



**MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

RESOLUCIÓN NÚMERO 67646 DE 2021

(20 OCTUBRE 2021)

“Por la cual se impone una sanción y se imparte ordenes administrativas”

Radicación 18 - 127153

VERSIÓN PÚBLICA

**EL DIRECTOR DE INVESTIGACIÓN DE PROTECCIÓN DE
DATOS PERSONALES**

En ejercicio de sus facultades legales, en especial las conferidas por los artículos 19 y 21 de la Ley 1581 de 2012, y los numerales 5 y 9 del artículo 17 del Decreto 4886 de 2011 y

CONSIDERANDO

PRIMERO: Que la Superintendencia de Industria y Comercio (“SIC”), a través del radicado 18 - 128153 - - 00 del 24 de abril de 2018, denuncia presentada por la apoderada la sociedad comercial COLOMBIA TELECOMUNICACIONES S.A. - ESP (“TIGO”) con NIT. 830.114.921-1 presentó denuncia en contra de la sociedad comercial **COMUNICACIÓN CELULAR S.A. - COMCEL S.A.** (“CLARO”) con NIT. 800.153.993-7, por: (i) presuntas vulneraciones al régimen de protección de datos consagrado por la Ley 1581 de 2012, artículos 17 y 18; (ii) ya que el operador, aparentemente, utilizó una base de datos general de todos los operadores de telefonía celular para realizar una campaña masiva de captación de clientes sin autorización previa, previa e informada, de los clientes en particular de dicho operador. Por dichas razones, y por las que se pasan a indicar, este Despacho decidió iniciar una investigación administrativa.

1.1. TIGO, a través del radicado 18 – 127163 - - 16 del 21 de febrero 2020, amplió la denuncia en contra de CLARO, así:

“[D]el seguimiento periódico realizado por la compañía para el análisis de tráfico de usuarios, se detectó la siguiente información, la cual contiene el detalle de las 10 líneas de Claro con más llamadas hacia tigo, con un total de 1,6 millones de llamadas durante el mes de diciembre de 2018 en los cuales se contactó a 641 mil usuarios de nuestra base de datos:

	3117946526	3224382226	3106895752
Llamadas	551.601	193.517	238.458
Usuarios contactados	160.836	52.359	73.510
Usuarios Pospago	93.421	36.981	34.044
Usuarios Prepago	67.415	55.378	39.466
Portaciones Efectivas	2.985	429	783
Portaciones Pospago	2.074	273	519
Portaciones Prepago	911	156	264
Efectividad (%)	1,90%	0,50%	1,10%
Efectividad Pospago(%)	2,20%	0,70%	1,50%
Efectividad Prepago(%)	1,40%	0,30%	0,70%
Usuarios Portados después de la llamada	2.967	425	766
Días Promedio de Portación después de la llamada	5	6	7

	3213721331	3112447933	3228484426	3204479072
Llamadas	153.240	121.534	96.309	73.785
Usuarios contactados	61.688	58.918	55.848	40.338
Usuarios Pospago	30.314	26.000	22.733	20.733
Usuarios Prepago	31.374	32.918	32.915	19.605
Portaciones Efectivas	228	263	652	86
Portaciones Pospago	158	164	318	60
Portaciones Prepago	70	99	334	26
Efectividad (%)	0,43%	0,40%	1,20%	0,20%
Efectividad Pospago(%)	0,53%	0,60%	1,40%	0,30%
Efectividad Prepago(%)	0,23%	0,30%	1,00%	0,10%
Usuarios Portados después de la llamada	228	253	640	83
Días Promedio de Portación después de la llamada	6	7	6	6

	3112461776	3204428134	3114874135	Total
Llamadas	87.711	41.467	75.223	1.637.825
Usuarios contactados	34.427	32.625	30.781	641.130
Usuarios Pospago	17.253	14.019	8.623	304.121
Usuarios Prepago	17.174	18.606	22.158	337.009
Portaciones Efectivas	159	188	102	5.875
Portaciones Pospago	109	114	39	3.828
Portaciones Prepago	50	74	63	2.047
Efectividad (%)	0,50%	0,60%	0,30%	0,90%
Efectividad Pospago(%)	0,60%	0,60%	0,50%	1,30%
Efectividad Prepago(%)	0,30%	0,40%	0,30%	0,60%
Usuarios Portados después de la llamada	153	164	98	5.795
Días Promedio de Portación después de la llamada	9	13	9	8

“Por la cual se impone una sanción y se imparte órdenes administrativas”

1.2. La sociedad comercial AVANTEL S.A.S -en reorganización- (“AVANTEL”) con NIT. 830.016.046 – 1, presentó denuncia en contra de CLARO por la presunta violación del Régimen de Protección de Datos por:

- (i) *“(. . .) llamadas son originadas por los centro de atención telefónica del operador Comcel, tal como se evidencia en algunas llamadas grabadas.;*
- (ii) *(. . .) no se indica la razón por la cual esos centro de atención telefónica tienen el número de celular de las personas contactadas vía telefónica, ella en razón a que se contestan con evasivas e información no comprobable (. . .) tal como se encuentra en las grabaciones, y;*
- (iii) *(. . .) se ha detectado un aumento de las portaciones de números nativos de Avantel con destino a Comcel, la cual genera duda respecto de cómo ocurrió el contacto con los titulares de tales líneas y si se tenía la autorización previa y expresa de datos personales por parte de Comcel.”*

1.3. El señor **ANDRÉS JAVIER DÍAZ RUBIO** (el “**DENUNCIANTE**”), identificado con la cédula de ciudadanía número 80.049.766 presentó denuncia en contra de Claro por la presunta violación al Régimen de Protección de Datos con base en lo siguiente:

“Segundo: Mi línea fue adquirida en la compañía en un plan familiar y está bajo mi uso por los mismos años que llevo laborando en la Compañía.

Tercero: La primera semana de noviembre de recibí una llamada por parte del Operador de telefonía Claro (. . .) en donde se me informaba (sic) que mi línea había sido seleccionada para ofrecer sus servicios, con sorpresa pregunté de donde había sacado mi número móvil, a lo que la asesora informó que los datos habían sido proporcionados directamente por la Superintendencia de Industria y Comercio.

Razón por la cual solicito (sic) se realice la validación interna con el fin de determinar dicha más aun cuando en la página de la misma si reposan mis datos por una reclamación que interpusé en el 2014, y desconozco si es de ahí que la señalada empresa obtuvo mis datos (. . .)”

1.4. La SIC mediante radicado 18 – 1271534 - - 07 del 1 de octubre de 2018, le informó a la sociedad CLARO que realizaría, los días 2 y 3 de octubre de 2018, una visita administrativa de inspección como parte de las averiguaciones preliminares. Dentro de esta, se le requirió la remisión de registro de llamadas aleatorias, las cuales fueron aportadas al expediente a través del radicado 18 – 127153 - - 8 del 16 de octubre de 2018. Como resultado de la visita, y anexada al expediente mediante el radicado 18-127153 - - 09 del 17 de octubre de 2018, el “Acta de Diligencia de Visita de Inspección Responsable y Encargado de Bases de Datos Personales – Ley 1581 de 2012” para el radicado de la referencia, con la cual se dejó constancia de varios aspectos relativos a la protección de datos de CLARO, incluyendo bases de datos, entrevistas a diversas áreas de Claro -Departamento de Tele mercadeo, Departamento de Seguridad de la Información, Departamento de Inteligencia de los Negocios, área de fidelización-, inspección de las instalaciones de la sociedad “Plaza Claro” en la ciudad de Bogotá, preservación de diversos correos electrónicos de empleados de la sociedad, consulta de verificación para determinar si los Titulares/Clientes de TIGO había tenido llamadas provenientes de CLARO.

Así mismo, el equipo forense de la SIC, a través del radicado 18 -127153 - 21 del 12 de marzo del 2020, radicó el documento denominado “Registro de Unificación-traspaso de Evidencias Digitales”, en los cuales se radicó los documentos de cadena custodia de lo hallazgos realizados los días 2 y 3 de octubre de 2018.

1.5. La SIC Mediante radicado 18 -127153 - 24 del 19 de mayo de 2020, la Dirección de Protección de Datos Personales de la SIC, requirió a la Comisión de Regulación de Comunicación (“C.R.C”), para que diera respuesta a ciertos cuestionamientos sobre la base datos denominada “Corte Inglés”¹; respuesta que fue remitida por parte de la C.R.C. a través de los

¹ Radicado 18 – 127153 - -“(i) Informe qué bases de datos, frente a las cuales ustedes tengan la calidad de Responsable del Tratamiento, son encargadas a la sociedad o establecimiento “Corte inglés” u otra sociedad para que sean administradas por ésta como de Encargada del Tratamiento; (ii) Informe cuál es el origen Constitucional, Legal y/o reglamentario de la(s) base(s) de dato(s) administrada(s) por el Corte Inglés o quien haga de sus veces, así como cualquier base datos donde la Comisión Regulación de Comunicaciones (“C.R.C.”) funja como Responsable del Tratamiento. De igual forma, informe, de acuerdo con su origen legal, la forma en que esta(s) base(s) de dato(s) es/son alimentada(s) por parte de la C.R.C. o terceros que tienen acceso a ella(s), así como su finalidad en relación con su origen legal; (iii) Remita copia del documento u acto por medio del cual la C.R.C. encargó al “Corte Inglés”, u otras sociedades, la administración de sus bases de datos; (iv) Informe, detalladamente, qué tipos de datos

“Por la cual se impone una sanción y se imparte órdenes administrativas”

radicados 18 -127153 - - 27 del 27 de mayo de 2020 y 18 -127153 - - 30 del 1 de junio de 2020, y sobre lo que cabe destacar que la base de datos denominada “Corte Inglés” hace referencia a la base de datos positiva y negativa creada en virtud de la modificación que realizó por la Ley 1453 de 2011, artículo 105, al incorporar el tipo penal “Manipulación de equipos terminales móviles”, cuyo objetivo es la mitigación de las conductas delictivas de reprogramación, remarcación, o modificación del número de identificación de los equipos terminales móviles. Cuya finalidad, de acuerdo, con la C.R.C. Resolución 5050 de 2016, artículo 2.7.1.1.: “[L]a restricción de la operación en las redes de telecomunicaciones móviles de los equipos terminales móviles reportados como hurtados y/o extraviados, en cumplimiento de lo dispuesto en el TÍTULO 11 del Decreto 1078 de 2015 y los artículos 105 y 106 de la Ley 1453 de 2011.

Así mismo, su implementación, de acuerdo con lo Expuesto por la C.R.C., estará a cargo de un tercero, para lo cual, se eligió a la compañía “Informática El Corte Inglés – IECISA” para que fungiera como Administrador de Base de Datos (“ABD”), y cuya función principal es permitir la interconexión entre la Base de Datos Administrativa (“BDA”) y las Bases de Datos Operativas (“BDO”), de propiedad de los Proveedores de Redes y de Servicios de Telecomunicaciones (“PSRT”)², tal como CLARO. En la BDA se encuentra la siguiente información, de acuerdo con el Anexo 2.6. de la C.R.C. Resolución 5050 de 2016 -la cual fue remitida por parte de la C.R.C. como anexo a la contestación al requerimiento-, la información necesaria para la Declaración de Uso de Equipo Terminal con IMEI Duplicado, exige de los usuarios la siguiente información: (i) Nombre; (ii) Tipo de documento y número; iii Ciudad y dirección de domicilio; (iv) IMEI, marca y modelo del equipo terminal móvil; (v) Líneas telefónicas con las cuales el usuario hace uso del equipo terminal móvil (negrilla fuera del texto), y; (vi) Nombre del punto de venta, dirección y ciudad en que adquirió el equipo terminal móvil; o en su defecto nombre y datos de contacto de la persona que le proporcionó el equipo bajo cualquier título.

El uso de estas bases de datos públicas, pero de acceso restringido por parte de los PSRT, como CLARO, está condicionado a que: “(. . .) el PRSTM debe solicitar, en los términos de la Ley 1581 de 2012 y el Decreto 1377 de 2013 (o aquellas normas que los modifiquen o sustituyan), autorización por parte del usuario, con consentimiento previo, expreso e informado, a través del medio que considere idóneo, para que la información que constituya un dato personal pueda ser remitida a las autoridades competentes. Esta autorización deberá ser verificable, independientemente del medio utilizado para obtenerla.”³

- 1.6. La SIC, mediante radicado 18 -127153 - - 25 del 19 de mayo de 2020, requirió a CLARO para que diera respuestas a un cuestionario en relación al uso de las bases de datos positiva y negativa administrada por el Corte Inglés⁴; y cuya respuesta se dio por parte del CLARO a

contiene cada una de la(s) base(s) de dato(s) encargadas al Corte Inglés o la sociedad encargada. Así mismo, explique si los operadores de telefonía celular tienen acceso a esta(s), así como cualquier tercero, y las condiciones de acceso a la(s) base(s) de dato(s). Remitir copia del acto jurídico general donde se estipulen de forma expresa las condiciones de acceso por parte de los operadores de telefonía celular o cualquier tercero; En ese sentido, remitir copia de las bases de datos y aclarar si tiene algún tipo codificación o valores especiales para su acceso respectivo, y en ese caso suministrar el acceso a la codificación o valores especiales para su acceso; (v) Informe, si en las condiciones establecidas para los operadores telefonía para el acceso a la(s) base(s) de dato(s), existe alguna estipulación -expresa o tácita-, que permitan el uso de su contenido para fines de mercadotecnia, marketing o propósitos comerciales, y en ese sentido, si le es posible utilizar aplicaciones propias o de terceros para la sustracción de información con las finalidades antes descritas; (vi) Informe si a los operadores de telefonía celular se les asigna, una vez firmadas las condiciones de uso de las bases de datos (incluyendo la denominada “Corte Inglés”), usuario y clave para el acceso a las bases de datos de las cuales la C.R.C. es la encargada; (vii) Remita copia del acuerdo de uso vigente celebrado entre la C.R.C. con Claro S.A., así como aquellos vigentes para los periodos 2017 a 2019, para el acceso a las bases de datos de las cuales a C.R.C. es la Responsable del Tratamiento, incluyendo, pero sin limitarse a aquella encargada la sociedad Corte Inglés; (viii) Informe, detalladamente, sobre las medidas de seguridad que tiene implementadas el Corte Inglés, o la sociedad encargada, para el acceso la(s) base(s) de dato(s) por parte de los operadores de telefonía celular, así como cualquier tercero, y; (ix) Informar si las bases de datos de los cuales la C.R.C. es Responsable, incluyendo aquella(s) en las que el Corte Inglés está Encargada, están sujetas a cualquier tipo de auditoría para su uso adecuado por parte de los operadores de telefonía celular o cualquier tercero. En caso afirmativo, remitir copia de las auditorías realizadas desde la implementación de la(s) base(s) de datos hasta el año 2019

² D.1078/15, art. 2.2.11.5.

³ R.5050/16, Anexo 2.6. sobre “INFORMACIÓN NECESARIA PARA LA DECLARACIÓN DE USO DE EQUIPO TERMINAL MÓVIL CON IMEI DUPLICADO”

⁴ Radicado 18-127153 - - 25 del 19 de mayo de 2021: (a) De acuerdo con el acta de visita, en el área de recepción se evidenció que las labores de recepción eran realizadas por parte de la sociedad Thomas Express, cuyos empleados tenían acceso (usuario y contraseña) para ingresar a la plataforma denominada “ANDOVER” de propiedad de Claro S.A. De acuerdo con lo anterior, remitir: (i) Copia del contrato vigente para el año 2018 con la sociedad Thomas Express; (ii) Copia de los acuerdos de confidencialidad, cláusulas de confidencialidad o equivalentes para los trabajadores de la sociedad Thomas Express que tenían acceso para el año 2018 a la plataforma denominada “ANDOVER” de Claro S.A.; (iii) Copia del aviso de privacidad aplicado a los visitantes de las instalaciones de Claro S.A. en el año 2018. (b) De acuerdo con el acta de visita, en el área del sótano se evidenció que las labores de vigilancia se realizan a través de CCTV, las cuales son ejecutadas por parte de la sociedad Occidente (empresa de seguridad), y cuyos empleados tenían acceso (usuario y contraseña) para ingresar a la plataforma denominada “VIDEO EXPERT”, con el cual se administra a nivel de sede principal 120 cámaras fijas y 7 cámaras 360; y a nivel nacional se administran 880 cámara para la vigilancia de otras sedes administrativas, comerciales y técnicas. De (i) copia de dichas bases de datos; (ii) copia del aplicativo para realizar el tratamiento en cuestión junto con su código fuente y las instrucciones de funcionamiento; (b) De acuerdo con lo expresado por parte de la señora María Verónica Trujillo, la entonces gerente de inteligencia de negocios, la lista de número para afiliación de terceros no clientes de Claro S.A. se forma aleatoriamente de los prefijos de numeración pública, la cual es comparada con el listado arrojado por parte del Corte Inglés. De acuerdo con lo anterior, por favor explicar de forma detallada el procedimiento por medio del cual se hace la comparación del listado aleatorio con la lista del Corte Inglés. (c) De acuerdo con lo expresado por parte del señor Germán Lopera, el entonces gerente de desarrollo facturación, Claro S.A. desarrolló un aplicativo para gestionar el proceso de portabilidad llamado Portanode que descarga las bases de datos del ABD (Corte Inglés) a través del uso de VPN y las credenciales asignadas por parte de la Comisión de Regulación de Comunicación. De acuerdo con lo anterior, remitir: (i) copia del programa denominado Portanode junto con su código fuente e instrucciones de uso; (ii) copia del acuerdo o condiciones de uso remitidas por parte de la C.R.C. o quien haga de sus veces, para la utilización del usuario y clave de acceso a la base de datos del Corte Inglés. (d) De acuerdo con el acta de visita, en el área de recepción se evidenció que las labores de recepción eran realizadas por parte de la sociedad Thomas Express, cuyos empleados tenían acceso (usuario y contraseña) para ingresar a la plataforma denominada “ANDOVER” de propiedad de Claro S.A. De acuerdo con lo anterior, remitir: (i) Copia del contrato vigente para el año 2018 con la sociedad Thomas Express; (ii) Copia de los acuerdos de confidencialidad, cláusulas de confidencialidad o equivalentes para los trabajadores de la sociedad Thomas Express que tenían acceso para el año 2018 a la plataforma denominada “ANDOVER” de Claro S.A.; (iii) Copia del aviso de privacidad aplicado a los visitantes de las instalaciones de Claro S.A. en el año 2018. (e) De acuerdo con el acta de visita, en el área del sótano se evidenció que las labores de vigilancia se realizan a través de CCTV, las cuales son ejecutadas por parte de la sociedad Occidente (empresa de seguridad), y cuyos empleados tenían acceso (usuario y contraseña)

“Por la cual se impone una sanción y se imparte órdenes administrativas”

través del radicado 18 -127153 - - 31 del 4 de junio de 2020, donde remitió la siguiente información a destacar: (i) Flujograma de proceso de generación de migración de prepago a post-pago, y ; (iii) Flujograma de proceso de generación de listados para portación, de los cuales se evidenció: (ii) el uso, para efectos de la formación a la lista de clientes no CLARO, el RESPONSABLE indicó el procedimiento de recolección se realiza a través de diversos pasos, entre ellos el *“Cruce de información de clientes portados del Corte Inglés para identificar clientes que se portaron a otra empresa”*, y; (ii) la remisión del aplicativo PORTANODE, especificaron que no fue desarrollado por CLARO, sino una herramienta que sirve de *“Gateway”* entre el ABD y los sistemas internos de CLARO, por lo que solo sirve para comunicarse entre el Punto A (ABD o la compañía española *“Informática El Corte Inglés – IECISA”*) y el Punto B (CLARO) en referencia a la portabilidad numérica.

