recuperado 69 mil celulares, antes se recuperaban 310 celulares por semana, hoy se están recuperando 5. 750 por semana".

En lo corrido del año la cifra de recuperación de móviles asciende 77.800. También dijo que desde el 20 de agosto "hemos desarticulado 29 organizaciones criminales que pertenecen a este conglomerado (…) antes se desarticulaba una organización por mes, ahora se están desarticulando diez por cada mes", en los transcurrido del 2015 se han desmantelado 40 organizaciones.

El Jefe del Estado, igualmente, señaló que en los últimos 90 días "han sido judicializadas 10.500 personas por robo de celulares, 400 personas por semana, esto se ha más que duplicado, ahora se están judicializando 877 personas por semana". De acuerdo con lo establecido la cifra total de personas judicializadas este año llega a 22.029.

http://wp.presidencia.gov.co/Noticias/2015/Noviembre/Paginas/20151125_12-Estrategia-contra-el-hurto-de-celulares-produce-en-solo-tres-meses-resultados-contundentes-en-el-pais.aspx#.Vs99ofnhBD8

consagradas en la Constitución". Dicho articulado, contiene la base constitucional, mediante la cual se desarrollaron las leyes estatutarias 1266 del 2008 y la 1581 de 2012, y sus decretos reglamentarios[2], que definieron los lineamientos legales para la protección de datos personales[3] en cuanto la recolección, tratamiento, circulación y transferencia de los mismos.

A partir de dicho cuerpo normativo, y partiendo de las reglas jurisprudenciales de la Corte Constitucional, se plantea para el caso concreto que, no obstante la finalidad pretendida con el sistema centralizado es la de contar con un diagnóstico periódico del estado de IMEIS duplicados de equipos terminales móviles que cursen tráfico de red en Colombia, por el contrario a lo pretendido, se podría generar un eventual alto riesgo de posibles atentados indiscriminados a la privacidad de los usuarios, a partir de los datos a que se obliga entregar por parte de los PRSTM, para su tratamiento a través del sistema centralizado que permitirían con su cruce y procesamiento establecer patrones de comportamiento y localización del usuario.

Dicha situación, es factible debido que se entregaría aún tercero (actualmente indeterminado) lo siguientes datos:

DATO A SUMINISTRAR AL TERCERO	EFECTO EN LA PRIVACIDAD DE LOS USUARIOS
Hora Inicio y Fin	Determina el momento exacto en el que el usuario cursa tráfico de red con los operadores.
IMEI	Identifica el Equipo Terminal Móvil.
IMSI	Identifica el número telefónico del usuario. Esta información, conjuntamente con los datos del usuario contenidos en el Registro de IMEIS o en el Reporte de Hurto o extravío permite identificar y determinar a la persona tenedora del servicio.
CELL IDENTITY	Identifica la celda a la cual se conecta el ETM cuando curse tráfico en la red. Dicha celda está geo localizada con coordenadas que deben suministrarse al tercero.
CÓDIGO DE LOCALIZACIÓN DE ÁREA (LAC) de inicio y fin de llamada	El código LAC permite identificar el área de localización usada en las redes móviles.
MOBILE STATION CLASSMARK (MSC)	De acuerdo con el Documento de Soporte de la CRC, este dato "*[p]ermite la identificación de escenarios en los*

[2] Las leyes referidas han sido reglamentadas mediante los Decretos 1727 del 2009, 2952 del 2010, 1377 del 2013 y 886 del 2014, en asuntos como tipos de datos, tratamiento de datos en casos de fuerza mayor, reglamento de registro de bases de datos, aviso de privacidad, autorización de datos sensibles, política de tratamiento, entre otros asuntos.

[3] Conforme lo dispone el literal c) del artículo 3 de la Ley 1581 del 2012, un dato personal es *"Cualquier información vinculada o que pueda asociarse a una o varias personales determinadas o determinables"*.

(empleado en el establecimiento de la llamada)	*que el equipo informa las capacidades de la tecnología de radio acceso que estén en desacuerdo con la información del TAC en la GSMA, así como los valores reportados que varían para un mismo IMEI.* *Este parámetro, a pesar que no se utilizará como uno de los criterios para la detección de IMEI duplicados en la etapa inter red, es de utilidad en el análisis posterior para apoyar las labores de identificación del equipo legítimo y sus duplicados*". El MSC contiene además el código de clasificación del equipo terminal móvil con la estación (celda), permitiendo identificar los niveles de revisión, el RF Power, algoritmo de encriptación, la capacidad de frecuencia y capacidad de mensajes cortos. Dichos datos identifican el nivel máximo de potencia/capacidad que puede alcanzar un terminal.

Los datos anteriormente referidos que se entregarán por decisión regulatoria a un tercero (actualmente indeterminado), para uso, tratamiento y procesamiento, no aseguraría el cumplimiento de una finalidad constitucionalmente legítima acorde con los principios de finalidad, necesidad y libertad, reconocidos en las reglas jurisprudenciales de la Corte Constitucional y acogidas por el Consejo de Estado.

- El **principio de libertad**, conforme lo indica la regla jurisprudencial contenida en la Sentencia C-748 del 2011. "Este principio, pilar fundamental de la administración de datos, **permite al ciudadano elegir voluntariamente si su información personal puede ser utilizada o no en bases de datos**". […] "En efecto, el ser humano **goza de la garantía de determinar qué datos quiere sean conocidos y tiene derecho a determinar lo que podría denominarse su "imagen informática**". (negrita añadida)

- El **principio de finalidad**, indica que "la finalidad no solo **debe ser legítima sino que la referida información se destinará a realizar los fines exclusivos para los cuales fue entregada por el titular**. Por ello, se deberá informar al Titular del dato de manera clara, suficiente y previa acerca de la información suministrada y por tanto, no podrá recopilarse datos sin la clara especificación acerca de la finalidad de los mismos. **Cualquier utilización diversa, deberá ser autorizada en forma expresa por el titular".** […] "Esta precisión es relevante en la medida que permite un control por parte del titular del dato, en tanto le es posible verificar si está haciendo (SIC) usado para la finalidad por él autorizada. **Es una herramienta útil para evitar arbitrariedades en el manejo de la información por parte de quien trata el dato**"[4]. (negrita añadida)

[4] Regla jurisprudencial contenida en la Sentencia C-748 del 2011.

Igualmente, "Si, con el tiempo, **el uso de los datos personales cambia a formas que la persona razonablemente no espera, debe obtenerse el consentimiento previo del titular**"[5]

- El **principio de necesidad**, fue desarrollado en sentencias T-307 de 1999, SU-082 de 1995, y T-176 de 1995, y refiere a que los datos personales registrados deben ser los estrictamente necesarios para el cumplimiento de las finalidades perseguidas con las bases de datos, de tal forma, que se encuentra **prohibido el registro y divulgación de datos que no guarden estrechan relación con el objetivo de la base de datos[6]. (negritas añadidas)**

Si se pretende expedir el proyecto regulatorio publicado, se presentaría clara transgresión a los principios de libertad, necesidad y finalidad, al no contemplar el respeto a las garantías que a continuación se referirán, en materia de autodeterminación digital, respeto del consentimiento libre, previo, expreso e informado; así como, que la finalidad del tratamiento sea constitucionalmente legítima, y referida a que cualquier uso diverso de los datos deba ser autorizado por su Titular. Igualmente, constitucionalmente está prohibido el registro y divulgación de datos que no guarden relación con el objetivo de la base de datos, que para el caso en comento, aquellos datos que no guarden relación con el objetivo a que son llamados los PRST en la provisión de redes y servicios de telecomunicaciones a través del espectro electromagnético asignado.