SEGUNDO: Que, con base en los hechos anotados, a partir de los cuales se advierte la presunta violación de las normas sobre protección de datos personales, y en particular las disposiciones contenidas en la Ley 1581 de 2012 y el Decreto 1377 de 2013 -incorporado al Decreto Único Reglamentario 1574 de 2015-, se profirió la Resolución 35890 del 7 de julio de 2020, por medio de la cual se formularon los siguientes cargos a la parte investigada con el fin de que se pronunciara sobre los hechos materia de investigación y aportara las pruebas que pretendiera hacer valer dentro del referido trámite:

- **“CARGO PRIMERO:** *La presunta vulneración, en su calidad de Responsable, del principio de finalidad (L.1581/12, art. 4(b)) y el deber de informar de forma debida sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada (L.1581/12, art. 17(c)).*
- **CARGO SEGUNDO:** *La presunta vulneración, en su calidad de Responsable del principio de libertad (L.1581/12, art. 4(c)) y el deber de solicitar y conservar copia de la respectiva autorización otorgada por el Titular en los términos establecidos por la ley ((L.1581/12, arts. 9 y 17(b), D.1377/13, arts. 5, 7, y 8 -incorporado en el D.1074/15-).”*

TERCERO: Que la investigada, mediante radicado 18 – 127153 - - 38 del 8 de julio de 2020, se realizó la notificación personal de la Resolución 35890 del 7 de julio de 2020, teniendo la Investigada un término de quince (15) días hábiles, una vez se surtiera la notificación personal, para presentar los respectivos Descargos. Sin embargo, debido a que la sociedad investigada no se presentó, se procedió, a través del radicado 18 -127153 - - 44 del 16 de julio de 2020, a realizar la notificación por aviso del Acto Administrativo de conformidad con lo establecido por el artículo 69 del Código de Procedimiento Administrativo y de la Contencioso Administrativo (*“C.P.A.C.A.”*). Este plazo, de acuerdo con el radicado 18 – 127153 - - 45 del 17 de julio de 2020, inició el 22 de julio de 2020 y finalizó el 12 de agosto de 2020. La Investigada, a través de los radicados 18 – 127153 - - 56 al 102 del 12 de agosto de 2020, presento Descargos en término.

- 3.1. Teniendo en cuenta la denuncia presentada por el [REDACTED], de conformidad con lo establecido por el artículo sexto Resolución 35890 del 7 de julio de 2020, en concordancia con el artículo 38 (1) del C.P.A.C.A., a través del radicado 18 -127153 - - 36 del 8 de julio de 2020, se le comunicó el contenido de la resolución de imputación de cargos con el fin de que se presentara como tercero interesado e hiciera valer sus derechos. Sin que se haya presentado a la investigación como tercero interesado.
- 3.2. Teniendo en cuenta la denuncia presentada por la sociedad comercial AVANTEL S.A.S -en reorganización- con NIT. 830.016.046 – 1, de conformidad con lo establecido por el artículo sexto Resolución 35890 del 7 de julio de 2020, en concordancia con el artículo 38 (1) del C.P.A.C.A., a través del radicado 18 -127153 - - 37 del 8 de julio de 2020, se le comunicó el contenido de la resolución de imputación de cargos con el fin de que se presentara como tercero interesado e hiciera valer sus derechos. De esta manera, esta sociedad, a través del radicado 18-127153- - 48 del 28 de julio de 2020, solicitó la integración como tercero

para ingresar a la plataforma denominada *“VIDEO EXPERT”*, con el cual se administra a nivel de sede principal 120 cámaras fijas y 7 cámaras 360; y a nivel nacional se administran 880 cámara para la vigilancia de otras sedes administrativas, comerciales y técnicas. De acuerdo con lo anterior, remitir: (i) Copia del contrato vigente para el año 2018 con la sociedad Occidente; (ii) Copia de los acuerdos de confidencialidad, cláusulas de confidencialidad o equivalentes para los trabajadores de la sociedad Occidente que tenían acceso para el año 2018 a la plataforma denominada *“VIDEO EXPERT”* que administra la seguridad CCTV de Claro S.A.; (iii) Copia de los avisos de seguridad distribuidos en la sede principal de Claro S.A., así como de aquellos distribuidos en las distintas sedes administrativas, comerciales y técnicas de Claro S.A. en Colombia sobre los cuales ejerzan la vigilancia desde la ciudad de Bogotá D.C. a través de la plataforma denominada *“VIDEO EXPERT”*. (f) Remita copia de la Política de tratamiento de datos vigente para el año 2018, así como copia del aviso de privacidad utilizado en el año 2018 para cada una de las operaciones donde Claro S.A. realizó tratamiento de datos privados.”

interesado dentro de la investigación, lo cual fue aceptado por parte de la SIC a través del radicado 18 – 127153 - - 51 del 31 de julio de 2020, al cumplir con los requisitos establecidos por el artículo 38 del C.P.A.C.A., dándosele un plazo de quince (15) días hábiles siguientes para solicitara y/o aportara las pruebas que pretendiera hacer valer, lo cual ocurrió a través del radicado 18 -127153 - - 103 del 25 de agosto de 2020.

- 3.3. Teniendo en cuenta la denuncia presentada por parte de la sociedad comercial COLOMBIA TELECOMUNICACIONES S.A. - ESP con NIT. 830.114.921-1, de conformidad con lo establecido por el artículo sexto Resolución 35890 del 7 de julio de 2020, en concordancia con el artículo 38 (1) del C.P.A.C.A., a través del radicado 18 -127153 - - 39 del 8 de julio de 2020, se le comunicó el contenido de la resolución de imputación de cargos con el fin de que se presentara como tercero interesado e hiciera valer sus derechos. De esta manera, esta sociedad, a través del radicado número 18 – 127153 - - 49 del 30 julio de 2020, solicitó la integración como tercero interesado dentro de la investigación, lo cual fue aceptado por parte de la SIC a través del radicado 18 – 127153 - - 104 del 16 de septiembre de 2020, al cumplir con los requisitos establecidos por el artículo 38 del C.P.A.C.A.

CUARTO: Que, mediante la Resolución 64874 del 15 de octubre de 2020, mediante la cual se incorporaron pruebas dentro de una investigación, se rechazan unas y se decretan otras, este Despacho determinó que cuenta con todos los elementos de juicio necesarias para decidir dentro la presente investigación, razón por la cual decidió los siguiente: (i) integrar pruebas; (ii) abrir etapa probatoria; (iii) decretar ciertas pruebas, y; (iv) negar otras. Siendo las pruebas integradas, negadas y decretadas a la actuación administrativa las siguientes:

4.1. Pruebas Recaudadas por la Dirección de Protección de Datos.

4.1.1. Los documentos aportados a través de la Denuncia con radicado número 18 – 12715 - 00 del 24 de abril de 2018 y radicado número 18 – 127153 - 16 del 21 de febrero de 2020, los cuales son los siguientes, a saber:

- (a) Copia del certificado de existencia y representación de la sociedad TIGO, donde se constata que [REDACTED] está en capacidad de representar a TIGO;
- (b) Copia de la queja presentada ante TIGO por [REDACTED];
- (c) Copia de la queja presentada ante TIGO por [REDACTED];
- (d) Copia de la queja presentada ante TIGO por [REDACTED];
- (e) Copia de la denuncia presentada ante TIGO por [REDACTED];
- (f) Documento de muestreo de las llamadas recibidas por los usuarios durante el primer trimestre del año 2018, donde se evidenció llamadas provenientes de números de prefijo de CLARO [REDACTED].

4.1.2. Los documentos aportados a través del radicado número 18 – 225775 – 00, acumulado a la presente actuación, los cuales son los siguientes, a saber:

- (a) CD con 13 grabaciones de llamadas de clientes;
- (b) CD con archivos PDF donde se certifica los números de AVANTEL portados a CLARO.

4.1.3. Radicado número 18-127153 - -07 del 1 de octubre de 2018, mediante el cual se le informó a CLARO que la Superintendencia de Industria y Comercio (“SIC”) realizaría, los días 2 y 3 de octubre de 2018, una visita administrativa de inspección como parte de las averiguaciones preliminares.

4.1.4. Radicado número 18-127153 - 08 del 16 de octubre de 2018, mediante el cual CLARO remitió la siguiente información como parte de solicitudes realizadas por la SIC en la visita administrativa realizada por la SIC los días 2 y 3 de octubre de 2018, a saber:

- (a) CD de grabaciones de 68 llamadas aleatorias realizadas entre el 19 y 23 de septiembre de 2018;
- (b) Copia de los registros de log correspondientes a los meses de febrero, marzo y abril de 2018;
- (c) Copia de los contratos celebrados con los call-center con nombre 127, logitec y Atento, y;
- (d) Copia de la licencia del aplicativo de monitoreo.

4.1.5. Radicado número 18-127153 - - 09 del 17 de octubre de 2018 mediante el cual se anexo al expediente el "Acta de Diligencia de Visita de Inspección Responsable y Encargado de Bases de Datos Personales – Ley 1581 de 2012".

4.1.6. Radicado número 18 -127153 - - 11 del 31 de octubre de 2018, se allegaron los siguientes documentos al expediente, a saber:

- (a) Copia de la queja presentada ante TIGO por parte del [REDACTED];
- (b) Audio de queja presentada por [REDACTED] donde indica que CLARO se comunicó con la Titular indicando su tiempo de afiliación, características del servicio y beneficios por cambiarse de operador;
- (c) Documento de muestreo de las llamadas recibidas por los usuarios en agosto de 2018.

4.1.7. Radicados número 18 -127153 - - 12 al 13 del 22 de noviembre de 2018, se radicó reiteradas veces los siguientes documentos:

- (a) Copia del audio de grabación donde una asesora comercial de CLARO se comunicó con [REDACTED], cliente de TIGO, ofreciendo sus servicios;

4.1.8. Radicado número 18 -127153 - - 15 del 27 de noviembre de 2018, se radicó los siguientes documentos:

- (a) Copia del correo enviado a TIGO por parte de [REDACTED] el día 18 de septiembre de 2018;
- (b) Copia de la comunicación enviada a TIGO por parte del [REDACTED] con fecha del 28 de septiembre de 2018;
- (c) Copia de la llamada hecha a TIGO por parte de la [REDACTED] manifestando su inconformidad con respecto al ofrecimiento hecho por CLARO;
- (d) Archivo Excel con detalle de las llamadas realizada por parte de CLARO a usuario de TIGO que posteriormente solicitaron portabilidad numérica.

4.1.9. Radicado número 18 -127153 - - 16 del 27 de noviembre de 2018, se radicó los siguientes documentos:

- (a) Copia de la queja presentada ante TIGO por parte [REDACTED], con cédula de extranjería 405.158;
- (b) Copia de la queja presentada ante TIGO por parte [REDACTED]

(c) Copia de la queja presentada ante TIGO por parte de [REDACTED];

(d) Copia de la queja presentada ante TIGO por parte de [REDACTED];

4.1.10. Mediante radicado número 18 -127153 - - 19 del 21 de octubre de 2019, se radicó los siguientes documentos:

(a) Copia de la queja presentada ante TIGO por parte de [REDACTED];

[REDACTED] Copia de la queja presentada ante TIGO por parte de [REDACTED];

(c) Copia del audio de llamada realizada por parte de una asesora comercial de CLARO al señor Carlos Andrés Téllez Ramírez (duración 6:04 minutos)

4.1.11. Radicado número 18 -127153 - - 21 del 12 de marzo del 2020, mediante el cual el se allegó el documento denominado "Registro de Unificación-traspaso de Evidencias Digitales, en los cuales se radicó los documentos de cadena custodia de lo hallazgos realizados los días 2 y 3 de octubre de 2018;

4.1.12. Radicado número 18 -12715 - - 22 del 30 de abril de 2020, la Dirección de Protección de Datos Personales de la SIC requirió a TIGO para respondiera unos cuestionamientos y remitiera información;

4.1.13. Radicado número 18 -127153 - - 23 del 19 de mayo de 2020, mediante el cual TIGO allegó, en razón del requerimiento con radicado 18 -127153 - - 22 del 30 de abril de 2020, la siguiente documentación:

(a) Archivo Excel con nombre completo, número de cédula, dirección de domicilio de los denunciantes, en los casos en que se contó con registro de teléfono fijo o dirección de correo electrónico se incluye la información;

(b) Archivo Excel con Información de los planes de voz y datos suscritos por los denunciantes cuya información se aporta en el numeral anterior.

4.1.14 Radicado número 18 -127153 - - 24 del 19 de mayo de 2020, mediante el cual la Dirección de Protección de Datos Personales de la SIC, requirió a la Comisión de Regulación de Comunicación ("C.R.C") para que diera respuesta a un requerimiento de información en relación con la finalidad de las bases de datos a que hace alusión los TIGO y AVANTEL en sus denuncias;

4.1.15. Radicados número 18 -127153 - - 27 del 27 de mayo de 2020 y 18 -127153 - 30 del 1 de junio de 2020, mediante los cuales la C.R.C. dio respuesta al requerimiento con radicado número 18 -127153 - 24 del 19 de mayo de 2020;

4.1.16. Radicado número 18 -127153 - 25 del 19 de mayo de 2020, mediante el cual la Dirección de Protección de Datos Personales de la SIC requirió a CLARO para que respondiera un cuestionario sobre los hallazgos de la visita de inspección administrativa del 2 y 3 de octubre de 2018;

4.1.17. Radicados número 18 -127153--31, 18 -127153 - - 32, 18 -127153 - - 33, y 18 -127153 - - 34 del 4 de junio de 2020, CLARO dio contestación al requerimiento realizado por la SIC a través del Radicado número 18 -127153 - 25 del 19 de mayo de 2020, anexando la siguiente documentación, a saber:

(a) Certificado de Existencia y representación de CLARO;

(b) Flujograma de proceso de generación de migración de prepago a post-pago;

- (c) Flujograma de proceso de generación de listados para portación;
- (d) Copia del contrato vigente para el año 2018 con la sociedad Thomas Express, copia de los acuerdos de confidencialidad, cláusulas de confidencialidad o equivalentes para empleados de la sociedad Thomas Express que tenían acceso para el año 2018 a la plataforma denominada “ANDOVER” de CLARO S.A, y copia de aviso de privacidad aplicado a los visitantes de la Claro S.A. en el año 2018;
- (e) Copia del Contrato vigente para el año 2018 con la sociedad Occidente, copia de los acuerdos de confidencialidad, cláusulas de confidencialidad o equivalentes para los trabajadores de sociedad Occidente que tenían acceso para el año 2018 a la plataforma denominada “VIDEO EXPERT” que administraba la seguridad CCTV de Claro S.A., copia de los avisos de seguridad distribuidos en las distintas sedes administrativas, comerciales y técnicas de CLARO S.A. en Colombia sobre los cuales ejerzan la vigilancia desde la ciudad de Bogotá D.C. a través de la plataforma denominada “VIDEO EXPERT”, y;
- (f) Copia de la Política de Tratamiento de datos vigentes para el año 2018, así como copia del aviso de privacidad utilizado en el año 2018 para cada una de las operaciones donde CLARO S.A. realizó tratamiento de datos privados.

4.1.18. Radicado número 18 -127153 - - 26 del 18 de mayo de 2020, mediante el cual TIGO radicó un oficio donde indicó que de los archivos CDR-3106085557, CDR-3232554006; CDR-3117946525_1; CDR-3117946525_2, y; CDR-3123425355, de los cuales se puede observar como presuntamente CLARO realizó cientos de llamadas en la misma fecha originadas desde el mismo número telefónico de dicho operador, y entre los que se encuentran los usuarios de TIGO denunciantes.

4.1.19. Radicado número 18 – 225775 - - 00 del 7 de septiembre de 2018, acumulado al radicado de la referencia, AVANTEL allegó un CD que contiene la siguiente información a saber:

- (a) CD con copia de 13 grabaciones realizadas a usuarios de AVANTEL;
- (b) Lista de usuarios de AVANTEL migrados a CLARO debido a las llamadas recibidas.