En desarrollo de lo anterior, en regla jurisprudencial contenida en Sentencias T-350 de 1993 y SU-082 de 1995, traídas a colación en Sentencia C-748 del 2011, reconoce que el habeas data es una garantía del derecho a la intimidad, así como una manifestación al libre desarrollo de la personalidad[7]. No obstante a partir de 1995, surge otra línea interpretativa que lo trata como un derecho autónomo y así ha prevalecido desde entonces. En sentencia SU-082 de 1995 el derecho de habeas data está compuesto por la autodeterminación informática y la libertad, y comprende las siguientes prerrogativas:

- El derecho a conocer las informaciones que a ella se refieren
- El derecho a actualizar tales informaciones, es decir, a ponerlas al día, agregándoles los hechos nuevos.
- El derecho a rectificar las informaciones que no correspondan a la verdad
- Derecho a la caducidad del dato negativo.

De esta manera se configura un derecho autónomo reconocido como **Libertad Informática y Autodeterminación**, la cual consiste "en la facultad de disponer de la información, de preservar la propia identidad informática, es decir, de permitir,

[5] Ibídem.
[6] Ibídem
[7] Sentencia T-340 de 1993 MP Carlos Gaviria Díaz

controlar o rectificar los datos concernientes a la personalidad del titular de los mismos, y que, como tales, lo identifican e individualizan ante los demás"[8].

En Sentencia SU-082 de 1995, se reconoce "la autodeterminación informática [como] la facultad de la persona a la cual se refieren los datos, para autorizar su conservación, uso y circulación, de conformidad con las regulaciones legales". Igualmente "el derecho a la autodeterminación informativa implica, como lo reconoce el artículo 15 de la Constitución, la facultad que tienen todas las personas de "conocer, actualizar y rectificar las informaciones que hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas"[9].

Dicha garantía a la libertad informática y la autodeterminación de la persona en materia de sus datos relacionados con el servicio móvil, se vería transgredido al impedir que la persona manifieste su consentimiento "previo, expreso e informado"[10] con relación a los datos que configuran su interacción con las redes móviles.

Al respecto, en sentencias C-729 de 2002 MP Eduardo Montealegre Lynett, y T-414 de 1992 MP Ciro Angarita Barón, la Corte Constitucional precisó las características de los datos personales – en oposición a los impersonales-, de acuerdo con los siguientes criterios:

i. Estar referido a aspectos exclusivos y propios de una persona natural
ii. Permitir identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos.
iii. Su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita, y
iv. Su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación.

Dada las características de los datos personales, en coherencia con el derecho a la libertad informática y la autodeterminación, la Corte Constitucional en Sentencia C-748 del 2011 ha reiterado que el consentimiento debe otorgarse en todo momento de manera "**previa, expresa e informadas**", y tiene como características lo siguiente:

- **Previa:** "*La autorización del dato debe ser suministrada en una etapa anterior al dato*" [11]. En Sentencia T-022 de 1993 la Corte Constitucional, reiterando el precedente contenido en la Sentencia T-592 del 2003, manifestó que la veracidad del dato no implica que el Responsable del Tratamiento no tenga el deber de obtener autorización anterior[12].

[8] Sentencia C-1147 del 2001 MP Manuel José Cepeda.
[9] Sentencia T-552 de 1997.
[10] Regla jurisprudencial contenida en la Sentencia C-748 del 2011.
[11] Ibídem.
[12] Ibídem.

- **Expresa:** "La autorización debe ser inequívoca, razón por la cual, al contrario de lo sostenido por algunos intervinientes, no es posible aceptarse la existencia, dentro del ordenamiento jurídico colombiano, de un consentimiento tácito[13].

  De las reglas jurisprudenciales vigentes, se trae a colación la contenida en la Sentencia T-592 del 2003 en la que se indica que el consentimiento expreso se traducía también en la prohibición de otorgarse autorizaciones abiertas y no específicas. *"[…] no obstante haberse otorgado autorizaciones para reportar la información crediticia, las mismas eran "abiertas y accesorias a las operaciones de crédito" por lo que no denotaban un real consentimiento de los otorgantes "en cuanto no estuvieron acompañadas de la información oportuna sobre su utilización, aparejada del alcance del reporte, ni de su contenido y tampoco del nombre y ubicación de la encargada de administrar la información"*.

- **Informado**: El titular no solo debe aceptar el Tratamiento del dato, sino también tiene que estar plenamente consciente de los efectos de su autorización. En Sentencia T-592 del 2003, la Corte Constitucional establece las siguientes reglas:

  i. **Los datos personales sólo pueden ser registrados y divulgados con el consentimiento libre, previo, expreso e informado del titular. Es decir no está permitido el consentimiento tácito del Titular del dato y sólo podrá prescindirse de él por expreso mandato legal o por orden de autoridad judicial,**
  ii. El consentimiento que brinde la persona debe ser definido como una indicación específica e informada, libremente emitida, de su acuerdo con el procesamiento de sus datos personales. Por ello, el silencio de su Titular nunca podrá inferirse como autorización del uso de su información y,
  iii. El principio de libertad no solo implica el consentimiento previo a la recolección del dato, sino que dentro de éste se entiende incluida la posibilidad de retirar el consentimiento y de limitar el plazo de su validez. (negritas añadidas)

Por lo anterior, se tiene total claridad constitucional acerca de la garantía que todo sujeto obligado, debe solicitar el consentimiento previo, expreso e informado del usuario, y que en todo caso, solo puede prescindirse del por "mandato legal o por orden judicial", resaltando que dicho mandato legal por referirse al ámbito de derechos y garantías de la persona, se debe dar cumplimiento al principio de estricta reserva legal, por tanto, solo el legislador en uso de sus competencias podría decretar de prescindir de dicho consentimiento del titular en casos específicos, es decir autorizar por medio del ley al tratamiento de datos personales bajo una finalidad concreta.

[13] Precedente contenido en la Sentencia C-748 del 2011, a partir de las reglas jurisprudenciales de las sentencias SU-089 de 1995, T-590 DE 1995, T-580 de 1995, y T-657 DE 2005.

A pesar que se pueda contar con la autorización o consentimiento del usuario, se presentaría una carga mayor, que significaría desplegar actividades para la obtención de los consentimientos previos, expresos e informados, lo que podría conllevar incluso a la modificación de los contratos vigentes con los usuarios.

No obstante, la Ley Estatutaria 1581 del 2012, en su artículo 10, establece ciertos casos en los que se permite realizar tratamiento de datos personales sin contar con la autorización previa de su titular, y está exclusivamente referido a aquella "*información requerida por una entidad pública o administrativa en ejercicio de sus funciones o por orden judicial*", así como entre otras causales, como en casos de "*urgencia médica o sanitaria*", "*datos de naturaleza pública*", "*tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos*".

La situación jurídica anteriormente referida, no es aplicable para el caso que atiende el presente asunto regulatorio, debido que no se está frente al cumplimiento de facultades regulatorias atribuidas a la Comisión de Regulación de Comunicaciones por mandato de la Ley 1341 del 2009, esto con ocasión a que la misma CRC en el Documento de Soporte al proyecto ha manifestado lo siguiente "*Se encontró además que para el proceso del ciclo inter red, dicha obligación no podrá estar a cargo de la CRC, como fue propuesto por la industria, dado que esta Entidad, a la luz del principio de legalidad en las actuaciones administrativas consagrado en los artículos 6º y 121º de la Constitución Política, **no posee facultades en la materia***". (Negritas añadidas)

Adicionalmente, y conforme lo indica la CRC en su documento de soporte "*de acuerdo con el artículo 106 de la Ley 1453 de 2011 y el Decreto 1630 de 2011, las competencias de la CRC se circunscriben a la adopción de medidas regulatorias que se concretan en la expedición de actos administrativos de contenido general, mediante los cuales se establezca el contenido de las obligaciones de información a cargo de los proveedores y comercializadores, así como las condiciones y características de las bases de datos positiva y negativa",* por lo anterior la CRC carece de total competencia incluso para expedir medidas regulatorias de obligación de implementación de un sistema centralizador de identificación de IMEIS ya que las mismas exceden incluso las atribuciones otorgadas por el artículo 106 de la Ley 1453 del 2011 y del Decreto 1630 de 2011 que se circunscriben a establecer las condiciones de las bases de datos positiva y negativa que son ajenas y diametralmente diferentes al sistema centralizador propuesto.

En conclusión, la CRC no cuenta con atribuciones legales para definir condiciones regulatorias para la creación de un sistema centralizador en el que se efectúe el tratamiento de datos personales de los usuarios.

Al respecto, de acuerdo con los postulados de la Corte Constitucional en Sentencia C-1011 de 2008, traídos a colación en el Concepto de la Superintendencia de Industria y Comercio de radicado 14-230347-3-0 suscrito el 5 de noviembre del 2014 por la Oficina Asesora Jurídica de la SIC, se manifestó lo siguiente:

"En relación, con las autoridades públicas o administrativas, señaló la Corporación que tal facultad "no puede convertirse en un escenario proclive al abuso del poder informático, esta vez en cabeza de funcionarios del Estado. Así, el hecho que el legislador estatuario haya determinado que el dato personal puede ser requerido por toda entidad pública, bajo el condicionamiento que la petición se sustente en la conexidad directa con alguna de sus funciones, de acompasarse con la garantía irrestricta del derecho al hábeas data del titular de la información […]

Para la Corte, esto se logra a través de dos condiciones: (i) el carácter calificado del vínculo entre la divulgación del dato y el cumplimiento de las funciones de la entidad del poder Ejecutivo; y (ii) la adscripción de dichas entidades de los deberes y obligaciones que la normatividad estatutaria predica de los usuarios de la información, habida consideración que ese grupo de condiciones permite la protección adecuada del derecho".

En refuerzo a lo anterior, la misma Ley Estatutaria 1581 del 2012 en su artículo 13, define a quiénes (titulares o terceros) se les puede suministrar los datos personales:

*"**Artículo 13. Personas a quienes se les puede suministrar la información**. La información que reúna las condiciones establecidas en la presente ley podrá suministrarse a las siguientes personas:*
***a)** A los Titulares, sus causahabientes o sus representantes legales.*
***b)** A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial.*
***c)** A los terceros autorizados por el Titular o por la ley".*

De lo expuesto es claro que sólo se puede suministrar información a terceras personas que sean entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial, o a terceros autorizados [y determinado] por el Titular o por la ley [principio de estricta reserva de ley].

De acuerdo con los postulados referidos, se puede concluir de manera preliminar lo siguiente:

1. La CRC ha indicado expresamente que no posee facultades para efectuar tratamiento de datos solicitados para la verificación centralizada.
2. El consentimiento del Titular es requerido en forma "previa, expresa e informada", y solo se puede prescindir por estricta disposición de Ley. Y se deja claridad, que no obstante se pudiere obtener, el usuario puede negarse a suministrarlo.
3. Los datos pueden transferirse a terceros siempre que tengan la calidad de entidad pública en ejercicio de sus competencias administrativas o judiciales, o a terceros autorizados por disposición de la Ley.
4. Si se pretende expedir el proyecto regulatorio publicado, se presentaría clara transgresión a los principios de libertad, necesidad y finalidad, al no contemplar el respeto a las garantías en materia de autodeterminación digital, respeto del

consentimiento libre, previo, expreso e informado; así como, que la finalidad del tratamiento sea constitucionalmente legítima, y referida a que cualquier uso diverso de los datos deba ser autorizado por su Titular.

Finalmente, frente al tema de la estricta reserva legal, no sobra recordar, que el Consejo de Estado, en decisión de la sección primera de la Sala de lo Contencioso Administrativo en decisión del 18 de febrero del 2016 (radicación 11001-0324-000-2013-00397-00, CP Guillermo Vargas Ayala) en proceso de nulidad contra la Nación – Ministerio de Justicia y del Derecho, Ministerio de Defensa Nacional, y Ministerio de Tecnologías de la Información y las Comunicaciones, manifestó para el caso del Decreto 1704 de 2012 que la obligación que tienen "los proveedores de redes y servicios de telecomunicaciones que operen al interior del territorio nacional de proveer los puntos de conexión y de acceso a la captura del tráfico de las comunicaciones que cursen por sus redes a los organismos de policía judicial con la sola orden del Fiscal General de la Nación, y demás autoridades competentes, constituye una transgresión al principio de estricta reserva de la ley, y un "exceso del ejercicio de la potestad reglamentaria" con fundamento en lo siguiente:

El Consejo de Estado, refiere como base jurídica de su sustentación, que en los siguientes instrumentos internacionales de derechos humanos se consagra esta garantía constitucional:

- La Declaración Universal de Derechos Humanos en su artículo 12 señala que: *"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques"*.
- El Pacto Internacional de Derechos Civiles y Políticos en su artículo 17.1 establece que: *"Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. Toda persona tiene derecho a la protección de ley contra esas injerencias o esos ataques"*.
- La Convención Americana sobre Derechos Humanos en su artículo 11.2 prevé: *"Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, no de ataques ilegales a su honra o reputación. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques."*

En materia de la limitación al derecho de la intimidad, en el contexto del tratamiento de datos personales, el Consejo de Estado trae como referencia las reglas jurisprudenciales de la Corte Constitucional, indicando que "*las limitaciones al derecho a la intimidad, al igual que de cualquier otro derecho fundamental, deben respetar los principios de razonabilidad y proporcionalidad en el contexto del sistema democrático*"[14]. Y solo a partir de autorización de juez de control de garantías (para

[14] Referido a Sentencias T-787 de 2004, T-453 de 2005, C-640 de 2010, y C-540 de 2012, entre otras.

el caso de dicha Sentencia) se podría autorizar una injerencia al marco de la intimidad del usuario. Al respecto, refiere el Consejo de Estado el precedente contenido en la Sentencia C-336 de 2007, en la cual, a "partir de las anteriores referencias jurisprudenciales, concluyó lo siguiente:

(i) que como principio general, toda medida de investigación que implique afectación de derechos fundamentales debe estar *precedida* de autorización del juez de control de garantías; y
(ii) que como consecuencia de ello el control posterior autorizado por la Carta (art. 250.2) respecto de ciertas medidas que afectan derechos fundamentales, configura una *excepción* a la regla general".

De esta manera se configura el ámbito de protección del derecho de la intimidad garantizando en ejercicio del poder judicial, aquellas interceptaciones a las comunicaciones de los usuarios.

Desarrollado el contexto anterior, para el Consejo de Estado y sobre el caso de la expresión *"o demás autoridades competentes"* contenida en el artículo 4º del Decreto 1704 de 2012, indicó que se entrañaba una "una habilitación genérica para que cualquier autoridad, y no solamente la Fiscalía General de la Nación, pueda acudir a los proveedores de redes y servicios de telecomunicaciones y solicitar el suministro de los datos del suscriptor, tales como su identidad, dirección de facturación y tipo de conexión. Estiman los demandantes que, por ese motivo, la frase demandada, además de una vulneración al derecho a la intimidad, supone un exceso en el ejercicio de la potestad reglamentaria por parte del Gobierno y un desconocimiento de la competencia para modificar leyes, toda vez que por Constitución y por Ley, se trata de una facultad que es privativa del ente investigador".

Sobre dicho motivo la Sala observó lo siguiente:

*"**(i)** Según se ha precisado en esta providencia, de acuerdo con lo establecido en el artículo 15 de la Constitución Política, la correspondencia y demás formas de comunicación privada son inviolables, pudiendo ser interceptadas o registradas mediante orden judicial **en los casos y con las formalidades que establezca la Ley**.*

[..]