4.2. Pruebas presentadas en conjunto con el escrito de Descargos presentado por CLARO

4.2.1. Anexo 2. Garantía procesal, la cual no se integra al expediente dado que no es impertinente, ya que conduce a probar o controvertir hechos de los alegados en el procedimiento administrativo y en los Descargos relacionados directamente con hechos objeto de debate;

4.2.2. Anexo 3. Comunicado Corte Inglés, el cual será integrado al expediente con el fin de determinar el funcionamiento de las bases de datos positiva y negativa, así como la base de datos de portabilidad numérica;

4.2.3. Anexo 4. Diagrama técnico de las bases de datos de portabilidad, el cual será integrado al expediente con el fin de determinar el funcionamiento de la base de datos de portabilidad numérica;

4.2.4. Anexo 5. Llamadas de contacto de tele mercadeo, la cuales serán integradas al expediente toda vez que pueden ser conducentes a probar los hechos los alegados en el procedimiento administrativo y en los Descargos;

4.2.5. Estados Financieros de los últimos (3) años, los cuales serán incorporados para tenerse en cuenta como criterio para la fijación de la respectiva multa en caso de que así se establezca.

4.2.6. Testimonio de [REDACTED] en calidad de Coordinadora de Relacionamiento de Agentes de la C.R.C., quien dio respuesta al requerimiento solicitado por la SIC, para que: (i) informe los roles normativos de la sociedad informática El Corte Inglés en calidad de ADB del proceso de portabilidad número y de ADB en el proceso de control y detección de IMEIS de equipos terminales;

“Por la cual se impone una sanción y se imparte órdenes administrativas”

- 4.2.7. Testimonio de [REDACTED], en calidad de Gerente de Proyectos PMP de la División de Ingeniería y Analítica de la sociedad Informática El Corte Inglés, Sucursal Colombia, para que: (i) Rinda testimonio sobre el funcionamiento técnico y regulatorio de cada uno de los procesos, sus diferencias y las interacciones con cada uno de los procesos, sus diferencias y las interacciones de estos con la herramienta PortaNode.
- 4.2.8. Testimonio de [REDACTED], en calidad de Gerente de Desarrollo de Comcel, quien lideró la implementación de PortaNode en la compañía, quien rendirá testimonio sobre: (i) el objetivo de la herramienta y sus interacciones a nivel técnico y reglamentario con las bases de datos administradas por El Corte Inglés; testimonio no será decretado, dado que el objeto de controversia no es la implementación de la plataforma PortaNode ni el marco normativo de implementación, sino la finalidad de los datos recolectados a través de ella y la posible destinación para otros fines no relacionados con su finalidad. Por tanto, de conformidad con lo establecido en el C.G.P, art. 168, es rechazado de plano.
- 4.2.9. Testimonio de [REDACTED], en calidad de Gerente de Desarrollo de Comcel, quien lideró la implementación de PortaNode en la compañía, y rendirá testimonio sobre: (i) El objetivo de la herramienta y sus interacciones a nivel técnico y reglamentario con las bases de datos administradas por el Corte inglés;
- 4.2.10. [REDACTED], Gerente de Seguridad Información y Protección Tecnológica, quien rendirá testimonio sobre la actividad de control y detección de IMEIS de equipos terminales, las bases de datos involucradas y su interacción con otras bases de datos o herramientas de la compañía CLARO;
- 4.2.11. Solicitó oficiar a la Coordinadora de Relacionamiento con Agentes de la C.R.C. para: (i) Aclarar la respuesta dada al requerimiento de la SIC, a través de las siguientes preguntas:
- *“¿Qué es el Corte Inglés: ¿Descripción de la Naturaleza jurídica y Objetivo? (Aclarar que actúa en calidad de ABD para el contrato de portación con todos los operadores y de ABD para la actividad y control de IMEIS de equipos terminales)*
 - *¿Qué bases de datos existen en los procesos de portabilidad? (Explicación técnica y regulatoria)*
 - *¿Qué es el ABD, qué hace, en virtud de qué disposiciones, cuales son sus alcances y roles?*
 - *Cualquier otra explicación y/o aporte relevante de cara al contexto.”*

4.3. Solicitud de pruebas por parte de AVANTEL

- 4.3.1. Las aportadas por AVANTEL mediante radicado 18-225775 - - 00 de 7 de septiembre de 2018, consistentes en un CD contentivo de la siguiente información: CD con copia de 13 grabaciones realizadas a usuarios de AVANTEL; Lista de usuarios de AVANTEL que se presumen migrados a COMCEL debido a las llamadas realizadas.
- 4.3.2. Oficiar a CLARO con el fin de que alleguen al expediente Flujogramas de los procesos asociados a las bases de datos positiva y negativa de que trata la Resolución CRC 3128/11 (compilada en la R. CRC 5050/16);
- 4.3.3. Oficiar a la C.R.C. y a la Dirección de Investigaciones de Protección de Usuarios de Servicios de Comunicaciones de la Superintendencia de Industria y Comercio, para que informen a su Despacho si han recibido quejas de consumidores y/o usuarios, relacionados con la presente actuación administrativa, cualquier tipo de información y/o documentación en formato físico o electrónica que se encuentre en su poder y resulte pertinente, conducente e idónea para el esclarecimientos de los hechos objeto de la denuncia.

4.4. Pruebas solicitadas por la investigada y los terceros interesados

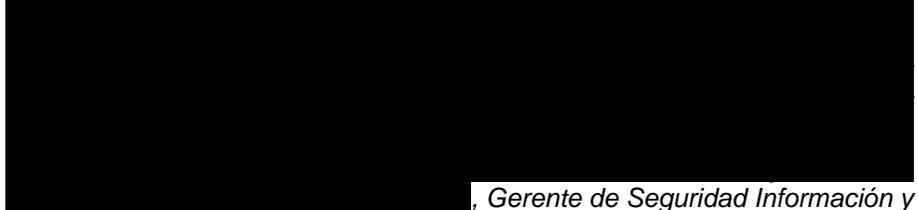
4.4.1. Pruebas solicitadas por parte de la Investigada.

De acuerdo con la Resolución 64874 del 15 de octubre de 2020, en relación con las pruebas solicitadas por parte de la Investigada, se decidió lo siguiente:

“Por la cual se impone una sanción y se imparte órdenes administrativas”

“ Las pruebas aportadas en los Descargos y relacionadas en la presente en los numerales 5.2.1. a 5.2.5 serán integradas al expediente como pruebas documentales, y serán analizadas de acuerdo con lo establecido en los artículos 176, 243 a 274 del C.G.P.”⁵

“(. . .) en relación con las pruebas testimoniales solicitadas por parte de la Investigada, es decir, los testimonios de los



, Gerente de Seguridad Información y Protección Tecnológica (. . .) la Dirección considera que las pruebas testimoniales solicitadas no son medio de prueba que permita demostrar que la Investigada, Claro, en calidad de Responsable del Tratamiento, dio cumplimiento al principio de finalidad y el deber de informar la finalidad de la recolección y los derechos que le asisten a los Titulares, así como tampoco que realizó la solicitud de autorización previa y conservar copia de la misma, en los términos expuestos en la Resolución 35890 del 7 de julio de 2020.”⁶

4.4.2. Pruebas solicitadas por parte el tercero interesado AVANTEL.

De acuerdo con la Resolución 64874 del 15 de octubre de 2020, con relación a las pruebas solicitadas por parte de AVANTEL como tercero interesado, se decidió lo siguiente:

“Las pruebas aportadas por AVANTEL en el documento de solicitud reconocimiento de tercero interesado, y relacionadas en la presente en el numeral 5.3.1., serán integradas al expediente como pruebas documentales, y serán analizadas de acuerdo con lo establecido en los artículos 176, 243 a 274 del C.G.P.”

“(. . .) en relación a la solicitud de oficiar a CLARO para que remita flujogramas asociados a las bases de datos positiva y negativa de que trata la Resolución CRC 3128/11 (compilada en la R. CRC 5050/16), existen dentro del expediente medios de prueba que establecen con claridad el funcionamiento de esta base de datos. Para el efecto es necesario revisar la respuesta dada por la C.R.C. previo requerimiento de la SIC, así como la respuesta dada por CLARO en relación con su interacción dicha base de datos, a lo cual debe incluirse el flujograma aportado en el documento Descargos. Por tal motivo, el Despacho considera que de acuerdo con el artículo 168 del C.G.P., la prueba resulta inútil, ya que solicitarle solo resultaría reiterativo, por lo que debe ser rechazada de plano.”⁷

“(. . .) en relación a la solicitud la C.R.C. y a la Dirección de Investigaciones de Protección de Usuarios de Servicios de Comunicaciones de la Superintendencia de Industria y Comercio para que estos informen si han recibido quejas de consumidores y/o usuarios, relacionados con la presente actuación administrativa, resulta pertinente indicar que, dentro del expediente, específicamente aquellas indicadas en la presente en 5.1.1., 5.1.2., 5.1.4., 5.1.6., 5.1.7., 5.1.8., 5.1.9. 5.1.10, 5.1.18 y 5.1.19 son indicativas de la presunta actuación de CLARO en relación a las llamadas a que hace mención el solicitante; razón por la cual su decreto resultaría impertinente toda vez que existen otros medios de prueba que permite probar el hecho alegado. Por tal motivo, de acuerdo con el artículo 168 del C.G.P., será rechazada de plano.”⁸

4.5. Pruebas decretas de oficio por parte del Despacho

De acuerdo con el considerando sexto de la Resolución 64874 del 15 de octubre de 2020, el Despacho Decretó las siguientes pruebas de oficio:

4.5.1. Requerir a la COMISIÓN DE REGULACIÓN DE COMUNICACIONES (“C.R.C”) con el fin de que indique:

- (a) Informe, de forma clara y precisa, cual es el origen normativo de la base de datos de portabilidad numérica. Lo anterior especificando la siguiente información: (i) finalidad;

⁵ R. 64874/20, p. 8.

⁶ R. 64874/20, p. 8 – 9.

⁷ R. 64874/20, p. 9.

⁸ R. 64874/20, p. 9.

“Por la cual se impone una sanción y se imparte órdenes administrativas”

(ii) forma de alimentación; y (iii) rol que desempeñan los operadores de telefonía celular y la empresa Corte Inglés de cara al uso de la base de datos de portabilidad numérica.

Para el efecto, y en cumplimiento de lo ordenado por la Resolución 64874 del 15 de octubre de 2020, a través del radicado 18 – 127153 - - 120 del 11 de noviembre de 2020, requirió la C.R.C. para que le diera respuesta al cuestionario, y al cual se le dio respuesta por parte de la C.R.C. a través de los radicados 18-127153 - - 121 a 123 del 23 y 24 de noviembre de 2020. En el radicado anteriormente indicado la C.R.C., expuso lo siguiente:

“(i) Marco legal y regulatorio de la Portabilidad Numérica en Colombia

Mediante la Ley 1245 de 2008 se estableció la obligación de la implementación de la portabilidad numérica en Colombia en los siguientes términos:

“Artículo 1°. Portabilidad numérica. Los operadores de telecomunicaciones que tengan derecho a asignación directa de numeración se obligan a prestar el servicio de portabilidad numérica, entendida esta como la posibilidad del usuario de conservar su número telefónico sin deterioro de la calidad y confiabilidad, en el evento de que cambie de operador, de conformidad con los requerimientos prescritos por la Comisión de Regulación de Telecomunicaciones (...)” SFT

Dado que los operadores del servicio de telefonía móvil, por la naturaleza de este servicio, tienen derecho a la asignación directa de numeración no geográfica, la obligación de prestación del servicio de portabilidad numérica recae directamente sobre ellos.

En todo caso, en la mencionada Ley se encomendó a la CRC establecer las condiciones para la implementación y operación de la portabilidad numérica, lo cual se materializó con la expedición de la Resolución CRC 2355 de 2010, actualmente compilada en el Capítulo 6 del Título II de la Resolución CRC 5050 de 2016. De esta manera y el concurso de los operadores móviles, desde el 29 de julio de 2011 los usuarios de telefonía móvil puedan portar su número cuando cambian de proveedor.

En este punto, es importante precisar que la portabilidad numérica es una herramienta regulatoria que facilita a los usuarios el ejercicio de su derecho a la libre elección de operador y de planes tarifarios, puesto que reduce o elimina los costos que podría enfrentar el usuario al tener que cambiar también de número telefónico cuando se desvincula de un operador e inicia un nuevo contrato con otro.

(ii) Condiciones regulatorias de la implementación y operación de la base de datos de portabilidad numérica

Un recurso fundamental en la provisión del servicio de telefonía es la numeración, puesto que con ella se identifican las líneas telefónicas, se determina el enrutamiento que se debe hacer al interior de la red de telefonía para establecer una comunicación y se desarrollan diferentes procesos propios del servicio. Dicho recurso de numeración es administrado por la CRC, quien lo asigna a los operadores móviles y estos a su vez a los usuarios.

Para establecer una comunicación entre un número telefónico A y un número telefónico B, al interior de la red de telefonía previamente se programa el enrutamiento que debe seguir la llamada para establecer la comunicación. En principio si la llamada es entre dos números que fueron asignados al mismo operador, la ruta de la llamada que se programa es al interior de la red de ese operador, pero si la llamada es entre dos números asignados a diferentes operadores, la ruta que se programa es la entrega de la llamada, por parte del operador que tiene asignado el número de donde se origina esta, al operador que tiene asignado el número de destino.

En ambiente de portabilidad numérica, la condición para el enrutamiento de las llamadas cambia, puesto que ahora hay números telefónicos que no están en la misma red del operador que es signatario de ellos, dado que se han portado a la red otro operador y por tanto la programación del enrutamiento de las llamadas se vuelve dinámico.

Debido a lo anterior, uno de los aspectos técnicos que se debieron resolver para la implementación de la portabilidad numérica móvil fue la manera en que se debían enrutar las llamadas. Para ello en su oportunidad se revisaron las diferentes soluciones disponibles en el mercado y se determinó que en

“Por la cual se impone una sanción y se imparte órdenes administrativas”

el largo plazo el esquema más eficiente y que representaba mayores beneficios correspondía al denominado “All Call Query –ACQ”, el cual implica, entre otros aspectos, la implementación y operación de una base de datos de números portados, la cual debe ser consultada por los operadores móviles previamente antes de enrutar cada llamada:

Es así como, en el artículo 10 de la Resolución CRC 2355 de 2010 (compilado en el artículo 2.6.3.1. de la Resolución CRC 5050 de 2016) se estableció que la implementación de la Portabilidad Numérica debía ser adelantada por los Proveedores de Redes y Servicios de Telecomunicaciones (en adelante PRST) mediante el esquema All Call Query -ACQ- de dos niveles, en el que se utiliza la Base de Datos Administrativa y Operativa, centralizada, y se dispone de Bases de Datos Operativas a cargo de dichos Proveedores.

Bajo este esquema, cada vez que un número es portado, este debe ser ingresado a la Base de Datos Administrativa y Operativa. Esta base es consultada en diferentes horas del día por los operadores móviles para actualizar su base de datos operativa. Esta última es consultada por cada operador para el enrutamiento de cada llamada:

Ahora bien, en el artículo 36 de la Resolución CRC 2355 de 2010 (compilado en el 2.6.7.1 de la Resolución CRC 5050 de 2016) se estableció la responsabilidad en la implementación y operación de la base de datos de números portados, así:

‘ARTÍCULO 2.6.7.1. ADMINISTRACIÓN DE LA BASE DE DATOS. La implementación, operación, seguridad, mantenimiento e integridad de la Base de Datos Administrativa, la comunicación de los cambios de Proveedor de Redes y Servicios de Telecomunicaciones por parte de los Usuarios, la coordinación de la sincronía para la actualización de las BDO, y el cumplimiento de las especificaciones técnicas y operativas detalladas definidas por la CRC, estará en cabeza del Administrador de Base de Datos, el cual debe ser un tercero neutral e independiente de los Proveedores de Redes y Servicios de Telecomunicaciones a los que hace referencia el ARTÍCULO 2.6.1.2 del TÍTULO II.

El Administrador de la Base de Datos será seleccionado conjuntamente por los Proveedores de Redes y Servicios de Telecomunicaciones que (...) implementen el esquema de enrutamiento ACQ, teniendo en cuenta criterios de eficiencia y maximización del beneficio para los Usuario

El Administrador de la Base de Datos será seleccionado conjuntamente por los Proveedores de Redes y Servicios de Telecomunicaciones que (...) implementen el esquema de enrutamiento ACQ, teniendo en cuenta criterios de eficiencia y maximización del beneficio para los Usuario’.

Es importante precisar que el mencionado Administrador de la Base de Datos (ABD) es un ente contratado directamente por los proveedores de redes de servicios de telecomunicaciones móviles con el fin de cumplir con las obligaciones relacionadas con la provisión de la facilidad de portabilidad numérica móvil establecidas en la Ley 1245 de 2008 y en el Capítulo 6 del Título 2 de la Resolución CRC 5050 de 2016. El ABD tiene a su cargo la administración, gestión e integridad de la Base de Datos Administrativa, la mediación de los cambios de Proveedor de Servicios de Telecomunicaciones y la coordinación de la sincronía de la actualización de las Bases de Datos Operativas involucradas en la Portabilidad Numérica. A la fecha el ABD es la empresa Informática El Corte Ingles S.A. (IECISA).