*Como se observa, es claro que **constitucionalmente toda intervención en un ámbito reservado de la intimidad de las personas como es el de las comunicaciones privadas goza de una reserva legal**. En consecuencia, sin perjuicio de límites materiales inexcusables que debe respetar el legislador como el principio de proporcionalidad, **la legitimidad de esta clase de injerencias estatales en lo personal dependerá de que haya sido prevista por una disposición con rango de ley**.*

Refiriéndose a esta materia la Corte Interamericana de Derechos Humanos ha señalado que "[e]l derecho a la vida privada no es un derecho absoluto y, por lo

tanto, puede ser restringido por los Estados siempre que las injerencias no sean abusivas o arbitrarias; por ello, las mismas deben estar previstas en ley, perseguir un fin legítimo y cumplir con ***los requisitos de idoneidad, necesidad y proporcionalidad****, es decir, deben ser necesarias en una sociedad democrática"*[15].

En el mismo sentido ha puesto de relieve que "el artículo 11 de la Convención reconoce que toda persona tiene derecho al respeto de su honra, prohíbe todo ataque ilegal contra la honra o reputación e impone a los Estados el deber de brindar la protección de la ley contra tales ataques"[16]*. En cuanto a este último aspecto, atinente a la protección legal que se debe proporcionar al derecho a la vida privada, la Corte ha señalado a propósito de las interceptaciones telefónicas, que* ***"teniendo en cuenta que puede representar una seria interferencia en la vida privada, dicha medida debe estar fundada en la ley, que debe ser precisa e indicar reglas claras y detalladas sobre la materia***[17]***, tales como las circunstancias en que dicha medida puede ser adoptada; las personas autorizadas a solicitarla, a ordenarla y a llevarla a cabo; el procedimiento a seguir, entre otros elementos"***[18].

(ii) *El legislador nacional precisamente mediante la* ***Ley 906 de 2004*** *(agosto 31) expidió el Código de Procedimiento Penal. En su artículo 14, referido a la protección del derecho a la intimidad, dispuso que no podrán hacerse registros, allanamientos ni incautaciones en domicilio, residencia, o lugar de trabajo, sino en virtud de orden escrita del* ***Fiscal General de la Nación*** *o su delegado, con arreglo de las formalidades y motivos previamente definidos en la Ley. Y agregó que deberá procederse de la misma manera (esto es, con orden escrita del Fiscal General de la Nación) cuando fuere necesario interceptar comunicaciones.*

[..]

(iii) *[…] El demandante, como antes se dijo, considera que la frase "o demás autoridades competentes" del artículo 4º del Decreto 1704 de 2012, además de vulnerar el derecho a la intimidad,* ***supone un exceso en el ejercicio de la potestad reglamentaria*** *por parte del Gobierno y un desconocimiento de la competencia para modificar leyes, toda vez que por Constitución y por Ley, la facultad de interceptar comunicaciones y de acudir a los proveedores de redes y servicios de telecomunicaciones y solicitar el suministro de los datos del suscriptor (tales como su identidad, dirección de facturación y tipo de conexión) para efectos de esa interceptación, es una facultad privativa de la Fiscalía General de la Nación.*

---

[15] Corte Interamericana de Derechos Humanos, Sentencia de 27 de enero de 2009, Caso Tristán Donoso *vs*. Panamá.
[16] Ibídem.
[17] Cfr. ECHR Case of Kruslin v. France, judgment of 24 April 1990, Serie A, No. 176-A, párr. 33, y Case of Huvig v. France, judgment of 24 April 1990, Serie A No. 176-B, párr. 32.
[18] Corte Interamericana de Derechos Humanos, Sentencia de 6 de julio de 2009, Caso Escher y Otros vs. Brasil.

(iv) Pues bien, en orden determinar si prospera o no la censura alegada, es preciso señalar que la potestad reglamentaria es entendida como la facultad constitucional que se atribuye de manera permanente al Gobierno Nacional, en cabeza del Presidente de la República, para expedir un conjunto de disposiciones jurídicas de carácter general y abstracto para la debida ejecución de la ley, a través de las cuales desarrolla las reglas y principios en ella fijados y la completa en aquellos detalles y pormenores necesarios que permiten su aplicación, ***pero que en ningún caso puede modificar, ampliar o restringir en cuanto a su contenido material o alcance***[19]*.*

[…]

(v) *Al examinar la normativa acusada a la luz de la disposición legal que le sirve de fundamento y de cara al alcance de la potestad reglamentaria conferida al Presidente de la República, encuentra la Sala que la frase "o demás autoridades competentes" del artículo 4º del Decreto 1704 de 2012 excede el contenido normativo del artículo 52 de la Ley 1453 de 2011, en cuanto que amplía las autoridades autorizadas para* ***ordenar*** *la interceptación de comunicaciones y solicitar la información necesaria para llevar a cabo dicho procedimiento, señalando además de la Fiscalía otras autoridades que no determinó ni precisó.*

En este caso, dado el carácter de asunto reservado a la Ley y la especial sensibilidad de la materia reglamentada, lo previsto por el artículo 52 de la Ley 1453 de 2011 ***constituye un marco inexcusable*** *-más de lo habitual si se quiere- para el ejercicio de la potestad reglamentaria que reconoce al Gobierno el artículo 189 numeral 11 de la Constitución Política.*

Por esta causa, es claro que la habilitación que contiene el precepto impugnado para que otras "autoridades competentes", indeterminadas e indefinidas, distintas a la Fiscalía General de la Nación, puedan acudir a los proveedores de redes y servicios de telecomunicaciones y requerir información personal de quienes se encuentran siendo investigados a efectos de llevar a cabo la interceptación de comunicaciones a que alude el referido artículo 52 reglamentado, constituye un exceso en el ejercicio de la

[19] Ha precisado la Corte Constitucional y el Consejo de Estado que si bien el sistema configurado por la Constitución Política de 1991 atribuyó la titularidad de la potestad reglamentaria al Presidente de la República, según lo refleja el numeral 11 de su artículo 189, no es menos cierto que la propia Carta también se encargó de radicar, de manera precisa, la potestad de producción de actos normativos de efectos generales y de carácter reglamentario en otros órganos constitucionales ubicados dentro de la Rama Ejecutiva (como por ejemplo los Ministerios) y aun fuera de ella. Esta facultad de expedir actos generales, en el caso de los Ministerios, se ejerce en todo caso, frente a la potestad reglamentaria del Presidente de la República, con criterio residual y subordinado. Entre otras sentencias, en la Corte Constitucional, ver las siguientes: C-805 de 2001; C-917 de 2002; C-1005 de 2008; C-372 de 2009 y C-748 de 2011. Y del Consejo de Estado, entre otras, las Sentencias de la Sección Tercera de 14 de agosto de 2008, proferida en el expediente con radicado núm. 11001-03-26-000-1999-00012-01(16230), C.P. Mauricio Fajardo Gómez y 7 de octubre de 2009, proferida en el expediente núm. 11001-03-26-000-2000-08448-01(18448), C.P. Enrique Gil Botero.

*potestad reglamentaria, ya que la Ley es clara en señalar que quien **ordena** la interceptación es **"el fiscal"** y no otra autoridad. Y cuando esta norma legal habla de otras "autoridades competentes" se está refiriendo a aquellas encargadas específicamente de la operación técnica de la respectiva interceptación, restringiendo a esa materia el ámbito de su competencia*

*El artículo 52 de la Ley 1453 de 2011, en lo que se refiere a la **autoridad encargada de ordenar la interceptación de comunicaciones** -que es la materia objeto de esa disposición- es claro y expreso en señalar como tal **al Fiscal que adelante la respectiva investigación**, de modo tal que en este aspecto la citada norma legal no exige precisión o puntualización en cuanto a su contenido y alcance, como sí pudiera requerirlo en otros aspectos no previstos ni desarrollados expresamente en ella[20]. Siendo ello así, no es procedente que el Reglamento introduzca modificaciones en relación con la autoridad competente para **ordenar** la interceptación[21].*

*En relación con esta situación debe llamarse la atención sobre cómo la jurisprudencia de esta Corporación ha señalado que: "Las facultades reglamentarias establecidas por el artículo 189 numeral 11 de la Carta, tal como lo ha sostenido la Sala en reiteradas oportunidades, fueron instituidas por el Constituyente como un mecanismo tendiente a garantizar la cumplida ejecución de las leyes, siendo ese el único fin autorizado por ese mandato superior. Así las cosas, al hacer uso de tales potestades, el ejecutivo debe inspirarse en el único propósito de aclarar y hacer mucho más explícita la norma de carácter legal, en orden a facilitar su adecuada interpretación, ejecución y cumplimiento y viabilizar su estricta observancia. En ese contexto, ha de entenderse que **las potestades a que alude el artículo constitucional anteriormente trascrito, no pueden ser ejercidas para ampliar o restringir los alcances de la Ley, apartándose de su sentido original y auténtico"**[22] (negrillas fuera de texto).*

En este orden de ideas, la expresión "o demás autoridades competentes" debe ser declarada nula, pues del análisis efectuado surge que extender la prerrogativa que el artículo 52 de la Ley 1453 de 2011 establece privativamente para la Fiscalía General

---

[20] Por ejemplo en materias como la persona o entidad destinataria de la orden, el tiempo para cumplirla, las formalidades de la solicitud de interceptación y de la orden impartida, etc.

[21] Además, si en gracia de discusión se admitiera que este aspecto requería desarrollo a través de una norma reglamentaria, es evidente que el acto acusado no cumpliría el cometido de la potestad reglamentaria, pues no contribuiría en nada a la debida ejecución de la ley señalar, como lo hace el decreto demandado, que la orden a que se refiere el artículo 52 de la Ley 1453 de 2011 la puede adoptar "la autoridad competente". Esta fórmula, claramente, no es precisa ni detallada a efectos de permitir la cumplida ejecución de la ley.

[22] Consejo de Estado, Sala de lo Contencioso Administrativo, Sección Primera, auto del 2 de septiembre de2010, Rad. No.: 11001-03-24-000-2007-00265-00. C.P.: Rafael E. Ostau de Lafont Pianeta.

de la Nación, es contrario a la norma legal en que la disposición reglamentaria se debía fundamentar".

Por lo anterior, no queda duda alguna que, por un lado, debe darse respeto irrestricto al derecho de la intimidad de los usuarios, y que toda injerencia sobre este, debe estar desplegado con estricta autorización de ley, por tanto, la regulación que expida la Comisión de Regulación e Comunicaciones no puede ser "***ejercidas para ampliar o restringir los alcances de la Ley, apartándose de su sentido original y auténtico"***[23]. Adicional a los postulados constitucionales anteriormente expresados, y dado que la CRC se ha declarado incompetente para conocer del tratamiento de datos que se realicen de manera centralizada, no puede ésta, modificar el alcance de ley (referencia a la Ley Estatutaria indicada) asignando de manera indiscriminada la facultad para tratar datos personales de los usuarios en un tercero indeterminado.

Por lo anterior consideramos y sugerimos se revise cuidadosamente los aspectos anteriormente referidos con el propósito de evitar posibles transgresiones a la constitución y la ley.

3. NO HAY SUFICIENTE INFORMACIÓN NACIONAL E INTERNACIONAL PARA ADOPTAR MEDIDAS DE CONTROL CONTRA DUPLICADOS.

No se encuentra en la experiencia internacional ninguna medida relevante que pueda ser replicable por la CRC para la determinación de regulación orientada a la identificación y control de IMEIS duplicados, y que guarde coherencia con el modelo del Estado Colombiano, el cual constitucionalmente es un Estado social de derecho, democrático, participativo y pluralista, fundado en el respeto de la dignidad humana.

Dicha coherencia constitucional, debe ser debidamente observada por la CRC, en orden a asegurar que cualquier experiencia internacional que sea traída como importante y válida para ser aplicada en Colombia, debe guardar con el modelo constitucional del Estado, y por tanto, asegurar la coherencia del llamado a que todas las "autoridades de la República están instituidas para proteger a las personas y residentes en su vida, honra, bienes, creencias y demás derechos y libertadas y para asegurar el cumplimiento de los deberes sociales del Estado y de los particulares"[24].

4. **SE DEBE PREVENIR LA OCURRENCIA O COMISIÓN DE DAÑOS ANTIJURÍDICOS**.

En virtud de la ley, todas las entidades del Estado están llamadas a adoptar medidas de manera que se prevenga la ocurrencia o comisión de daños antijurídicos. Teniendo lo anterior como punto de partida, de acuerdo con la Agencia Nacional de Defensa Jurídica del Estado[25], indica lo siguiente:

[23] Referencia a la decisión Consejo de Estado.
[24] Constitución Política, artículo 2.
[25] AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO. Guía para la generación de política de prevención del daño antijurídico. Marzo del 2013.

"[L]as decisiones administrativas tienen la capacidad de afectar la distribución de beneficios y de las cargas públicas; es decir, las decisiones estatales determinan los recursos disponibles para los particulares".

La característica esencial del Estado es su poder de constreñir, capacidad que es utilizada para tomar decisiones sobre la distribución de los beneficios de los cuales los administrados pueden disfrutar y de las cargas que los particulares deben soportar (Stigler 1971). Así, la administración pública, al ejercer sus funciones legalmente conferidas, está tomando decisiones generales y concretas que afectan el uso de recursos públicos o que están imponiendo una carga a los administrados. La facultad constitucional de controlar la actividad administrativa[6], otorgada a los jueces, no solo les permite cuestionar las decisiones y actuaciones del Gobierno sino que también convierte a la jurisdicción en un foro en que se desarrolla la competencia por obtener recursos del Estado y evitar las cargas públicas".

Reconociendo que las decisiones regulatorias podrían eventualmente ocasionar daños antijurídicos, se expone que una expedición de la decisión regulatoria publicada, e incluso una continuidad de los efectos parciales de la Resolución 4813 del 2015, podría conllevar por parte de los usuarios a altos riesgos en materia de litigios judiciales y tutelas, por la generación o manifestación de daños antijurídicos en contra de los usuarios, por la afectación de sus derechos en materia de intimidad, privacidad, autodeterminación informática; así como la transgresión al principio de estricta reserva de la ley, debido que se estaría eventualmente expidiendo una norma que podría transgredir los principios constitucionales expuestos, así como un posible exceso de la potestad regulatoria.

Se hace por tanto un llamado respetuoso para que se evalúen los riesgos y se planteen medidas adecuadas para la prevención de los posibles daños antijurídicos que se evidencian pueden presentarse con la implementación de un sistema de verificación centralizada a cargo de un tercero, y con impactos para los usuarios.

5. RESPONSABILIDAD JURÍDICA DEL TERCERO CENTRALIZADOR.

En caso que la CRC decida continuar con la implementación de un sistema centralizador, se pone de presente, que por ningún motivo, la responsabilidad jurídica en materia de tratamiento de datos personales y asuntos de intimidad y privacidad de los usuarios pueda extenderse a los PRSTM.

Al respecto, la responsabilidad del tercero centralizador sería estrictamente autónoma, no obstante se obligue a los PRSTM contratar a dicho tercero. Para el caso concreto, no aplicaría el criterio de delegación o el de "por cuenta de" para el cumplimiento de las obligaciones establecidas en la Ley 1581 del 2012, que en todo caso solo recaerán en cabeza del tercero actualmente indeterminado.