Ahora bien, de acuerdo con lo establecido en el artículo 38 de la Resolución CRC 2355 de 2010 (compilado en el artículo 2.6.7.3 de la Resolución CRC 5050 de 2016) dentro del contrato suscrito entre el ABD y los Proveedores de Redes y Servicios de Telecomunicaciones se deben incluir las siguientes obligaciones para el ABD:

- *Ser responsable por el dimensionamiento, contratación, planeación de los equipos y sistemas necesarios para la implementación y operación de la Base de Datos Administrativa, de conformidad con las especificaciones técnicas y operativas definidas por la CRC.*
- *Mantener la confidencialidad de las informaciones de los procesos de portación, cuando dicha información por disposición legal tenga carácter confidencial o reservado.*

“Por la cual se impone una sanción y se imparte órdenes administrativas”

- *Garantizar en todo momento la reserva de la información de la Base de Datos Administrativa. Dicha información solo podrá ser utilizada para los fines específicos asociados a la portabilidad numérica.*
- *Garantizar los intercambios de informaciones entre los Proveedores de Redes y Servicios de Telecomunicaciones por medio de interfaces abiertas y protocolos comunes.*
- *Garantizar, sin costos adicionales, la disponibilidad de la información necesaria para el enrutamiento de comunicaciones hacia números portados a los Proveedores del servicio de telefonía móvil; a los Proveedores de Larga Distancia Internacional que cursen tráfico con las redes de dichos proveedores; y a los Proveedores de telefonía fija que implementen el esquema de enrutamiento ACQ. La disponibilidad de esta información debe ofrecerse en un servidor electrónico, permitiendo su acceso a través de Internet en forma segura.*
- *Adelantar en los tiempos definidos en la regulación todas las comunicaciones y actividades necesarias para llevar a cabo los Procesos de Portación. Dichas comunicaciones se realizarán mediante mensajes electrónicos con todos los proveedores involucrados en el proceso.*
- *Mantener la Base de Datos Administrativa actualizada y coordinar la sincronía de la actualización de las Bases de Datos Operativas, garantizando la consistencia e integridad de la información contenida en las mismas.*
- *Mantener el registro histórico de números portados por un período no inferior a cinco (5) años, y una vez finalizado el (los) contrato(s), hacer entrega de dicho registro a los respectivos Proveedores de Redes y/o Servicios de Telecomunicaciones, teniendo en cuenta para el efecto las condiciones de confidencialidad aplicables.*
- *Controlar los procesos de portación, garantizando su eficacia y eficiencia.*
- *Establecer un sistema de administración de cupos para reserva de portaciones dentro de las ventanas de cambio, cuya información deberá estar actualizada y disponible para los Proveedores a los que hace referencia el numeral 2.6.1.2.1 del ARTÍCULO 2.6.1.2 del TÍTULO II.*
- *Asignar el NIP a Usuarios de servicios móviles y realizar la verificación de la Solicitud de Portación.*
- *Disponer en la BDA de mecanismos de redundancia y contingencia para garantizar la operación continua de la Portabilidad Numérica.*
- *Resolver las fallas que se presenten asociadas a la operación de la Portabilidad Numérica.*
- *Proveer en tiempo real la información requerida por la CRC, incluyendo entre otros los siguientes elementos:*
 - *Solicitudes de Portación iniciadas y finalizadas, incluyendo los plazos de las mismas, discriminadas por proveedor.*
 - *Solicitudes de Portación rechazadas y discriminadas por Proveedor y causa.*
 - *Registro de fallas, con sus causas, procedimientos y tiempos de solución.*

De otra parte, en el artículo 4 de la Resolución CRC 2566 de 2010 (compilado en el artículo 2.6.11.4 de la resolución CRC 5050 de 2016) se establece que el ABD y los Proveedores de Redes y Servicios de Telecomunicaciones siempre deberán permitir el acceso al servicio de administración de la base de datos de la portabilidad numérica a otros Proveedores de Redes y Servicios. En el mismo artículo se precisa que el acuerdo entre el ABD con nuevos Proveedores de Redes y Servicios asignatarios directos de numeración geográfica o no geográfica, siempre estará sujeto al principio de no discriminación.”

4.5.2. Requerir a la sociedad INFORMÁTICA EL CORTE INGLÉS S.A., Sucursal Colombia -IECISA (“El Corte inglés”) con el fin de que indique:

- (a) Informe, de forma clara y precisa, cual es el origen normativo de la base de datos de portabilidad numérica. Lo anterior especificando también la siguiente información: (i) finalidad; (ii) forma de alimentación; y (iii) rol que desempeñan los operadores de telefonía celular y la empresa Corte Inglés de cara al uso de la base de datos de portabilidad numérica.
- (b) Indicar cual es el Rol normativo del Corte Inglés de cara a las bases de datos negativa y positiva de reportes de IMEI y portabilidad numérica. Lo anterior especificando también la siguiente información: (i) bajo que aplicación licenciada a los operadores se

“Por la cual se impone una sanción y se imparte órdenes administrativas”

información a procesar, así como de las ofertas de mejora al proceso de portabilidad numérica en Colombia, incluyendo la administración de la Base de Datos de Portabilidad (BDA); a gestionar los procedimientos de portación que incluye la comunicación de los cambios de PRSTM por parte de los Usuarios y la coordinación de la sincronía para la actualización de las Bases de Datos Operativas (en adelante BDO); y a prestar el servicio de administración de números portados de conformidad con las especificaciones técnicas y operativas señaladas en el contrato y sus anexos, así como, las definidas en la Resolución Compilatoria CRC 5050 de 2016, Capítulo 6, y las normas que desarrollen, aclaren, modifiquen o complementen el proceso de portabilidad numérica móvil en Colombia, y las que se determinen en el Comité Técnico de Portabilidad (en adelante CTP) o el contrato a través del Comité de Decisiones Conjuntas en adelante el CDC. Todo lo anterior con la finalidad de hacer efectivo el derecho de los usuarios a la portabilidad numérica a que hace referencia la Ley 1245 de 2008.

La base de datos de portabilidad numérica es alimentada por la información que proporcionan los operadores de telefonía móvil a través de intercambio de mensajería SOAP en protocolo de XML, utilizando medios de comunicación de redes como canales dedicados o enlaces por internet y estableciendo con cada operador móvil, VPNs site to site que permitan transportar la información de forma segura y encriptada.

El rol que desempeñan los operadores de telefonía móvil es permitir al usuario el derecho a la portación a través del intercambio de mensajería con el ABD para los procesos de portabilidad. Para este proceso, el operador receptor envía la solicitud al operador donante con la información del usuario a portar. El ABD recibe la información, la almacena en la base de datos de números portados e informa al operador donante del proceso. El operador donante valida la solicitud y acepta o rechaza la portación. En caso de rechazo (conforme a las causales Resolución No 5929 de 2020), el ABD lo valida y envía la confirmación tanto al donante como receptor para continuar con el proceso. En caso de aceptación, el ABD confirma al operador donante y receptor la ventana de cambio y genera el archivo para informar a todos los operadores los números que finalmente serán portados para que sean sincronizados en los diferentes elementos de red de los operadores y el usuario pueda activar su servicio en el nuevo operador.

(2) Indique cual es el rol normativo del Corte Inglés de cara a las bases de datos negativa y positiva de reportes de IMEI y portabilidad numérica. Lo anterior especificando también la siguiente información: (i) bajo que aplicación licenciada a los operadores realizan su consulta y manipulación; (ii) indicar que rol cumple “ABD” para cada una de las bases de datos mencionadas, y (iii) si la totalidad de bases de datos implicadas en la portabilidad numérica son aquellas a que hace alusión la norma que crea, desarrolla y da finalidad a la portabilidad numérica;

Respuesta:

Que de conformidad con la Ley 1453 de 2011, el Decreto 1630 del 19 de mayo de 2011, Decreto 2025 de 2015, así como de la Resolución CRC 3128 del 07 de septiembre de 2011, modificada por las Resoluciones CRC: 4813 de 2015, 4868 de 2016, 4937 de 2016, 4948 de 2016, 4986 de 2016 y 5038 de 2016, compilada por la Resolución CRC 5050 de 2016 y las normas que la desarrollen, aclaren, modifiquen o complementen, los PRSTM están obligados a realizar la contratación del administrador de las bases de datos positiva y negativa para la restricción de la operación en las redes de telecomunicaciones móviles de los equipos terminales móviles reportados como hurtados y/o extraviados.

Que para el efecto, los PRSTM construyeron conjuntamente unas Condiciones Generales de Contratación que contienen las condiciones mínimas técnicas, económicas y jurídicas para la contratación de la mencionada base.

Que se realizó una selección objetiva, en la cual participaron varios proponentes y se escogió a Informática El Corte Inglés para suscribir este contrato.

EL ABD, de acuerdo con los términos y condiciones contenidas en el Contrato y sus anexos, se obliga para con todos y cada uno de los PRSTM a llevar a cabo la implementación, prueba, montaje, operación, seguridad, administración, calidad, mantenimiento, actualización, respaldo e integridad

“Por la cual se impone una sanción y se imparte órdenes administrativas”

de las bases de datos positiva y negativa para la restricción de la operación en las redes de telecomunicaciones móviles de los equipos terminales movibles reportados como hurtados y/o extraviados de conformidad con las especificaciones técnicas y operativas señaladas en el presente Contrato en cabeza del ABD, las definidas por la regulación o el Contrato a través del Comité de Decisiones Conjuntas en adelante el CDC.

Con respecto a una aplicación licenciada de uso para los operadores, Informática El Corte Ingles con su experiencia en el sector de telecomunicaciones y específicamente en el ámbito de la portabilidad numérica, ofrece un amplio portafolio de soluciones a empresas de telecomunicaciones, para este caso, ofrece la solución llamada PortaNode, el software que permite al operador móvil interactuar con el ente central de portabilidad para el intercambio de mensajería para dar cumplimiento a los distintos procesos regulatorios de portabilidad numérica móvil.

Con respecto a la base de datos operativa de IMEIs, Informática El Corte Ingles ofrece la solución cliente llamada MobLystNode o SRTMNode, software que permite al operador móvil interactuar con el ente central de IMEIs para el intercambio de mensajería para dar cumplimiento a los distintos procesos regulatorios para el control de hurto de terminales en base de datos positiva y negativa.

En cuanto al ROL que desempeña Informática El Corte Ingles, en su rol de ABD, es necesario precisar lo siguiente:

ABD con relación a la Portabilidad Numérica

ABD: persona jurídica que tiene a su cargo la administración, gestión e integridad de la Base de Datos Administrativa, la mediación de los cambios de Proveedor de Servicios de Telecomunicaciones y la coordinación de la sincronía de la actualización de las Bases de Datos Operativas involucradas en la Portabilidad Numérica.

Obligaciones del ABD para portabilidad numérica:

- Ser responsable por el dimensionamiento, contratación, planeación de los equipos y sistemas necesarios para la implementación y operación de la Base de Datos Administrativa, de conformidad con las especificaciones técnicas y operativas definidas por la CRC. Mantener la confidencialidad de las informaciones de los procesos de portación, cuando dicha información por disposición legal tenga carácter confidencial o reservado.*
- Garantizar en todo momento la reserva de la información de la Base de Datos Administrativa. Dicha información sólo podrá ser utilizada para los fines específicos asociados a la portabilidad numérica.*
- Garantizar los intercambios de informaciones entre los Proveedores de Redes y Servicios de Telecomunicaciones por medio de interfaces abiertas y protocolos comunes.*
- Garantizar sin costos adicionales la disponibilidad de la información necesaria para el enrutamiento de comunicaciones hacia números portados a los Proveedores a los que hace referencia el numeral 2.6.1.2.1 del ARTÍCULO 2.6.1.2 del TÍTULO II resolución 5050 de 2016 y a los Proveedores de Larga Distancia Internacional que cursen tráfico con las redes de dichos proveedores y hayan adelantado el proceso de pruebas para la implementación de la portabilidad numérica. La disponibilidad de esta información debe ofrecerse en un servidor electrónico, permitiendo su acceso a través de Internet en forma segura.*
- Adelantar en los tiempos definidos en la regulación todas las comunicaciones y actividades necesarias para llevar a cabo los Procesos de Portación. Dichas comunicaciones se realizarán mediante mensajes electrónicos con todos los proveedores involucrados en el proceso.*
 - Mantener la Base de Datos Administrativa actualizada y coordinar la sincronía de la actualización de las Bases de Datos Operativas, garantizando la consistencia e integridad de la información contenida en las mismas.*
 - Mantener el registro histórico de números portados por un período no inferior a cinco (5) años, y una vez finalizado el (los) contrato(s), hacer entrega de dicho registro a los respectivos Proveedores de Redes y/o Servicios de Telecomunicaciones, teniendo en cuenta para el efecto las condiciones de confidencialidad aplicables.*
- Controlar los procesos de portación, garantizando su eficacia y eficiencia.*
- Disponer en la BDA de mecanismos de redundancia y contingencia para garantizar la operación continua de la Portabilidad Numérica.*

“Por la cual se impone una sanción y se imparte órdenes administrativas”

- Resolver las fallas que se presenten asociadas a la operación de la Portabilidad Numérica.

Las bases de datos de portabilidad numérica en el ABD, únicamente son utilizadas para este servicio, fueron creadas y destinadas únicamente para este fin. No existe intercambio de información ni relación con la base de datos positiva ni negativa.

ABD con relación a la base de datos positiva y negativa

ABD: Persona jurídica encargada de la Administración de la BDA en la cual se almacena la información asociada a equipos terminales móviles.

Obligaciones del ABD con relación a la base de datos positiva y negativa.

- Responsabilizarse por el dimensionamiento, provisión y planeación de los equipos y sistemas necesarios para la implementación y operatividad de la base de datos centralizada, acogiendo las disposiciones regulatorias contenidas en el CAPÍTULO 7 del TÍTULO II, en particular las definidas en la SECCIÓN 3 resolución 5050 de 2016.
- Asegurar la correcta implementación y operación de la BDA.
- Garantizar el intercambio continuo de información entre la BDA y las BDO de cada PRSTM, y la BDA y el Ministerio de TIC, empleando interfaces y sistemas de soporte de arquitecturas abiertas con protocolos comunes estandarizados.
- Actualizar diariamente la información de IMEI contenida en la BDA, con la información desagregada de los IMEI de los equipos que son importados legalmente al país, a partir del 1o de diciembre de 2015 de acuerdo con lo establecido en el Decreto 2025 de 2015 o el que lo sustituya, adicione o modifique.
- Verificar contra la BDA positiva y BDA negativa los IMEI que remita el Ministerio de TIC como parte del proceso de validación de que trata el artículo 4° del Decreto 2025 de 2015 o el que lo sustituya, adicione o modifique, e informar a dicho Ministerio respecto de cada uno de los IMEI, si se encuentran o no registrados en dichas BDA
- Proporcionar los estándares, guías de manejo, seguridad, procedimientos de acceso y control de toda la documentación necesaria para garantizar el acceso a la BDA, así como su actualización y disponibilidad permanente.
- Garantizar que la BDA pueda ser accedida de manera permanente y simultánea desde cualquier PRSTM, por lo que deberá definir un sistema de concurrencias acorde con dicho requerimiento, e informar a la Dirección de Vigilancia y Control del Ministerio de TIC (vigilanciaycontrol@mintic.gov.co) y a la CRC las fallas, novedades, contingencias o inconsistencias relacionadas con la información de los IMEI que son incluidos o retirados de las bases de datos positiva y negativa.
- Garantizar que el acceso a la información almacenada en la BDA se encuentre disponible los siete (7) días a la semana, las veinticuatro (24) horas al día.
- Definir e implementar políticas de respaldo de la información, de tal manera que se minimice el riesgo de daño o pérdida de la misma.
- Garantizar la protección de los datos personales almacenados en la BDA, los cuales podrán ser utilizados únicamente para los fines establecidos en el CAPÍTULO 7 del TÍTULO II resolución 5050 de 2016 y no podrán ser divulgados, ni compartidos, ni utilizados para otros fines.
- Disponer de mecanismos que permitan tener trazas de auditoría completas y automáticas relacionadas con el acceso a la BDA y las actividades de actualización o manipulación de la información, incluyendo la capacidad de generar alertas a efectos de mitigar los riesgos asociados con el manejo inadecuado de la información, apoyar el cumplimiento de las disposiciones regulatorias aplicables y satisfacer los requerimientos de auditoría.
- Suministrar las herramientas e interfaces adecuadas para la realización de consultas en línea, registro a registro, por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, la CRC y demás organismos autorizados para acceder a la BDA. Así mismo, poner a disposición del público una consulta vía Web registro a registro, de los IMEIs que se encuentren incluidos en la base de datos negativa

Con relación a si la totalidad de bases de datos implicadas en la portabilidad numérica son aquellas a que hace alusión la norma que crea, desarrolla y da finalidad a la portabilidad numérica, se indica que Informática El Corte Inglés, da cumplimiento a la resolución compilatoria 5050 de 2016 en lo que respecta a la base de datos de portabilidad numérica.

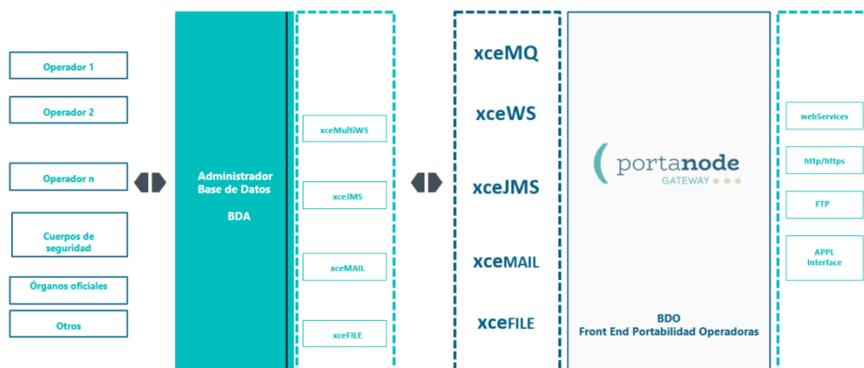
(3) Remitir flujograma que explique la funcionalidad e interacción de las bases de datos Positiva y Negativa para registro de IMEIS y Portabilidad Numérica

“Por la cual se impone una sanción y se imparte órdenes administrativas”

con el aplicativo Portando y ABD. En relación indique si la información allí contenida puede ser sustraída, y de ser posible por favor dar una muestra del total de la información almacenada en ambas de datos para los siguientes números de cédulas de ciudadanía [REDACTED]

Respuesta:

Diagrama interacción base de datos portabilidad numérica y PortaNode



Durante esta interacción entre el ABD y el operador, se utilizan las siguientes bases de datos:

BASE DE DATOS ADMINISTRATIVA (BDA) PARA LA PORTABILIDAD NUMÉRICA: Base de datos administrada por el ABD, que contiene como mínimo la información necesaria para el enrutamiento de comunicaciones hacia números portados, y que se actualiza de conformidad con el Proceso de Portación.