De acuerdo con los ejemplos de la jurisprudencia traídos de la Directiva Europea 1/2010, y referidos por la Corte Constitucional en Sentencia C-748 del 2011, "permite identificar al responsable de otros agentes que participan en el proceso, es él que determina los fines y medios esenciales de tratamiento de datos"; refiere la Corte, que "[d]e esta manera se requiere determinar si las atribuciones en materia de tratamiento de datos personales se da por **competencia legal explícita o si la misma se da por la "capacidad de influencia del hecho**". Dicha distinción generará un marco claro de atribuciones en materia de privacidad y tratamiento de datos, que en todo caso deben ser exigidos de manera autónoma al centralizador, y no como encargo que efectúa los operadores al mismo.

A partir de lo anterior, es el encargado de tratamiento quien tendrá los deberes de diligencia y cuidado respectivos al que estaría obligado conforme lo dispone la Ley 1581 del 2011.

6. UTILIDAD Y POCO IMPACTO DEL CICLO CENTRALIZADOR A CARGO DE UN TERCERO

Dado que conforme al Diagnóstico Preliminar de Tráfico de IMEIS realizado por la CRC con base en los datos suministrados por los PRSTM, se encuentra que los IMEIS duplicados son tan solo alrededor del 4% del problema (en el escenario más ácido conforme la CRC, aunque estimaciones internas con aplicación de algoritmos tiempo y distancia sería menos del 1% del problema), se observa de poca utilidad la propuesta de un ciclo inter-redes centralizado con un tercero por lo siguiente:

1. Es una alternativa regulatoria excesivamente onerosa (se estima alrededor de cuatro millones de dólares por PRSTM) que no va a permitir lograr la erradicación del problema de los IMEI duplicados en Colombia, puesto que estos, son regrabados presuntamente en establecimientos públicos que actualmente no cuentan con ninguna medida de control o registro previo establecido por las Autoridades.

2. Conforme lo contemplado en la propuesta regulatoria, se observa poca la utilidad de la información que arroje la detención, ya que los operadores previamente detectarán los duplicados intra-redes y de allí se podría establecer un universo claro de IMEIS a ser aplicadas medidas de control administrativo que determine la CRC o medidas judiciales en el marco de procesos de judicialización por la comisión de conductas antijurídicas.

3. El proceso de detención centralizado con un tercero no es infalible, y podrá arrojar falsas alarmas (tal y como lo reconoce la CRC en su documento soporte y en el proyecto regulatorio), que implicará mayor carga para los operadores sin un claro beneficio. Se resalta que los PRSTM no cuentan en su objeto social con atribuciones que le signifique realizar investigaciones de tipo de informática forense, por lo que no puede generarse una obligación regulatoria que atente contra el objeto social de las compañías, así como con la naturaleza del servicio de telecomunicaciones prestados por licencia o concesión.

4. Se observa que la información arrojará patrones de comportamiento de los usuarios, que va en contravía de las garantías constitucionales en materia de intimidad y privacidad.

5. No se evidencia utilidad de establecer algoritmos o procesos para arrojar datos propios de temáticas de las ciencias físicas, como lo es la determinación lógica o improbable de la velocidad del desplazamiento del equipo. Dicho requerimiento o exigibilidad, transgrede todo tipo de lógica para convertirse en una materia objeto de regulación de las telecomunicaciones.

6. No se tiene claridad suficiente sobre la aplicación de algoritmos que estaría a cargo del centralizador, lo cual podría conllevar a múltiples modificaciones regulatorias con un alto costo para los PRSTM. Hasta tanto no se tenga claridad suficiente y delimitada de los procedimientos y algoritmos a aplicar, con la debida justificación y legitimidad constitucional para ejecutarlos, se solicita por favor abstenerse de tomar una decisión sobre el objeto regulatorio pretendido en el presente proyecto.

7. La iniciativa regulatoria no ha surtido el proceso real y estricto de verificación de impacto regulatorio **previo** a la decisión, que ha recomendado aplicar la OCDE en sus políticas y recomendaciones sobre Gobernanza Regulatoria.

8. Hasta que no se cuente con la suficiente información de las medidas de control de duplicados a aplicar, no es prudente ni consecuente expedir normas que creen un sistema del que no se tiene claridad sobre su utilidad final.

9. Finalmente, el problema de hurto a ETM, no es de responsabilidad de los operadores, no obstante se coadyuva con soluciones al mismo. La responsabilidad por el control y judicialización de los responsables, y quienes cometan dichos delitos recae exclusivamente por disposición de la ley, en la Policía Judicial, Fiscalía y las Autoridades Locales de Policía (Alcaldes e Inspectores de Policía).

   Adicionalmente, se expresa que un esquema centralizado en el ciclo inter-redes va más allá de la coadyuvancia referida.

7. COMENTARIOS ESPECÍFICOS

De no aceptar las consideraciones anteriores, se pide por favor tener presente los siguientes comentarios específicos:

APARTE	COMENTARIO
Artículo 1	Respecto de la definición de **IMEI Repetidos entre redes,** no debería promoverse diferencia regulatoria entre "IMEI Repetidos" e "IMEI Duplicados". En este aspecto, el comportamiento que se debe definir es en que dichos IMEIS no son únicos y coinciden en su totalidad en numeración para varios dispositivos ETM. Sobre **IMEI Alterados** se propone orientar la definición a cualquier IMEI

	NO original desde fabricación. Se sugiere que no se adopte más terminología y definiciones que hagan más compleja la implementación del proyecto.
Artículo 2	Se sugiere manejar la etapa de validación centralizada solo para IMEI Duplicados, y por tanto, no es procedente mezclar con acciones correspondientes a la etapa de control para Inválidos, No Registrados, No Homologados, los cuales ya se están trabajando por el operador en etapas previas. Respecto del numeral 4.2.2, se debe especificar cuáles campos del CDR son solicitados. Esto, debido que por ningún motivo se puede dejar abierta la posibilidad que sean requeridos campos diferente de los solicitados, debido que esto ocasiona más costos a los operadores. Se sugiere que se contemplen los mismos campos que se están manejando para la etapa de diagnóstico. Se reitera que el suministro de información de los CDR no debe ser indeterminado, y por tanto, debe circunscribirse a datos específicos que sean identificados previamente para su extracción del mismo CDR. Adicionalmente, la CRC debe tener presente como funciona las diferentes redes de los PRST, para el caso de TigoUne, se hace necesario realizar modificaciones tecnológicas a nivel de centrales de conmutación, a nivel de mediación de red, para el manejo de la nueva información originada en la central, y esto tendría un impacto en los sistemas de información de la compañía. Ocasionando mayores costos por la necesidad de desarrollos tecnológicos con los proveedores de dichos elementos de red, así como la decodificación de los datos del CDR para permitir suministrar la información en los términos que establece la propuesta regulatoria.
Artículo 3	Antes de avanzar con la implementación de validaciones centralizadas para los datos, se debería realizar una nueva fase de diagnóstico por parte de la CRC similar a la que se inició en Diciembre de 2015, para identificar el estado y la efectividad del control basado en CDR de voz, si se llegará a identificar que aún existe un umbral asociado a un % de ETM ilegales en el mercado colombiano entonces se podría adoptar las correspondientes decisiones teniendo presente previamente dicho impacto. Adicionalmente, se reitera que la medida propuesta por parte de la CRC es onerosa y de poca utilidad, debido que el porcentaje de IMEIS que estaría sujeto de identificación sería ínfimo. Respecto del punto 10a.2, literal b: se indica que TigoUne no maneja en sus CDR, en lo correspondiente a llamadas originadas o llamadas terminadas los campos de LAC, y en el de CELL_ID no se cuente con el dato de final de la llamada. Tampoco se cuenta en CDR un campo