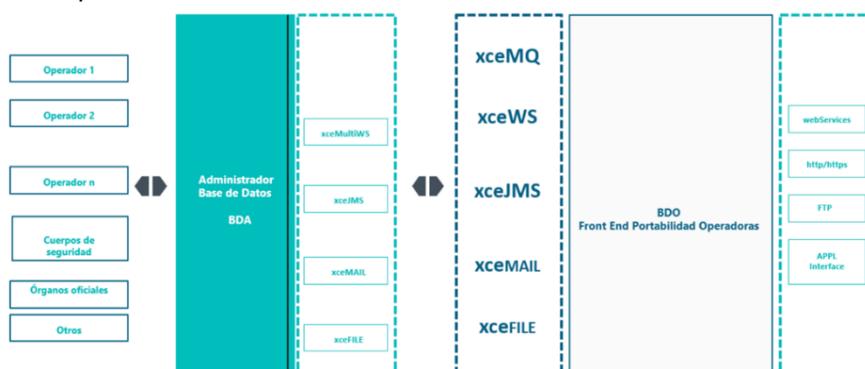
Es importante aclarar que la BDA de portabilidad numérica no está interconectada ni tiene relación con la BDA positiva y negativa de terminales móviles, ni con las BDO positiva y negativa de los operadores.

BASE DE DATOS OPERATIVA (BDO) PARA LA PORTABILIDAD NUMÉRICA: Base de datos administrada por un determinado Proveedor de Servicios de Telecomunicaciones, que contiene la información necesaria para el enrutamiento de las comunicaciones hacia números portados, la cual es obtenida y actualizada desde la BDA. La información que intercambia a través de servicios web con el ABD solo es del determinado Operador (solicitud de portación, solicitud de nip, cancelación de portación).

El intercambio de información entre el ABD y el operador móvil se realiza a través de una conexión segura establecida entre las 2 entidades (ABD y Operador Móvil), a través de protocolos de comunicaciones seguros como VPN, donde la información viaja cifrada por seguridad.

Como resultado del proceso de portabilidad, al final de cada día el ABD deja en su servidor varios ficheros que contienen la numeración, código donante, código receptor, NRN, identificador del proceso y fecha de ventana de cambio. Este archivo resultante de los procesos exitosos de portabilidad es descargado desde el ABD por los operadores móviles para realizar el enrutamiento y activación de los servicios móviles en las redes de comunicaciones. Se aclara que este archivo no contiene datos personales y/o información sensible de los abonados de telefonía móvil.

En el proceso de registro de terminales móviles interactúa el ente central o ABD con el operador de telefonía móvil.



“Por la cual se impone una sanción y se imparte órdenes administrativas”

La configuración técnica para el funcionamiento de las bases de datos positiva y negativa constará de una Base de Datos centralizada –BDA- interconectada con bases de datos operativas -BDO- de propiedad de los PRSTM. La función de las Bases de Datos Positivas es identificar y llevar un registro de los equipos terminales móviles que registran actividad en la red y de aquellos que pueden ser habilitados en las redes de los PRSTM. La función de las Bases de Datos Negativas es llevar un registro de los equipos terminales móviles que no pueden ser habilitados en las redes de los PRSTM por haber sido reportados como hurtados y/o extraviados por parte del propietario del equipo terminal móvil o el propietario autorizado por éste.

Es importante aclarar que la BDA positiva y negativa no está interconectada ni tiene relación con la BDA de Portabilidad Numérica, ni con las BDO de portabilidad numérica de los operadores.

PortaNode, al ser un producto de software que interactúa con el ente central de portabilidad numérica (BDA), no tiene ninguna relación con las BDA positiva y negativa ni con la BDO de IMEI del operador, ya que están dispuestas para fines diferentes.

Para el funcionamiento de PortaNode no se requiere consultar la base de datos de IMEI, cumpliendo con los requerimientos definidos en la regulación.

La única interacción de PortaNode es con la BDA de portabilidad numérica, por lo que se tiene establecido un canal de comunicación por VPN con el ABD para el intercambio de información a través de web services o acceso por sftp a los ficheros que genera el ABD. No hay acceso del operador directamente a la base de datos del ABD.

Así mismo, tanto la BDA de portabilidad como la BDA positiva y negativa se encuentran en ambientes e infraestructuras diferentes y separadas entre sí, de modo tal que no hay conexión a nivel lógico ni físico que permita interactuar entre ellas.

Del mismo modo, no existe interacción entre PortaNode y la base de datos de IMEI del operador para ningún proceso del sistema, ya que cada aplicación es independiente en sus procesos hacia el ABD.

Con relación con la pregunta si la información allí contenida puede ser sustraída, vale la pena aclarar, que los únicos que tienen acceso a consultar la información son los operadores móviles, organismos de control como CRC y Mintic, Entidades Policivas y Judiciales, a través de protocolos seguros por VPN, lo cual controla el acceso y evitar que terceros puedan acceder.

Así mismo, se aclara que para cierto detalle de información, un operador no puede consultar información sensible o confidencial de otro operador, solo se puede consultar información relevante para todos los operadores y que son necesarios para los procesos tanto de portabilidad como bases de datos positivas y negativas.

Sobre la información de los siguientes numeras de documentos (i) [REDACTED] fueron consultados en la base de datos administrativa de portabilidad e IMEI (listas blancas y negras) y los resultados fueron:

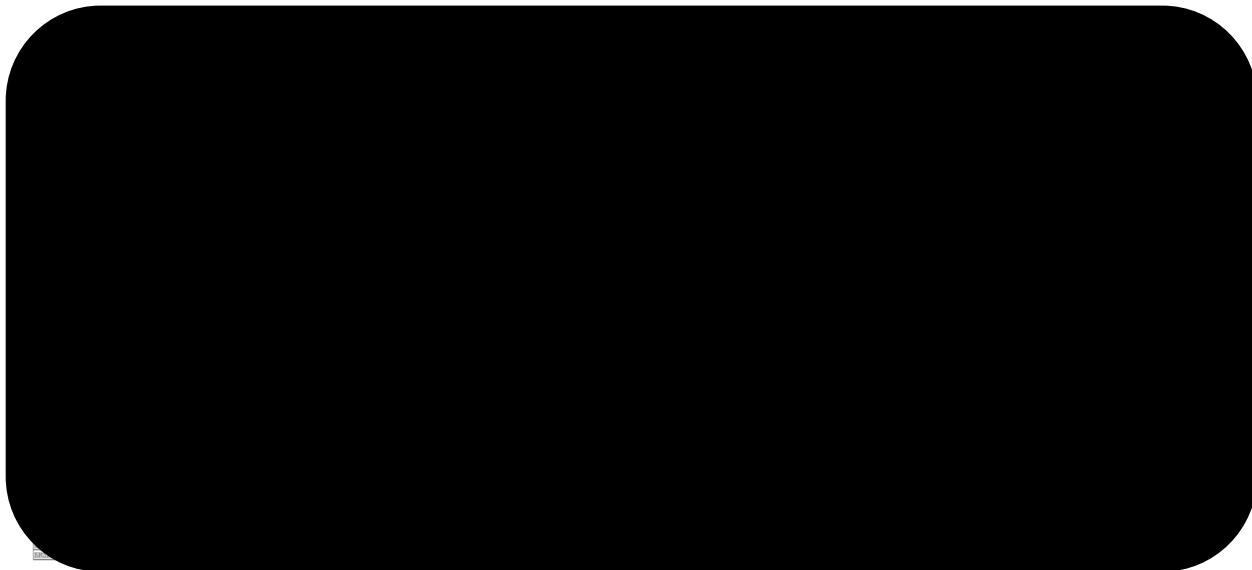
BDA Portabilidad numérica: no se encontraron datos relacionados con los números de documentos [REDACTED]

BDA Positiva y Negativa para registro de IMEIS: se adjunta a este comunicado fichero en Excel llamado Positiva_Negativa_Portabilidad_SIC_20201112.xlsx con la información encontrada.

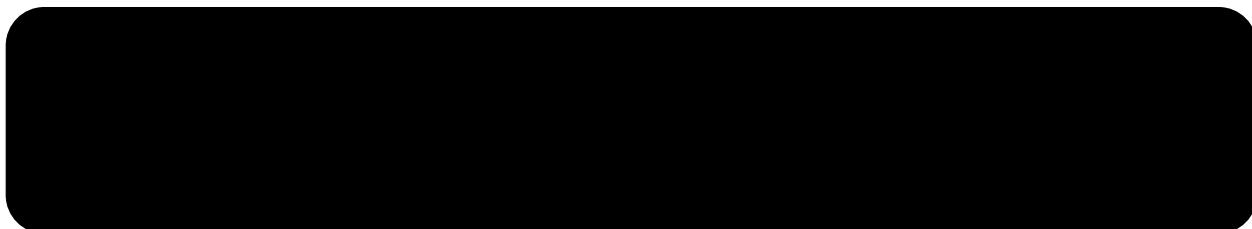
Dentro de los ficheros de Excel remitidos por parte del Corte inglés la información remitida es la siguiente:

“Por la cual se impone una sanción y se imparte órdenes administrativas”

(a) **BDA POSITIVA**



(b) **BDA POSITIVA**



QUINTO: Que, una vez integradas las pruebas y practicadas las pruebas decretadas de oficio por parte del Despacho, a través de los radicados 18 -127153 - - 126 al 128 del 7 de abril de 2021, se dio cierre a la etapa probatoria y se le dio traslado por un término de diez (10) días a CLARO, como investigada, y a TIGO y AVANTEL, como terceros interesados, los cuales presentaron alegatos de conclusión, así:

5.1. Alegatos de conclusión de CLARO

Mediante radicado 18 – 127153 - - 135 del 22 de abril de 2021, CLARO presentó sus respectivos alegatos de conclusión donde expuso lo siguiente:

“1. Las imputaciones fácticas y el cargo de infracciones de formuló la Dirección en el acto de apertura de la investigación.

Mediante la resolución número 35890 del 7 de julio de 2020, la Dirección de Investigación de Protección de Datos Personales ordenó el inicio de la investigación administrativa de la referencia, y formuló cargos contra la sociedad Comunicación Celular de la siguiente forma:

CARGO PRIMERO: La presunta vulneración, en su calidad de Responsable del principio de finalidad (L.1518/12, art. 4(c)) y el deber de informar de forma debida sobre la finalidad de recolección y los derechos que le asisten por virtud de la autorización otorgada (L.1581/12, art. 17(c)).

CARGO SEGUNDO: La presunta vulneración, en su calidad de Responsable del principio de libertad (L.1581/12, art. 4(c)) y el deber de solicitar y conservar copia de la respectiva autorización otorgada por el Titular en los términos establecidos por la ley (L.1581/12, arts. 9 y 17(b), D.1377/13, arts.5,7 y 8 - incorporado en el D.1074/15-).

En ese orden, y de conformidad con lo dispuesto en la resolución de apertura de esta investigación administrativa, la Dirección sostuvo que CLARO presuntamente habría infringido las citadas normas bajo los siguientes supuestos fácticos:

Fundamentación fáctica del cargo No. 1:

“De este modo, se puede establecer preliminarmente que CLARO en su condición de Responsable del Tratamiento de Datos, actuó en contradicción de mandato legal de realizas el tratamiento de la información de los Titulares

“Por la cual se impone una sanción y se imparte órdenes administrativas”

en virtud a la finalidad legítima de acuerdo con la norma que da fundamento legal a la creación de la base de datos, al dar uso distinto, **y fuera de su marco legal de la información personal contenida en la base de datos positiva y negativa creada en virtud de la Ley 1453 de 2011, cuya finalidad es la de restringir “(. . .) la operación de redes de telecomunicaciones móviles de los equipos de terminales móviles reportados como hurtados y/o extraviados”**; aun cuando la Corte Constitucional proscribió la recolección de (. . .) de datos para una finalidad diferente a la inicialmente prevista”, dado que (i) como bien expresaron, en el radicado 18 – 127153-31 del 4 de junio de 2020, y en su anexo 3, **se realizó “cruce de información de clientes portados del Corte Inglés para identificar clientes que se portaron de otra empresa”; (ii) Que para estos efectos se utilizó la aplicación PORTANODE la cual tiene acceso a la totalidad de los IMEI-IMSI-MSISDN de los equipos terminales móviles e información personal y sensible de los propietarios registrados en Colombia de cada uno de los PSRTM activos en el país, y; (iii) una vez extraídos estos datos, se realizaron, como bien se estableció en las averiguaciones preliminares, llamadas de varios números CLARO a números TIGO, AVANTEL, y del denunciante sin que mediara la autorización, previa e informada, para contactar con los Titulares para procesos de captación de clientes y marketing.**

Así las cosas, CLARO, en caso de probarse, es responsable de la vulneración al régimen de protección de datos contenido en la Ley 1581 de 2012, Decreto 1377 de 2013 -incorporado al Decreto 1074 de 2015- **por realizar el tratamiento de la información personal y sensible contenido en la base de datos creada en virtud de la Ley 1453 de 2011-base de datos positiva y negativa, con una finalidad distinta a la prevista por la norma que le dio origen**, utilizándola para fines de marketing y capacitación masiva de Titulares afiliados a otros PSRT o operadores, y sin que mediara la autorización, previa y expresa, de los Titulares para la utilización de la información otorgada en virtud de la finalidad de la ley habilitante de la base de datos positiva y negativa; tratamiento que no se encuentra dentro del espectro de “(. . .) la operación de redes móviles reportados como hurtados y/o extraviados la operación en las redes de telecomunicaciones móviles de los equipos terminales móviles reportados como hurtados y/o extraviados”, y por tanto ilegal.” (subrayas y negrita fuera del texto).

Fundamentación fáctica del cargo No. 2

“De acuerdo a lo anterior, se puede evidenciar que CLARO aprovechó el acceso que tiene a la base de datos positiva y negativa, creada en virtud de la Ley 1453 de 2011, a través del aplicativo PORTANODE, y cuya finalidad es “[L]a restricción de la operación en las redes de telecomunicaciones móviles de los equipos terminales móviles reportados como hurtados y/o extraviados; la cual está alimentada por los IMEI-IMSI-MSISDN de los equipos terminales móviles, la información personal sensible que los Titulares otorgan en virtud del registro, para solo estos efectos- el cual aplica para todo el territorio nacional, con el fin de llevar a cabo llamadas masivas a usuarios de otros operadores a nivel nacional para que estos migraran de su operador a CLARO, sin que mediara su consentimiento, previo y expreso, para darle el tratamiento distinto a [L]a restricción de la operación en las redes de telecomunicaciones móviles de los equipos terminales móviles reportados como hurtados y/o extraviados, lo cual es la finalidad ulterior de las bases de datos positivas y negativa” (subrayas y negrita fuera del texto)

2. Inexistencia de transgresión normativa por parte de CLARO

Resulta importante para esta compañía reiterar que la SIC no puede confundir el proceso de portabilidad numérica y sus bases de datos, con el proceso de control u detección de IMEIS y sus bases de dato, ya que a pesar de que ambos procesos son administrados por el Corte Inglés en calidad de ABD-administrador de bases de datos-, el cual es contratado por los prestadores tanto para el proceso de portabilidad numérica, como para el proceso de control y detección de IMEIS, pues dichos procesos son independientes, tal como lo afirmó el Corte Inglés en la respuesta dada por al requerimiento realizado por la misma dirección dentro de la presente investigación:

“Las bases de datos de portabilidad numérica en el ADB, únicamente son utilizadas para este servicio, fueron creadas y destinadas únicamente para este fin. No existe intercambio de información ni relación con las bases de datos positiva ni negativa”.

De igual forma El Corte Inglés sostuvo:

“Por la cual se impone una sanción y se imparte órdenes administrativas”

Es importante aclarar que la BDA positiva y negativa no está interconectada ni tiene relación con la BDA de portabilidad numérica, ni con las BDO de portabilidad numérica de los operadores.

La BDA positiva contiene:

- i) Los IMEI de todos los equipos terminales móviles que ingresan importados legalmente al país a partir el 1 de diciembre de 2015, de acuerdo con lo establecido en el artículo 4 del Decreto 2025 de 2015 o el que lo sustituya, adicione o modifique;*
- ii) Los IMEI cuyos usuarios realizaron en el registro de los datos de identificación del propietario o usuario autorizado por éste, dado cumplimiento al proceso de registro IMEI dispuesto en el artículo 2.7.3.4. del capítulo 7 del título II, o como resultado del proceso de detección de cambio de ETM respecto a la SIM de que se trata el numeral 2.7.2.1.7. del artículo 2.7.2.1. del capítulo 7 del título II.*
- iii) Los IMEI que hasta el 30 de noviembre de 2015 fueron cargados por los PRSTM luego del proceso de importación al país.*

La BDA negativa contiene:

- i) Los IMEI de los equipos terminales móviles que han sido reportados como hurtados o extraviados a cualquier PRSTM que opere en el país, asociados a los datos que trata el numeral 2.7.2.1.23 del artículo 2.7.2.1. del capítulo y del título II.*
- ii) Los IMEI bloqueados por no registro en la BD positiva;*
- iii) Los IMEI reportados como hurtados o extraviados en otros países con los cuales se realice intercambio de bases de datos negativas o través de bases de datos centralizadas.,*
- iv) Los IMEI que sean detectados como duplicados, inválidos o no homologados, a partir de que la CRC establezca las condiciones en las cuales se debe proceder al bloqueo de dichos IMEI.*
- v) Los IMEI reportados por el PRSTM con tipo de bloqueo “reincidente” como resultado del proceso establecido en el parágrafo 1 del artículo 2.7.3.3. del capítulo 7 del título II.*
- vi) Los IMEI reportados por el PRSTM como resultado de procedimientos de detección y control de fraudes en la suscripción del servicio, o por pérdida de equipos en inventario o instalaciones que aun no. Han sido vendidos, los cuales deben ser incluidos como tipo de bloqueo “administrativo”. Este tipo de bloqueo deberá empezar a realizarse a más tardar el 1 de enero de 2017. El PRSTM que incluya estos IMEI en la base de datos negativa, deberá contar con los respectivos soportes que evidencien el fraude o la pérdida de los equipos.*

En consecuencia, vale la pena recordar que, a diferencia de la base de datos de portabilidad numérica, la BDA de control de IMEIS si se compone por una base de datos positiva y negativa, tal y como se explicó en los Descargos presentados por la compañía en concordancia con lo dispuesto en el artículo 2.7.3.2. de la Resolución 5050 de 2016:

< En efecto, el ABD de acuerdo con los términos y condiciones contenidas en el Contrato y sus anexos, se obliga para con todos y cada uno de los PSRTM a llevar a cabo la implementación, prueba, montaje, operación, seguridad, administración, calidad, mantenimiento, actualización, respaldo e integridad de las bases de datos positiva y negativa para la restricción de la operación en las redes de telecomunicaciones móviles de los equipos terminales reportados como hurtados y/o extraviados de conformidad con las especificaciones técnicas y operativas señaladas en el Contrato en cabeza del ABD, las definidas por la regulación o el Contrato a través del Comité de Decisiones Conjuntas en 4.

(. . .)

4.. Conclusiones Finales

Comcel no ha incumplimiento sus obligaciones en materia de protección de datos pues:

Como se explicó a lo largo de este escrito, las bases de datos de portabilidad no contienen datos personales respecto de los cuales se requiere contar con autorización, expresa e informada por parte del titular, sino que lo incorporado en la misma corresponde a un listado público de números que no identifican de manera personal a ningún usuario en concreto. “

5.2. Alegatos de conclusión de TIGO

Mediante radicado 18 -127153 - - 134 del 21 de abril de 2021, TIGO presentó sus respectivos alegatos de conclusión donde expuso lo siguiente:

“(. . .)

CAPÍTULO III. ALEGATOS DE CONCLUSIÓN

1. INCUMPLIMIENTO DE LAS NORMAS

*Reiterando los argumentos ya expuestos, se debe tener presente que la base de datos de la que COMCEL ha extraído información para finalidades distintas a las que dieron origen a su creación, es la **base de datos centralizada de portabilidad numérica móvil**, misma que fue concebida con el único propósito de permitir el enrutamiento de las llamadas. Esto es:*

La base de datos centralizada de portabilidad numérica móvil de la que COMCEL ha extraído información para configurar la lista de números a contactar de clientes que no pertenecen a este operador, como quedó consignado en la visita efectuada a las instalaciones de este operador, tiene por finalidad permitir el proceso de portabilidad numérica de acuerdo con lo dispuesto en el título II de la Resolución compilatoria CRC 5050 de 2016.

La base de portabilidad es en esencia aquella administrada por el ABD que para este caso se encuentra en cabeza de la sociedad Informática El Corte Inglés S.A. y es puesta a disposición de todos los operadores de servicios de telecomunicaciones con la única finalidad de implementar la portabilidad numérica, específicamente para el enrutamiento de llamadas hacia los números portados.

De acuerdo con el artículo 2.6.3.1, Capítulo 6 del Título II de la Resolución CRC 5050, en la solución técnica para la implementación y operación de la portabilidad numérica en Colombia los operadores móviles deberán enrutar las comunicaciones con destino a números no geográficos de redes, de acuerdo con el esquema de ACQ all call query de dos niveles en el que se utiliza la base de datos administrativa centralizada y se dispone de bases de datos operativas a cargo de los operadores, por tanto, es con este objetivo que los operadores pueden tener acceso a la información de todos los números portados hacia todos los operadores móviles del país.

A lo largo de esta investigación, desde el 24 de abril de 2018, hemos presentado diversos ejemplos del mal obrar de COMCEL, relacionando pruebas y hechos del uso indebido que ha dado la investigada a la base de portabilidad, realizando llamadas a usuarios, utilizando sus datos de manera indiscriminada y sin contar con las autorizaciones respectivas, violando abiertamente la normatividad de la materia. Lo anterior, se ha visto claramente demostrado a través de las denuncias elevadas por TIGO y otros operadores de telecomunicaciones en contra COMCEL, así como los argumentos esgrimidos por la SIC en la Resolución número 35890 de 2020, de los cuales se puede concluir de forma contundente que, COMCEL ha puesto en marcha desde hace por lo menos dos años, prácticas para el tratamiento de datos personales abiertamente contrarias a lo dispuesto en la Ley 1581 de 2012 y el Decreto 1377 del 2013. De lo cual se puede extraer que.

- 1. COMCEL pese a tener acceso a la base de portabilidad numérica administrada por la ABD como cualquier operador, la utiliza para fines distintos a la que fue creada.*
- 2. COMCEL no cuenta con la autorización de los usuarios para dar un tratamiento distinto a los datos personales contenidos en la base de portabilidad, ni informó adecuadamente a los titulares e identificar una condición jurídica para dicho tratamiento, presupuestos que de hecho no son posibles en este caso, toda vez que como se insiste, la base de datos tiene una finalidad específica de permitir el enrutamiento de llamadas de líneas portadas.*

*Por su parte la Ley 1581 de 2012 en su artículo 4, establece que para el tratamiento de cualquier tipo de datos personales, incluidos los considerados públicos, es necesario dar aplicación al **principio de finalidad**, esto es, todo uso de información personal que se pretenda debe tener un propósito específico, acorde a la ley e informando el titular de manera previa, clara y suficiente y en todo caso, el tratamiento de datos personales para una finalidad*

“Por la cual se impone una sanción y se imparte órdenes administrativas”

distinta a la permitida por ley deberá contar con autorización expresa del titular de los datos.

Adicionalmente, la Ley 1581 señala que las actividades de recolección de datos personales obedecen a una finalidad legítima de acuerdo con la Constitución y la ley, determinando que el propósito para la cual será usada dicha información deberá comunicarse al titular de manera previa o concomitante con el otorgamiento de la autorización por parte de este, cuando ella sea necesaria o, en general, siempre que el titular solicite información al respecto.

Según estas consideraciones, COMCEL no solo ha venido utilizando datos personales con fines distintos a los manifestados en la ley que da origen a la base de datos, sino que además no cuenta con los consentimientos de los titulares de la información para este efecto, ni para ningún otro tipo de tratamiento que pudiera equipararse a las finalidades de la base de datos o ser previsto por los afectados.

De otro lado y no menos importante, se debe resaltar la existencia de otra obligación normativa en lo relacionado con la privacidad de la información referente a la responsabilidad demostrada, esto es, que se hace necesario exhortar a los representantes legales de COMCEL para que den cuenta de las directrices que frente al tratamiento de datos personales se están impartiendo al interior de esta organización y que acciones correctivas y eficientes han tomado para evitar las prácticas ilegales expuestas.

Según estas consideraciones, COMCEL no solo ha venido utilizando datos personales con fines distintos a los manifestados en la ley que da origen a la base de datos, sino que además no cuenta con los consentimientos de los titulares de la información para este efecto, ni para ningún otro tipo de tratamiento que pudiera equipararse a las finalidades de la base de datos o ser previsto por los afectados.

De lo anterior queda claro que COMCEL se ha apartado de su deber legítimo de cumplir con las normas de protección de datos personales, dándole finalidades distintas a las bases de datos a las que tiene acceso como operador de servicios de telecomunicaciones. Tan así, que tal y como se informó en el escrito del 11 de agosto de 2020, dicha situación pudo corroborarse por lo sostenido por COMCEL en la visita realizada por la SIC:

“(…) los listados de números son aleatorios de los prefijos de la numeración pública, los cuales son cotejados posteriormente con los archivos públicos del Corte Inglés de consulta para los operadores para efectos de portabilidad numérica, por lo que estos pueden ser descargados para su consulta y actualización. Adicionalmente, el personal del Departamento de Inteligencia de los Negocios explicó que mediante el procedimiento de aprovisionamiento OSS se realiza la descarga del Administrador de Base de Datos de Portabilidad o “ADB” del Corte inglés para consulta de todos los operadores. Finalmente, explicó que CLARO desarrolló un sistema para gestionar la portabilidad llamado PORTANODE, el cual descarga los datos de ADB y se encarga de (i) activar los usuarios; (ii) desactivar los usuarios, y; (iii) relación de cambios para comunicación. La comunicación entre ADB y la lista del Corte inglés se realiza a través de VPN y credenciales asignadas a la compañía (...)”

En virtud de todo lo anterior, es claro que COMCEL continúa ejecutando actos que violan el régimen de protección de datos personales, haciendo uso de la base de portabilidad con un propósito distinto a su finalidad.

Así las cosas, reafirmo todos y cada uno de los argumentos que ha presentado TIGO dentro del asunto de la referencia.

2. PRUEBAS RECAUDADAS POR LA SIC:

Con respecto a las pruebas recaudadas por la SIC, manifestamos que apoyamos los hallazgos encontrados, los cuales soportan las evidencias aportadas por Tigo en su oportunidad, y mencionadas anteriormente. Por lo anterior, solicitamos a la SIC que acepte la siguiente pretensión:

CAPÍTULO IV. PETICIÓN

Por las razones expuestas, se solicita de manera respetuosa a la SIC confirmar los cargos formulados y, en consecuencia, proceder la imposición de la correspondiente sanción, teniendo en cuenta, además, la calidad de tercero interesado de TIGO. (. . .)”

“Por la cual se impone una sanción y se imparte órdenes administrativas”

5.3. Alegatos de conclusión de AVANTEL

Mediante radicado 18 -127153 - - 132 del 19 de abril de 2021, AVANTEL presentó sus respectivos alegatos de conclusión donde expuso lo siguiente:

(...)

II.- LOS HECHOS DENUNCIADOS Y LO PROBADO DENTRO DE LA ACTUACION ADMINISTRATIVA.

*Corresponde a su Despacho declarar, conforme al material probatorio obrante en el expediente administrativo, que la sociedad COMUNICACION CELULAR S.A. que opera en Colombia bajo la marca “CLARO” en los mercados de prestación de servicios de telecomunicaciones, incurrió en infracción al Régimen Legal de Protección de Datos Personales al contactar y realizar ofrecimientos comerciales a un grupo significativo de ciudadanos **que NO otorgaron su autorización para el tratamiento de datos personales a la denunciada y, en consecuencia, utilizando dicha contravención al Régimen de Datos Personales desplegó una estrategia desleal y con fines concurrenciales en contra de varios de sus competidores, dentro de los cuales se destacan aquellos reconocidos como terceros interesados en la presente actuación administrativa.***

COMCEL no pudo probar ni la justa causa para contar en sus bases de datos con la información de contacto de estos ciudadanos, ni mucho menos acreditó el hecho de contar, respecto de estos ciudadanos, con la totalidad de autorizaciones previas, informadas y oportunas para su tratamiento de datos personales, pudiendo incluso, mediante dicha omisión, haber contactado a usuarios registrados ante el Registro Nacional de Números excluidos- RNE.

Conforme a las consideraciones expuestas por AVANTEL en el memorial en que se solicitó reconocimiento de su Despacho como tercero interesado, la realidad es que al margen de no haberse probado un acceso, uso o aprovechamiento ilegal de las bases de datos positiva y administrativa de hurto a celulares o de portabilidad numérica, si en gracia de discusión COMCEL hubiese accedido a la información de tráficos de AVANTEL como consecuencia del Roaming Automático Nacional que cursa por su red, dicha circunstancia NO resulta equivalente, ni puede ser entendida como una autorización para el tratamiento y uso de la información contenida en los CDR (Call Data Register) con fines comerciales, de tal manera que no existe forma alguna en la que COMCEL pueda probar que contaba con dicha autorización por parte de los titulares de datos, en los términos de la Ley 1581 de 2012 y del Decreto 1377 de 2013.

Así las cosas, se probó de manera contundente que COMCEL obtuvo de forma irregular dichos datos personales, y en total oposición al deber de tutela que respecto al derecho fundamental le compete, decidió además disponer de los mismos con fines explotativos, anteponiendo su ánimo de lucro a los derechos fundamentales de los ciudadanos contactados irregularmente y ejerciendo, aun en perjuicio de los ciudadanos y competidores, un ejercicio abiertamente abusivo de su posición de dominio en los servicios de Voz y datos móviles.

En efecto, AVANTEL pudo probar que COMCEL realizó 1.794.006 llamadas a sus abonados entre el mes de enero hasta el 27 de julio de 2020, tal como se aprecia en la siguiente tabla:

Llamadas	Claro Movil
Ene	203.584
Feb	350.548
mar	322.222
Abr	205.576
may	202.642
Jun	291.687
Jul	217.747
Total general	1.794.006

Elaboración propia

“Por la cual se impone una sanción y se imparte órdenes administrativas”

Sin perjuicio de advertir a su Despacho que las conductas aquí denunciadas y desplegadas por la empresa denunciada, persisten y han tenido vocación de continuidad, tal y como se aprecia en el siguiente cuadro:

Llamadas	Claro Móvil
Ago	647.284
Sep	599.542
Oct	455.948
Nov	568.207
Dic	725.579
Ene	694.128
Feb	861.077
Marzo	874.629
Abril	232.426
Total General	5.658.820

Elaboración propia

Conforme al cuadro anterior, CLARO desde agosto de 2020 hasta la fecha de este memorial, ha realizado desde sus call centers 5.658.820 llamadas usuarios Avantel. **Si se tiene en cuenta que Avantel al tercer trimestre de 2020 (según el informe trimestral Colombia tic) contaba con 1.4 millones de líneas móviles, se concluye que en promedio, durante los últimos 9 meses CLARO realizó en promedio 5 intentos de contacto por cada usuario de servicios de la base total de usuarios Avantel, circunstancia que no solo evidencia su dolo y conciencia al realizar dichos contactos en contravención al régimen de protección de datos personales vigente, sino también una conducta o estrategia cuyo objeto o por efecto no es otro que sacar a mi representada del mercado.**

En resumen, se encuentra probado en el expediente que COMCEL desconoció de forma consciente, premeditada y con fines concurrenciales, tanto la Constitución Política, como las normas legales vigentes de protección y tratamiento de datos personales, así como la regulación de carácter general y concreto que ha expedido la CRC en materia de Hurto a Celulares y portabilidad numérica y, en concreto, las normas que desarrollan el objeto y finalidad de las bases de datos regulatorias.

Igualmente y sin perjuicio de lo expuesto, se probó que COMCEL no acreditó la existencia de autorización previa, informada y expresa de los titulares de datos personales para efectos de ser contactados con fines comerciales, de mercadeo, retención o fidelización, Circunstancia que conforme sustentamos previamente, se ha tornado en una **conducta continuada desplegada por la denunciada** y que adicionalmente, gestiona administra y explota datos con información de ciudadanos que en el pasado fueron sus usuarios, sin perjuicio del decaimiento de la autorización para su tratamiento, como consecuencia de la finalización de la relación contractual y de servicios, con lo cual, por esta vía también estaría infringiendo las normas constitutivas del Régimen de Protección de Datos Personales vigente.

IV. PETICIONES

Que se declare que COMCEL S.A. incurrió en infracción a la Ley Estatutaria 1581 de 2012, y del Decreto 1377 de 2013, y que atendiendo a la gravedad de los hechos y a la cantidad significativa de colombianos afectados con su proceder, se imponga la multa más alta prevista en la Ley, se le impongan las obligaciones de hacer y no hacer que su despacho estime pertinentes para garantizar la cesación de la conducta, así como las demás consecuencias, acciones y abstenciones que su despacho estime pertinentes, conducentes e idóneas para garantizar la protección de los derechos fundamentales conculcados.

Igualmente, en caso de que su Despacho evidencie que el actuar de COMCEL materializó mas de una conducta reprochable a la luz de la normatividad de protección de Datos Personales, proceda a imponer de forma individual e independiente, por cada una de las infracciones identificadas, la máxima multa permitida en la Ley, e imponga las órdenes de hacer o no hacer necesarias para evitar que la afectación continúe.”

SEXTO: Competencia de la Superintendencia de Industria y Comercio

La Ley 1581 de 2012, artículo 19 establece la función de vigilancia que le corresponde a la Superintendencia de Industria y Comercio para garantizar que en el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la mencionada Ley.

SÉPTIMO:**Análisis del caso****7.1. Estructura de las bases administradas por el “Corte Inglés” de acuerdo con la normativa vigente y su uso por parte de los PSRTM.**

De conformidad con lo aportado en la etapa probatoria por parte del Corte Inglés y la C.R.C., así como las conclusiones propias del Despacho, se procede a dar una explicación de la estructura tanto de la base de portabilidad numérica como de las bases de datos positiva y negativa, con el propósito de aclarar su origen normativo, finalidad específica y la interacción por parte de los PSRTM para efectos de la evaluación de la posible vulneración por parte CLARO, por lo que no se hará una descripción amplia de las mencionadas bases de datos, sino de aquellos donde se hace la recolección y tratamiento de datos y la finalidad de estos:

7.1.1. Bases de Datos de Portabilidad Numérica (Ley 1245 de 2008 y C.R.C. Resolución 5050 de 2016)

De conformidad con la Ley 1245 de 2008 y la C.R.C. Resolución 5050 de 2016, las bases de datos de portabilidad numérica tienen como finalidad permitir la portabilidad numérica a los usuarios de telefonía celular de la totalidad de los proveedores de Redes y servicios de telecomunicaciones, bajo criterios estándar fijados por el Plan Nacional del Numeración y demás reglas aplicables.

En ese sentido, la C.R.C. Resolución 5050 de 2016, en explicación dada por parte del Corte Inglés⁹ y la C.R.C.¹⁰ al requerimiento realizado por parte de este Despacho, indicaron que para la consecución de la portabilidad numérica, por requerimiento legal, entre totalidad de los proveedores de Redes y servicios de telecomunicaciones (“PRSTM”) y un tercero imparcial denominado Administrador de la Base de Datos Administrativa (“ABD”) -en la actualidad el Corte Inglés-, celebrar un contrato donde el ABD tiene como función esencial, a favor de los PRSTM, la implementación, migración, prueba, montaje, operación, seguridad, administración, calidad, mantenimiento, adecuación y respaldo e integridad de la solución técnica de la información a procesar, incluyendo la administración constante de la base de datos de portabilidad.

Para el efecto, la C.R.C. Resolución 5050 de 2016, por explicación del Corte Inglés, la portabilidad numérica se realiza a través de la comunicación de dos bases de datos: (i) Base de Datos Administrativa (“BDA”): la cual es administrada por el ABD, y que contiene el mínimo de información necesaria para el enrutamiento de comunicación hacia números portados, y que se actualiza de acuerdo con el proceso de portación. Es necesario indicar que la información mínima necesaria es la siguiente, de conformidad a la C.R.C. R.5050/16, art. 2.6.4.3., a saber: (a) nombre completo; (b) número de documento de identidad; (c) autorización del suscriptor del contrato en caso de una línea pos-pago más una copia del documento de identidad, en caso de que el solicitante sea distinto al suscriptor; (d) número telefónicos asociados a la portabilidad numérica, y (e) proveedor donante. (ii) Base de Datos Operativa (“BDO”): Base de datos operada por los PRSTM que contiene la información necesaria para el enrutamiento de las comunicaciones hacia números portados, la cual es obtenida desde de la BDA. En todo caso, siempre se tendrá acceso, a través de la BDO de cada PRSTM, a la totalidad de los números telefónicos inscritos activos.