	"Mobile Station Classmark" pues éste es empleado a nivel de señalización de red para establecimiento de llamadas. Los CDR de TigoUne sólo registran llamadas contestadas o cursadas, no se registran en CDR procedimientos de señalización de las comunicaciones, en línea con la industria puesto que almacenar CDR de señalización de las comunicaciones (Voz, datos, SMS) requiere grandes sistemas de almacenamiento debido al volumen de información, resultando demasiado costoso para el operador. Sobre los puntos 10a.4 y 10a.5: Se sugiere que dicho informe cambie a periodicidad mensual, con información totalizada por mes. Del punto 10a.5: PARÁGRAFO 1: La CRC establece que la entrega de la información por parte de los PRSTM se hará conforme a las reglas y procedimientos dispuestos en la Ley 1581 del 2012. Al respecto, se precisa que en todo caso es necesario contar con la autorización del titular, y en caso de no contar con la autorización, no puede existir la obligación de compartir los datos que no sean consentidos por el Titular. PARAGRAFO 2: Los campos solicitados por la CRC deben quedar claros y definidos, no dejar abierto a la posibilidad de requerir más campos en cualquier momento, debido a los cambios y desarrollos que esto genera en el operador y sus correspondientes impactos operativos. Se sugiere continuidad con los campos referidos en la Resolución CRC 4813 de 2015. Respecto del punto 10a.5: PARAGRAFO 3: Se generará requerimientos de grandes capacidades de almacenamiento, debido que los CDR de los usuarios ya son guardados en bodegas de datos, y tener que almacenar adicionalmente esta nueva información generaría una duplicidad de información almacenada.
Artículo 4	Del punto 10b.2 literal iv: Se reitera que En TigoUne no se tiene el CDR de finalización de la llamada. En lo correspondiente a la expresión *"Con base en la distancia entre estaciones base de fin de llamada e inicio de la siguiente llamada y la diferencia de tiempo entre la hora de finalización de una llamada y la hora de inicio de la siguiente llamada, deberá determinarse si la velocidad a la cual debió desplazarse el equipo terminal móvil es lógica o es improbable dadas las condiciones de…."*, TigoUne considera que no es necesario ni oportuno calcular parámetros de velocidad de desplazamiento de cada ETM. El PRSTM tiene como funciones brindar servicio de comunicaciones a los usuarios y este tipo de cálculos físicos se relacionan con entes de **investigación forense** o con estudios con fines académicos. Se reitera que no es función del operador efectuar dicha acciones, y de hacerlo requería infraestructura de gran potencia

	que pueda procesar todos los CDR que se registran y ejecute los cálculos solicitados para cada uno de los IMEI involucrados en la comunicación. Además, se resalta tal y como se expresó anteriormente, que dicha información genera parámetros de comportamiento del usuario, y su localización, por tanto vulnera sus derechos a la privacidad, autodeterminación informática y la intimidad, garantizados en el bloque de constitucionalidad y la ley. En la expresión *"El proceso de detección debe estar en la capacidad de considerar las distancias de cobertura de los sectores de estaciones base, y demás factores que, dada la configuración de las redes, puedan generar falsas alarmas (por ejemplo: celdas adyacentes, distancias de cobertura en zonas urbanas, semiurbanas o rurales, agrupación de estaciones base por ciudad, municipio o región, etc.)",* TigoUne considera que el discernimiento de este tipo de eventos y la casuística que conlleva, es demasiado compleja, pues las redes de comunicación móvil por su naturaleza tienen implícito factores externos y no controlados que inciden sobre las condiciones de radio propagación de las señales afectando esto las condiciones para celdas adyacentes y distancias de cobertura entre otros.

8. PROPUESTAS

A continuación se desarrollan las propuestas y alternativas:

1. **VERIFICACIÓN INTRAREDES A PARTIR DE INFORMACIÓN EN REPOSITORIO CENTRALIZADO**.

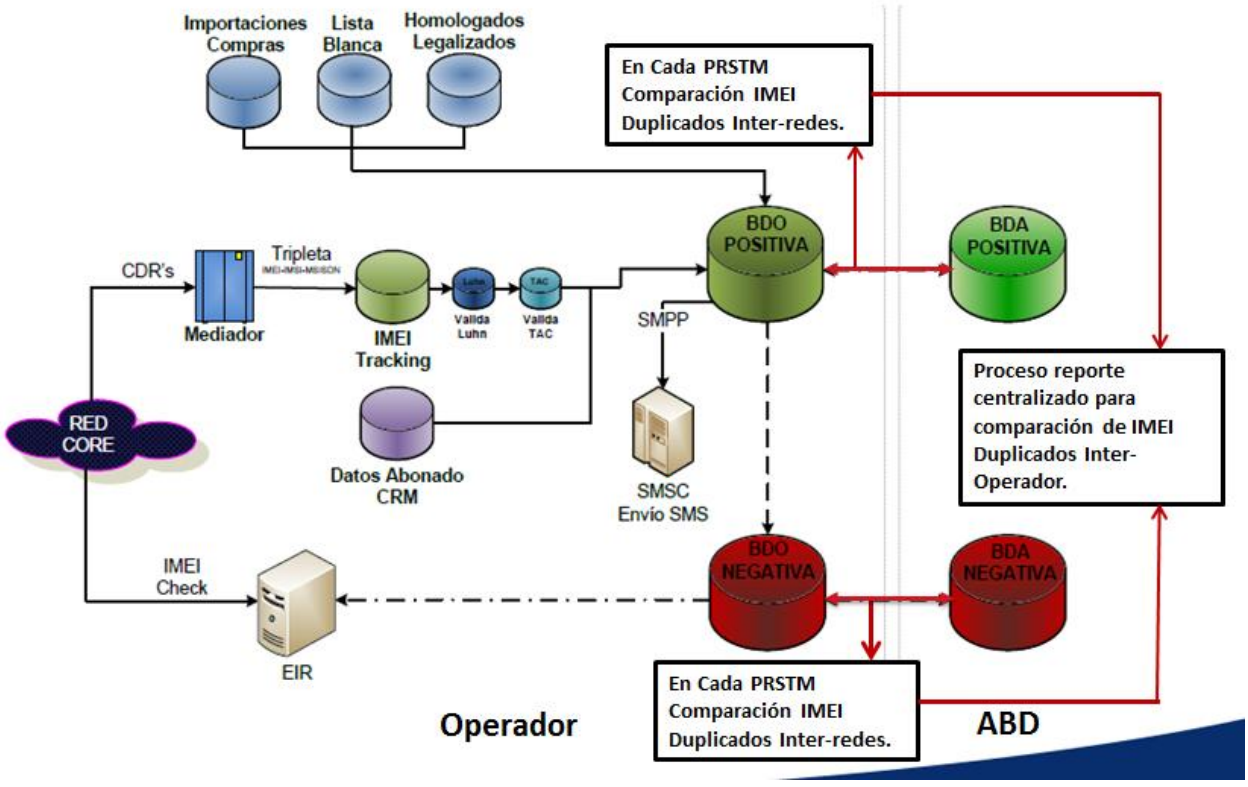
   Cada operador efectúa la identificación de IMEIS conforme con lo siguiente:

   - Cada operador tiene acceso a la BDA(+) y BDA(-) con lo cual es posible que cada PRSTM realice la comparación de sus propios IMEI obtenidos de sus CDR contra los registrados en BDO(+) y BDO(-) y estos a su vez comparados contra los IMEI de los demás operadores que existe en BDA(+/-).
   - Cuando se identifique que existen IMEI duplicados con las demás redes móviles, se podrá compartir los CDR de dicho IMEI en un directorio por operador con los eventos del día identificado [para lo cual es indispensable en todo caso definir la autorización/consentimiento del usuario, conforme con la ley].
   - Se pueden conservar los 4 campos (IMEI, IMSI, Tipo de evento, Fecha/hora del evento) y las coordenadas de Latitud y Longitud de la celda donde se identificaron los eventos asociados a dicho IMEI. Se aplica algoritmo de proximidad.
   - El repositorio centralizado del reporte debe estar en la autoridad competente (CRC, MinTIC).
   - Cada operador recoge del repositorio centralizado la información de IMEI duplicados que le han puesto otros PRSTM ahí y compara contra su propia información (4 campos + coordenadas)
   - Si el resultado de la comparación es la detección de un IMEI Duplicado se deberá enviar mínimo 2 notificaciones mensuales vía SMS al MSISDN asociado a

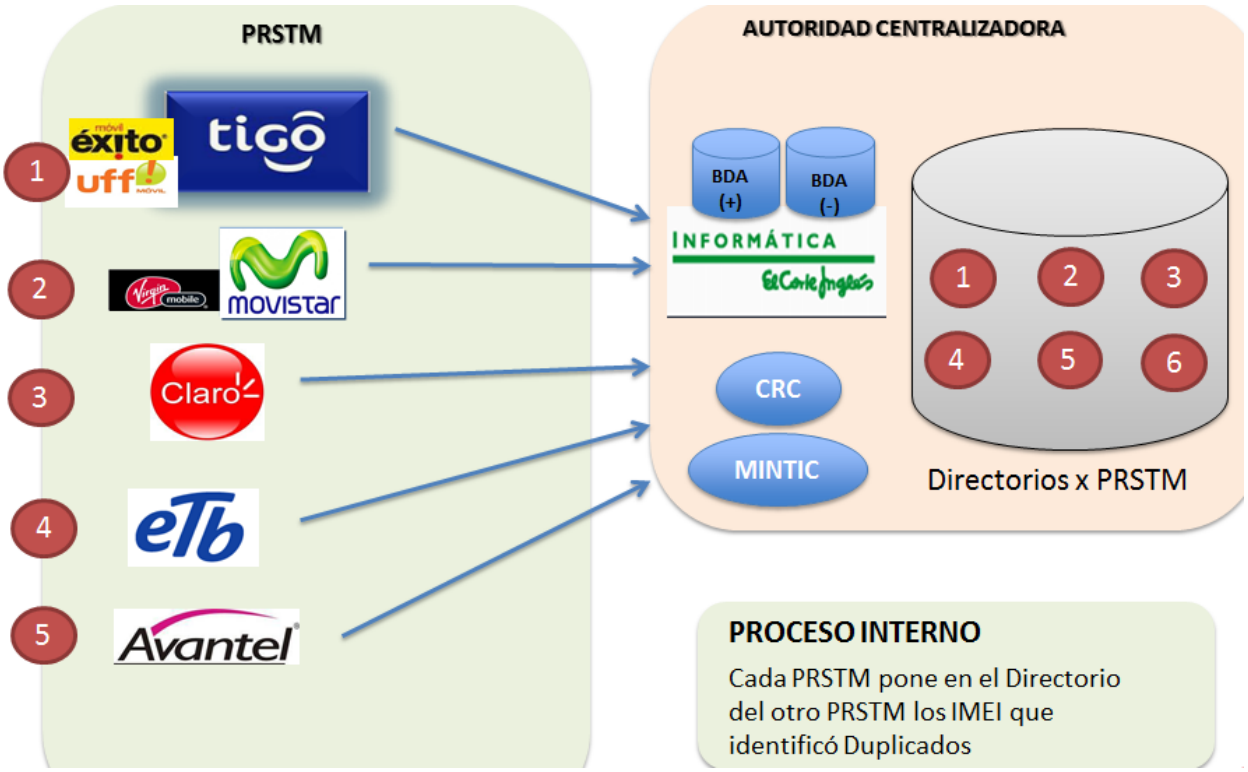
dicho IMEI por los siguientes 6 meses y al final del periodo enrutar todas sus llamadas salientes a un IVR para informar la invalidez del IMEI y solicitar al usuario el cambio del ETM. Se permitirán llamadas entrantes a la línea.

- El proceso de notificación anterior deberá ser ejecutado por los PRSTM involucrados en la duplicidad del IMEI.
- Solo podrá permanecer habilitado con servicio el IMEI que se identifique que es el original después de las validaciones físicas del equipo en el Centro de Atención al Cliente del PRSTM u oficina del OMV validando IMEI tanto en Hardware como Software y su respectiva factura de compra comprobando propiedad y legalidad del equipo (Ej.: equipo fue comprado en el mismo PRSTM).
- Finalizado el procedimiento anterior, se consolida la lista de IMEIS duplicados, y por estar en presunta comisión de delitos, se deberá establecer la obligación regulatoria de reportar dicha información a la Fiscalía General de la Nación.

A continuación el diagrama de la propuesta:



Elaboración TigoUne



Elaboración TigoUne

Como variante de la alternativa propuesta se plantea que cada PRSTM Identifica en sus CDR de tráfico los IMEI Duplicados, luego los pone en el repositorio centralizado para ser recogido y comparado por los demás PRSTM.

2. REGISTRO OBLIGATORIO DE ESTABLECIMIENTOS DEDICADOS AL MANTENIMIENTO Y VENTA DE PARTES DE ETM.

Similar a la actual obligación regulatoria de registro de personas autorizadas a la venta de equipos terminales (Res CRC 4584 de 2014), y semejante al registro de importadores y exportadores de ETM (Decreto 2025 del 2015), se debe establecer un registro de establecimientos dedicados al mantenimiento y venta de partes de ETM, con el propósito de fortalecer el control de dichos establecimientos por parte de las autoridades de policía judicial y de policía local (alcaldes e inspectores)

Los establecimientos dedicados a dichas actividades, es el único eslabón de la cadena que falta por definir condiciones regulatorias que permitan su control, esto debido que presuntamente, en dichos establecimientos se pudiere estar realizando actividades de duplicación de los IMEI a ETM hurtados.

Dicho registro, iría en línea para combatir el flagelo contra el hurto a ETM, de acuerdo con lo indicado en el documento de soporte que refiere “Dado que, de

acuerdo a las investigaciones adelantadas por la Policía Nacional, las bandas dedicadas al hurto de ETM proceden a la modificación o alteración del Identificador Internacional del Equipo Móvil (IMEI, por sus siglas en inglés) para eludir el bloqueo en las bases de datos negativas, recurriendo al uso de números de IMEI eventualmente ya asignados a otros equipos, así como de números de IMEI con estructura y formato erróneos1, se tiene como consecuencia la reventa y reintroducción al mercado de los equipos hurtados, los cuales pueden obtener servicio en las redes móviles dado que el IMEI bloqueado fue modificando evadiendo el control de la base de dato negativa".

Cordialmente,

JAIME ANDRÉS PLAZA FERNÁNDEZ
Vicepresidente de Regulación TigoUne

CC. Ingeniero
JUAN MANUEL WILCHES DURÁN
Director
Comisión de Regulación de Comunicaciones
Calle 59 A bis #5-53 Piso 9
Email: atencion.cliente@crcom.gov.co
Bogotá D.C

Doctor
SIMÓN GAVIRIA MUÑOZ
Director DNP
Calle 26 No. 13-19 Edificio FONADE
Bogotá D.C.

Doctora
PAULA ACOSTA MÁRQUEZ
Directora para la Ejecución de Gobierno y Áreas Estratégicas
Presidencia de la República
Casa de Nariño Carrera 8 N° 7 - 26
Email: paulaacosta@presidencia.gov.co
Bogotá D.C

Doctor
SEBASTIÁN GONZÁLEZ CÓRDOBA
Presidencia de la República
Casa de Nariño Carrera 8 N° 7 - 26
Email: sebastiangonzalez@presidencia.gov.co
Bogotá D.C