Dicha información es intercambiada entre el ABD y el PRSMT a través de una conexión segura mediante VPN, donde la información viaja cifrada, en virtud de que la C.R.C. Resolución 5050 de 2016, artículo. 2.6.4.4. estableció que el suministro de información deberá ser automatizado mediante sistemas informáticos y medios electrónicos, de forma que garantice la rapidez, integridad, y seguridad en el desarrollo del proceso de portabilidad. Para el efecto, de acuerdo con lo indicado por parte del Corte Inglés, el sistema informático que presta en la actualidad este servicio es el programa denominado PORTANODE.

Una vez establecida que son las bases de datos de portabilidad numérica, y que información es solicitada para el proceso de portabilidad, es necesario aclarar cual es el proceso

⁹ Radicado 18-127153 - - 126 del 12 de febrero de 2021.

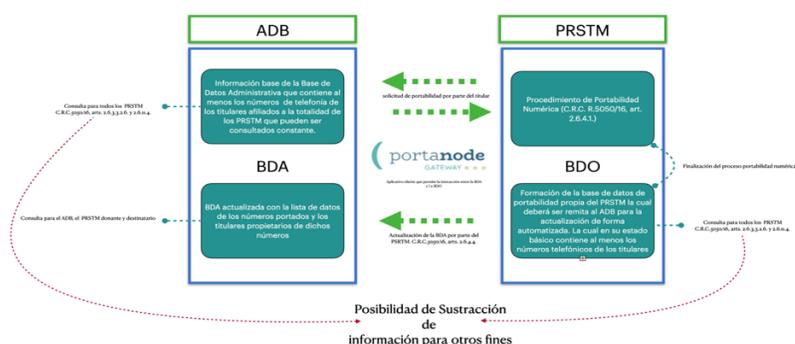
¹⁰ Radicados 18-127153 - - 121 al 123 del 23 de noviembre de 2020.

“Por la cual se impone una sanción y se imparte órdenes administrativas”

de portabilidad numérica y las etapas que se deben surtir, así como algunos aspectos de consulta permanente para los PRSTM en las bases de datos de portabilidad. En relación con el proceso de portabilidad, la C.R.C. Resolución 5050 de 2016, artículo 2.6.4.1., estableció que las etapas para cada solicitud de portabilidad numérica: (i) Generación de NIP de confirmación; (ii) Solicitud de portación (etapa de la portabilidad donde se solicita la información a que hace referencia el artículo 2.6.4.4.); (iii) verificación por parte del ABD; (iv) aceptación o rechazo a la solicitud por parte del proveedor donante, y; (v) planeación ventana de cambio. En el proceso de portabilidad numérica, la C.R.C. Resolución 5050 de 2016, artículo 2.6.4.4., en relación con el intercambio de información que se realiza a través del programa PORTNODE; lo cual, de acuerdo con la C.R.C. en respuesta a la solicitud realizada por parte de este Despacho, se trata de una solución bajo el esquema All Call Query (“ACQ”) de dos niveles¹¹, lo cual significa que se trata de una arquitectura centralizada con una base de datos nacional de referencia de portabilidad administrada por ABD, y Bases de Datos Operacionales (“BDO”) administrada por los PRSTM y que para su interacción se surta, se usa un programa cliente denominado PORTANODE. Esta información es enviada al ADB para actualización de la DBA.

Aunado a todo lo anteriormente expuesto, la C.R.C. Resolución 5050 de 2016, artículos 2.6.3.3.2.6. y 2.6.11.4., respectivamente, establecieron la obligación para el ABD y los PRSTM, bajo condiciones no discriminatorias, acceso al servicio de administración de la base de datos de portabilidad numérica a otros PRSTM, lo cual puede ser interpretado como la posibilidad, para todos los PRSTM, de acceso a datos mínimos dentro de las bases de datos, lo cual, incluye, pero sin limitarse, al menos a la totalidad de los números telefónicos de los usuarios inscritos en cualquier modalidad de cada uno de los PRSTM y recolectados, puesto que los datos a que hace referencia el artículo 2.6.4.4. solo se solicitan al momento de la solicitud efectiva de portabilidad numérica, por lo que le es posible a todos los PRSTM consultar la totalidad de los números telefónicos de los usuarios de cada PRSTM como base mínima de la BDA.

El siguiente cuadro simplifica la interacción entre la BDO y la BDA, y los datos a que tienen acceso los PSRTM en las diferentes etapas del proceso de portabilidad:



Fuente: Elaboración del Despacho

Frente a esta información, así como toda aquellas que se recolecta por parte de los PRSTM, la C.R.C. Resolución 5050 de 2016 estableció tres mecanismos que limita el uso de la información que se recolecte por parte de los PRSTM, uno general, aplicable a cualquier actividad que realice los PRSTM, y dos específicos para efectos de la portabilidad numérica. El primero, se encuentra dentro de la C.R.C. Resolución 5050 de 2016, artículos 2.1.1.8., el cual estableció lo siguiente:

“Los datos personales podrán ser intercambiados con otros proveedores de servicios de comunicaciones sólo para efectos de la prevención y control de fraudes en las comunicaciones y el cumplimiento de las disposiciones legales y regulatorias que así lo exijan. En todo caso, por tratarse de tratamiento de datos personales, se requerirá la autorización expresa del titular para este fin, la cual podrá obtenerse de manera expresa desde la firma del contrato.”

¹¹ Ver Documento Análisis para la implementación de la Portabilidad Numérica en Colombia, planteamientos generales sobre esquemas de implementación expedido por la Comisión de Regulación de Comunicaciones.

“Por la cual se impone una sanción y se imparte órdenes administrativas”

En cuanto a los específicos, la C.R.C. Resolución 5050 de 2016, artículo 2.6.7.3., estableció como deberes específicos del ABD, por una parte, mantener la confidencialidad de la información de los procesos de portación cuando dicha información, por disposición legal, tenga el carácter de confidencial o reservado; por otra parte, garantizar en todo momento la reserva de la información de la BDA, solo pudiendo utilizar, extensible para los PRSTM, la información que allí se recolecta para los fines específicos de la portabilidad numérica.

De esta manera, se concluye que las bases de datos de portabilidad numérica son de acceso restringido -solo puede ser accedida por el ABD o aquellos que detenten la calidad de PRST, a través de PORTANODE, y con una finalidad específica, portabilidad numérica a solicitud del titular, donde se recolecta y trata información personal¹² dependiendo de si se realiza la solicitud de portabilidad numérica, pero que consultada puede identificar al sujeto a través de la marcación del número registrado con el mero ingreso a la base de datos administrativa. Por lo que cualquier tratamiento adicional que se haga con dicha información, deberá solicitar nuevamente la autorización del titular para dichos efectos.

7.1.2. Bases de datos de Datos Positiva y Negativa (Ley 1453 de 2011 y C.R.C. Resolución 5050 de 2016)

De conformidad con la Ley 1453 de 2011 y la C.R.C. Resolución 5050 de 2016, la base de datos positiva y negativa tiene origen en la incorporación del tipo penal “Manipulación de equipos terminales móviles”, cuyo objetivo es la mitigación de las conductas delictivas de reprogramación, remarcación, o modificación del número de identificación de los equipos terminales móviles. Así mismo, la Ley 1453 de 2011, artículo 22, numeral (21), le entregó a la C.R.C. la facultad de *“(. . .) definir las condiciones y características de bases de datos, tanto positivas como negativas, que contengan la información de identificación de equipos terminales móviles, así como establecer las obligaciones de los proveedores de redes y servicios de comunicaciones, comercializadores, distribuidores o cualquier comerciante de equipos terminales móviles, y las relativas al reporte de la información de identificación de dichos equipos ante la CRC y al suministro de esta información a los usuarios.”*

Así mismo, Ley 1453 de 2011 indicó expresamente lo siguiente sobre dichas bases de datos *“Las bases de datos de que trata el presente numeral, deberán ser implementadas y administrativas <sic> de manera centralizada, a través de un tercero, por parte de los proveedores de redes y servicios de comunicaciones y la información consignada en dichas bases de datos tendrá carácter público, sin perjuicio de la información que contenga datos personales, la cual será protegida de conformidad con lo establecido por la ley.”*, por lo que la C.R.C. solo se encarga de fijar las características técnicas de las bases de datos.

Para el efecto, de acuerdo con la normativa vigente¹³, y tal como lo explicó la C.R.C. ¹⁴, se designó a la compañía “Informática El Corte Inglés – IECISA” para que fungiera como Administrador de Base de Datos (“ABD”), y cuya función principal es permitir la interconexión entre la Base de Datos Centralizada (“BDA”) y las Bases de Datos Operativas (“BDO”), de propiedad de los Proveedores de Redes y de Servicios de Telecomunicaciones (“PRSTM”)¹⁵, entre los cuales se encuentra CLARO y los terceros interesados.

La finalidad específica asignada por la C.R.C. Resolución 5050 de 2016, artículo 2.7.1.1., es la siguiente:

“[L]a restricción de la operación en las redes de telecomunicaciones móviles de los equipos terminales móviles reportados como hurtados y/o extraviados, en cumplimiento de lo dispuesto en el TÍTULO 11 del Decreto 1078 de 2015 y los artículos 105 y 106 de la Ley 1453 de 2011.

Las disposiciones previstas en el CAPÍTULO 7 de TÍTULO II aplican a los Proveedores de Redes y Servicios de

¹² L.1581/12, art. 3(c): Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

¹³ Ibidem.

¹⁴ Radicados 18 -127153 - - 27 del 27 de mayo de 2020 y 18 -127153 - - 30 del 1 de junio de 2020.

¹⁵ D.1078/15, art. 2.2.11.5.

“Por la cual se impone una sanción y se imparte órdenes administrativas”

Telecomunicaciones Móviles y al Administrador de la Base de Datos, de conformidad con lo previsto en el presente CAPÍTULO, así como a todos los usuarios de servicios prestados por los Proveedores de Redes y Servicios de Telecomunicaciones Móviles.

Para el cumplimiento de esta finalidad las bases de datos positiva y negativa se encuentra estructurada de la siguiente manera, a saber: (i) **Base de Datos Positiva:** “[E]sta base contendrá la información correspondiente a IMEI-IMSI-MSISDN de los equipos terminales móviles registrados dando cumplimiento al proceso de registro de IMEI dispuesto en el artículo 2.7.3.4, el cual entre otros aspectos, como parte del procedimiento de registro de IMEI y en **forma previa al registro de los datos personales del usuario, el PRSTM deberá solicitar al usuario su autorización para el tratamiento de la información de sus datos personales, conforme a las reglas previstas en el Decreto 1377 de 2013.**¹⁶ (Negrilla fuera del texto), y; (ii) **Base de Datos Negativa:** “[L]a función de las Bases de Datos Negativas es llevar un registro de los equipos terminales móviles que no pueden ser habilitados en las redes de los PRSTM por haber sido reportados como hurtados y/o extraviados por parte del propietario del equipo terminal móvil o el propietario autorizado por este, por ser detectados con un IMEI sin formato, inválidos, no homologados, duplicados o no estar registrados en la Base de Datos Positiva.”¹⁷

En referencia al mecanismo de acceso a las bases de datos negativa y positiva para los PSRTM, el Corte Inglés, en respuesta¹⁸ a la solicitud de información¹⁹ realizada en la etapa de pruebas, indicó que “ofrece la solución cliente llamada MobLystNode o SRTMNode, software que permite al operador móvil interactuar con el ente central de IMEIs para el intercambio de mensajería para dar cumplimiento a los distintos procesos regulatorios para el control de hurto de terminales en base de datos positiva y negativa.” En este punto es necesario aclarar que la SIC debe modular su posición en referencia a la imputación de cargos, por cuanto el aplicativo para acceder a las bases de datos positiva y negativa, no es PORTANODE, sino MobLystNode o SRTMNode, por lo que la sanción debe centrarse en escatimar, teniendo en cuenta las pruebas, si la información contenida en las bases de datos de portabilidad numérica fue utilizada con una finalidad distinta a la fijada por la Ley.

Dicho lo anterior, debe indicarse que, en materia de privacidad y protección de datos sobre los datos contenidos en las bases de datos positiva y negativa, la C.R.C. R. 5050/16 estableció los siguientes mecanismos: (i) el PRSTM debe solicitar, en los términos de la Ley 1581 de 2012 y el Decreto 1377 de 2013, autorización por parte del usuario, con consentimiento previo, expreso e informado, a través del medio que considere idóneo, para que la información que constituya un dato personal pueda ser remitida a las autoridades competentes; (ii) el ABD debe garantizar la protección de los datos personales almacenados en la BDA, los cuales podrán ser utilizados únicamente para los fines establecidos en la C.R.C. Resolución 5050 de 2016.

En conclusión, las bases de datos positiva y negativas de acceso restringido exclusivo para los PRSTM, el ABD, y algunas entidades públicas definidas por la Resolución 5050 de 2016, artículo 2.7.3.6., “(. . .) el Ministerio de Tecnologías de la Información y las Comunicaciones, la Superintendencia de Industria y Comercio y la CRC, así como las autoridades policivas y judiciales, podrán consultar en línea la información consignada en la Base de Datos Negativa y en la Base de Datos Positiva, en forma exacta y actualizada, registro a registro”; y cuya finalidad se limita a “[L]a restricción de la operación en las redes de telecomunicaciones móviles de los equipos terminales móviles reportados como hurtados y/o extraviados, por lo que otro uso requeriría al solitud de una nueva autorización por parte del PRSTM, de lo contrario, sería un uso ilegal.

7.2. Sobre la supuesta violación al debido proceso por imposibilidad de acceso al expediente.

La sociedad investigada indicó en los siguientes radicados: 18 – 127153 - - 47 del 22 de julio de 2020, 18 – 127153 - - 105 del 2 de octubre de 2020, 18 – 127153 - - 129 del 8 de abril de 2021, que la SIC violó su derecho fundamental al debido proceso, en especial al de contradicción, toda vez que no se le ha suministrado en forma el acceso al expediente digital y

¹⁶ Op.Cit., respuesta al cuestionamiento 4 de la SIC.

¹⁷ Ibidem.

¹⁸ Radicado 18- 127153 - - 126 del 12 de febrero de 2020.

¹⁹ Radicado 18 – 127153 - - 124 del noviembre de 2020.

“Por la cual se impone una sanción y se imparte órdenes administrativas”

físico.

Al referente, resulta importante indicar que el derecho al debido proceso establecido en la Constitución Política (“C.P.”), art. 29, es un eje fundamental de la actuación administrativa, lo cual permea la actuación obligando a la administración a garantizarlo en cada una de las etapas del proceso administrativo -previa ley habilitante-; y el cual, en materia de la posibilidad de contradicción y aporte de pruebas, debe sujetarse a lo siguiente:

“i.) La efectividad de ese derecho en las instancias administrativas supone la posibilidad de que el administrado interesado en la decisión final que se adopte con respecto de sus derechos e intereses, pueda cuestionarla y presentar pruebas, así como controvertir las que se alleguen en su contra (CP, art. 29), pues, a juicio de la Corte, de esta forma se permite racionalizar el proceso de toma de decisiones administrativas, en tanto que ello evidentemente constituye un límite para evitar la arbitrariedad del poder público (. . .)”²⁰

Por tanto, teniendo en cuenta lo anterior, y por habilitación del C.P.A.C.A., art. 53 – 64, la SIC habilitó el Sistema de Trámites por medio del cual se puede llevar a cabo los procedimientos administrativos a través de medios electrónicos; sobre lo cual toca se pone especial énfasis al contenido de los artículo 58 y 59, los cuales permiten que los procedimientos administrativos de adelanten a través de medios electrónicos donde se podrán almacenar todos los documentos de la actuación asegurando la autenticidad y veracidad para su reproducción. Sin embargo, el artículo 54 del C.P.A.C.A., estableció que toda persona tiene derecho a actuar frente a las autoridades administrativas utilizando los medios electrónicos, para lo cual tendrá que registrar su correo electrónico en la base de datos dispuesta para el efecto. Lo anterior debe articularse con las condiciones de acceso al expediente expedidas por la SIC a través de la Resolución 28182 de 2020 debido a la emergencia económica, social y ecológica causada por el COVID-19, por lo que ordenó que *“(. . .) el trámite de las actuaciones administrativas sancionatorias y disciplinarias que se surten ante las dependencias de esta Superintendencia, durante la vigencia de la emergencia sanitaria decretada por el Ministerio de Salud, se adelantará de manera virtual a través de las tecnologías de la información y las comunicaciones, incluida la asistencia a audiencias.”* De esta manera, se estableció los mecanismos de las tecnologías de la información y las comunicaciones para que los ciudadanos e investigados pudieran consultar los expedientes.

Sin embargo, tal como ya se indicó, para la consulta se requirió un registro ante el correo contactenos@sic.gov.co, y de forma adicional para las investigaciones surtidas por este Despacho, habeasdata@sic.gov.co, con lo cual se hacía el registro ante la base de datos del aplicativo de consulta. Procedimiento que se le informó en cada etapa de la actuación administrativa. A esto debe aunársele que en las actuaciones administrativas sancionatorias, el deber la autoridad, para garantizar el derecho fundamental al debido proceso, y su instrumentalización a través del acceso al expediente, se ve concretizado en prestar los medios físicos y digitales para su consulta, pero es deber de la parte cumplir con el deber de registro y realizar la consulta, pues en el derecho administrativo no es deber de la entidad dar copias del expediente de la actuación a los investigados adjuntas a las actuaciones administrativas, sino procurar los medios para que este, como deber procesal, realice la consulta del expediente por sus propios medios, en virtud del C.P.C.A., artículos 5, numeral (2) y 7, numeral (9), los cuales establecen claramente que es derecho para los ciudadanos/investigados y deber de las entidades públicas, tal como la SIC, proveer los medios para que los ciudadanos/investigados puedan consultar o revisar el expediente, no por ello remitir piezas del expediente en particular²¹, salvo aquellas donde se requiera notificación personal.

En el caso concreto, CLARO a través del radicado 18 – 127153 - - 47 del 22 de julio de 2020, solicitaron como garantías procesales lo siguiente: (i) teniendo en cuenta el contenido de los Decreto 417 de 2020, Decreto 491 de 2020, y Resolución 19831 de 2020, esta última proferida por la SIC en relación a los proceso jurisdiccionales de competencia desleal y propiedad industrial, remitir copia integral digital del expediente a la dirección electrónica para notificaciones judiciales, esto es,

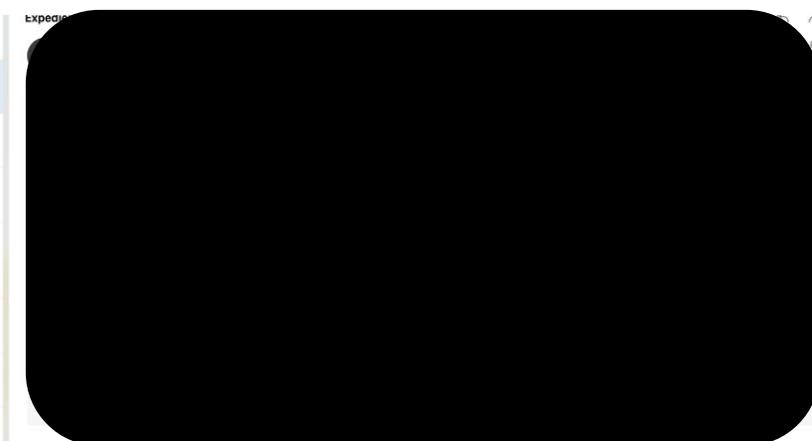
²⁰ Corte Constitucional [C.C.] Sentencia C-034/14, M.P. María Victoria Correa Calle, Gaceta de la Corte Constitucional [G. C. C.] (Vol. n/d, p. 5) (Colom.) (citando la sentencia T-1341/01 sobre la aplicación del debido proceso a las actuaciones administrativas para evitar la arbitrariedad de la administración).

²¹ Nótese del lenguaje del C.P.A.C.A., art. 5 (1) que las actuaciones que surten las entidades públicas pueden ser adelantadas o promovidas por cualquier medio tecnológico o electrónico disponible en la entidad, razón por la cual en el caso en concreto, para garantizar el derecho al debido proceso, en especial el derecho al acceso al expediente, se permitió el acceso a través de dos mecanismos: (1) acceso al expediente a través del aplicativo de consulta previo registro, y; (2) consulta del expediente a través del drive de Google de la entidad con permiso de acceso al correo de notificaciones del

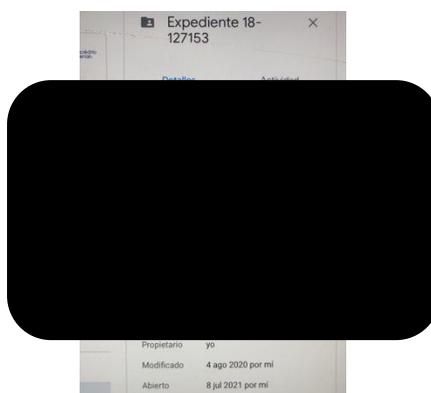
“Por la cual se impone una sanción y se imparte órdenes administrativas”

notificacionesclaromovil@claro.com.co; (ii) Suspender los términos en cuanto no tiene acceso a la totalidad del expediente. En virtud de esta solicitud, a través de radicado 18 -127153 - - 54 del 3 de agosto de 2020, el Despacho le indicó a CLARO lo siguiente: (i) la Resolución 19831 de 2020 aplicó solo para los procesos jurisdiccionales en conocimiento de la SIC, por lo que materia de actuaciones administrativas, como la presente, se emitió la Resolución 121169 de 2020; la cual suspendió a partir del 1 de abril de 2020 los términos para actuaciones administrativas avocadas ante la SIC, incluyendo los términos para la caducidad; (ii) la Resolución 28182 de 2020 reanudó a partir del 16 de junio 2020 los términos de las actuaciones administrativas sancionatorias y disciplinarias que se surten en cualquier dependencia de la Entidad; (iii) la Resolución 28182 de 20, artículos 2 y 3, estableció la prestación de servicios de manera virtual y presencial pero bajo el estricto seguimiento de los protocolos de bioseguridad; (iv) En razón de la Resolución 28182 de 2020, y a partir de la notificación de la resolución de imputación de cargos del presente caso, CLARO ha tenido la posibilidad de tener acceso al expediente digital y físico; (v) adicionalmente, para garantizar el derecho al acceso al expediente, y de esta manera la debido proceso, el expediente y su piezas físicas se digitalizaron en el google drive y se le dio acceso al correo de notificaciones de CLARO: notificacionesclaromovil@claro.com.co; (vi) así mismo, se le permitió el acceso físico al expediente con visita programada el día 5 e agosto de 2020 a las 10 am., y a la cual asistió uno de sus abogados, el cual sacó copia del expediente.

Así mismo, habiéndose otorgado el permiso al correo de notificaciones de Claro, la persona encargada de su manejo se contactó con la SIC el 4 de agosto de 2020 para que se le otorgara permiso a su correo personal en los siguientes términos:



Como se observa en la siguiente captura de pantalla, la funcionaria tuvo acceso al expediente digital desde la misma fecha; por lo que, en consecuencia, CLARO tuvo acceso al expediente desde el inicio de la actuación:



Por tanto, desde el 4 de agosto de 2020, CLARO como investigada, tuvo acceso a la copia del expediente físico contenido en el drive de google de la entidad para su consulta. De igual forma, el 5 de agosto de 2020, se le permitió a uno de los abogados de CLARO la revisión integral del expediente físico, con las actuaciones surtidas a la fecha, con el fin de que pudiera tener elementos de juicio para poder ejercer su derecho a la defensa, lo cual, junto con el acceso digital en el portal de la entidad y la copia en el drive de Google de la entidad, garantiza el derecho al debido proceso y contradicción de la investigada desde el inicio de la investigación administrativa con la imputación de cargos.

Así mismo, y teniendo en cuenta la solicitud de acceso al expediente realizada por los terceros interesados, y para garantizar el derecho al debido proceso y derecho de contradicción,

“Por la cual se impone una sanción y se imparte órdenes administrativas”

nuevamente se les indicó como tener acceso al expediente, para lo cual se les indicó el siguiente procedimiento para dicho acceso:

“(1) Enviar un correo electrónico a contactenos@sic.gov.co o habeasdata@sic.gov.co, solicitando el acceso al expediente a través de la plataforma servicios en línea, indicando: número de radicado, nombre completo de la persona que va a consultar el expediente, número de identificación y correo electrónico autorizado;

(2) Una vez reciba respuesta positiva respecto de la solicitud de acceso, la sociedad debe registrarse en servicios en línea link <https://servicioslinea.sic.gov.co/servilinea/ServiLinea/Portada.php> y a través del mismo link posteriormente al registro puede consultar el expediente de manera digital.”²²

De igual forma, reiterando la posición del despacho de permitir el acceso al expediente a las partes por todos los medios legalmente establecidos para el efecto, se le confirmo a las partes, incluyendo CLARO, la posibilidad de acceso al expediente ubicado en el drive de Google de la entidad, para lo cual solo requerían enviar un correo electrónico en los términos establecidos en el numeral (1) del radicado 18 – 127153 - - 108 del 14 de octubre de 2020. De esta manera, la SIC buscó garantizar el derecho al debido proceso, en especial el de contradicción de CLARO, así como de las partes terceras interesadas en la actuación del radicado. El contenido del anterior documento, nuevamente le fue enviado a CLARO a través del radicado 18 – 127153 - - 109 del 14 de octubre de 2020, sin que se hayan manifestado al referente.

La SIC, procurando siempre el acceso al expediente, en la resolución 64874/20, por medio de la cual se incorporaron pruebas, se rechazan unas y se decretas otras, se decidió en el considerando noveno que CLARO, así como los terceros interesados, podrían tener acceso al expediente sometiéndose al siguiente procedimiento, a saber:

“(. . .) Que en virtud de la situación actual, teniendo en cuenta el Estado de Emergencia Económica, Social y Ecológica decretado por el Gobierno Nacional, se ha restringido el ingreso a las instalaciones de la Superintendencia, en consecuencia, se establecieron las medidas pertinentes para permitir el acceso completo a los expedientes, por lo que las sociedades CLARO, AVANTEL y TIGO deberán:

- (i) Una vez reciba respuesta positiva respecto de la solicitud de acceso, la sociedad debe registrarse en servicios en línea link <https://servicioslinea.sic.gov.co/servilinea/ServiLinea/Portada.php> y a través del mismo link posteriormente al registro puede consultar el expediente de manera digital;*
- (ii) Enviar un correo electrónico a contactenos@sic.gov.co o habeasdata@sic.gov.co, solicitando el acceso al expediente a través de la plataforma servicios en línea, indicando: número de radicado, nombre completo de la persona que va a consultar el expediente, número de identificación y correo electrónico autorizado.*

No obstante, en aras de garantizar los derechos de defensa y contradicción de la sociedad investigada, en el caso en que la misma considere necesario el acceso del expediente en físico, deberá enviar un correo electrónico a la dirección de correo habeasdata@sic.gov.co, solicitando que le asignen una cita para que pueda examinar el expediente, con el número de la referencia, en las instalaciones de la Superintendencia de Industria y Comercio en la ciudad de Bogotá. Lo anterior por cuanto se deben garantizar el ingreso a las instalaciones con las adecuadas medidas de bioseguridad. Lo anterior sin perjuicio que se adopte cualquier otra medida especial y excepcional para la revisión del expediente por parte de la investigada y los terceros interesados.”

Se reitera entonces el interés de este Despacho de garantizar el derecho fundamental al debido proceso, en especial el derecho contradicción, permitiéndole a CLARO, como investigada, y dentro de las circunstancias fijadas por la Emergencia económica, social y ecológica creada por el COVID-19, acceso constante al expediente a través de medios

²² 18-127153 - - 108 del 14 de octubre de 2020, p. 1.

“Por la cual se impone una sanción y se imparte órdenes administrativas”

virtuales, incluyendo, el acceso físico previo agendamiento de cita en acatamiento de las medidas de bioseguridad establecidas por la Entidad para el efecto. Aunado a lo anterior, es necesario poner en evidencia que el contenido de la resolución 64874 de 2020 fue debidamente notificado a CLARO tal como lo prueban los radicado 18 – 127153 - - 116 del 16 de octubre de 2020 y 18 – 127153 - - 118 del 9 de noviembre de 2020, dejando en evidencia que el acuse de recibo del mencionado Acto Administrativo el 16 de octubre de 2020, con lo cual CLARO sabía sobre la metodología de acceso al expediente, sin perjuicio del acceso ya concedido desde la notificación de la resolución de imputación de cargos, y el acceso al expediente virtual y las piezas físicas digitalizadas a través del drive de Google de la Entidad.

Una vez practicadas las pruebas y cerrada la etapa probatoria, a través del radicado 18-127153 - - 126 del 7 de abril de 2021, se le corrió traslado para presentar alegatos de conclusión a CLARO, en donde se le indicó nuevamente lo siguiente para garantizar el acceso al expediente:

“(. . .) Así las cosas, y en virtud de la situación actual, teniendo en cuenta el Estado de Emergencia Económica, Social y Ecológica decretado por el Gobierno Nacional, se ha restringido el ingreso a las instalaciones de la Superintendencia, en consecuencia, se establecieron las medidas pertinentes para permitir el acceso completo a los expedientes, por lo que la sociedad debe:

(i) enviar un correo electrónico a contactenos@sic.gov.co o habeasdata@sic.gov.co, solicitando el acceso al expediente a través de la plataforma servicios en línea, indicando el número de radicado del expediente;

(ii) una vez reciba respuesta respecto de la solicitud de acceso, la sociedad debe registrarse en servicios en línea link <https://servicioslinea.sic.gov.co/servilinea/ServiLinea/Portada.php> y a través del mismo link posteriormente al registro puede consultar el expediente digitalmente.

No obstante, en aras de garantizar los derechos de defensa y contradicción de la sociedad, en el caso en que la misma considere necesario el acceso del expediente en físico, deberá enviar un correo electrónico a la dirección de correo habeasdata@sic.gov.co, solicitando que le asignen una cita para que pueda examinar el expediente, con el número de la referencia, en las instalaciones de la Superintendencia de Industria y Comercio en la ciudad de Bogotá. Lo anterior por cuanto se deben garantizar el ingreso a las instalaciones con las adecuadas medidas de bioseguridad.”

A pesar de estas garantías de acceso al expediente, habilitadas desde el inicio de la actuación administrativa sancionatoria, y reiteradas en cada etapa de este, CLARO por intermedio de su representante legal, FERNANDO ANDRÉS PERDOMO CORDOBA (el “Representante Legal”), solicitó a través del radicado 18 -127153 - - 129 del 8 de abril de 2021, acceso al expediente digital por intermedio de su correo electrónico corporativo; razón por la cual este Despacho, mediante el radicado 19-127153- - 130 del 12 de abril de 2021, se le informó lo siguiente:

“(. . .) En virtud de la situación actual, teniendo en cuenta el Estado de Emergencia Económica, Social y Ecológica decretado por el Gobierno Nacional, se ha restringido el ingreso a las instalaciones de la Superintendencia, en consecuencia, se establecieron las medidas pertinentes para permitir el acceso completo a los expedientes, por lo que la sociedad debe:

(i) Enviar un correo electrónico a contactenos@sic.gov.co o habeasdata@sic.gov.co, solicitando el acceso al expediente a través de la plataforma servicios en línea, indicando: número de radicado, nombre completo de la persona que va a consultar el expediente, número de identificación y correo electrónico autorizado;

(ii) (ii) Una vez reciba respuesta positiva respecto de la solicitud de acceso, la sociedad debe registrarse en servicios en línea link <https://servicioslinea.sic.gov.co/servilinea/ServiLinea/P>

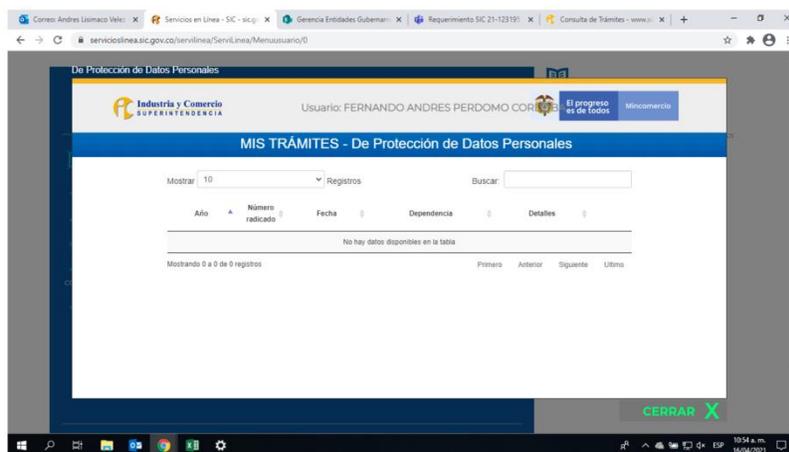
“Por la cual se impone una sanción y se imparte órdenes administrativas”

ortada.php y a través del mismo link posteriormente al registro puede consultar el expediente de manera digital.

En todo caso, se aclara que la sociedad comercial CLARO, tal como establece el radicado 18 -127153 - - 54 del 3 de agosto de 2020, actualmente posee acceso digital al expediente mediante el correo: notificacionesclaromovil@claro.com.co, y con este mismo, acceso a la copia del expediente en Google Drive de la Entidad.

No obstante lo anterior, en aras de garantizar los derechos de defensa y contradicción de la sociedad comercial CLARO, en el caso en que la misma considere necesario el acceso del expediente en físico, deberá enviar un correo electrónico a la dirección de correo habeasdata@sic.gov.co, solicitando que le asignen una cita para que pueda examinar el expediente, con el número de la referencia, en las instalaciones de la Superintendencia de Industria y Comercio en la ciudad de Bogotá. Lo anterior por cuanto se deben garantizar el ingreso a las instalaciones con las adecuadas medidas de bioseguridad.”

A pesar de las habilitaciones dadas para el acceso al expediente, mediante el radicado 18 – 127153 - - 131 del 16 de abril de 2021, el Representante Legal de CLARO manifestó: (i) “. . .) el correo del 8 de abril de 2021 fue el correo donde solicitamos el acceso al expediente de la referencia, incluso en dicho correo se encuentra toda la información que ustedes requieren para el acceso (Numero de radicado del expediente, nombre completo de la persona que consulta, número de identificación y correo electrónico autorizado), sin embargo, una vez ingresamos a la plataforma virtual con dicho correo y contraseña, no se visualiza el expediente 18-127153, tal y como lo demuestra el siguiente pantallazo:



(. . .) No hemos recibido respuesta positiva frente a la solicitud de acceso al correo [REDACTED]; (ii) En relación con el acceso al expediente a través del drive de google de la Entidad y el servicio web de la entidad, no fue posible el acceso a estos mediante el correo: notificacionesclaromovil@claro.com.co. Razón por la cual solicitó nuevamente a la plataforma de servicios de la SIC con el correo del apoderado de CLARO, y; (iii) también solicitó cita presencial para el lunes 19 de abril 2021, en el entendido de que el plazo para presentar alegatos de conclusión culminaba el 21 de abril de 2021, y el acceso al expediente, particularmente para el representante legal de la sociedad, se solicitó desde el 8 de abril de 2021.

Al respecto, la SIC mediante radicado 18-127153 - - 133 del 20 de abril de 2021, y a pesar de que el Representante Legal de CLARO no cumplió el procedimiento para dar acceso al expediente, se le concedió a partir del 19 de junio de 2020 acceso a la plataforma de la SIC para su consulta. De igual forma, se le programó visita para la revisar físicamente el expediente en las instalaciones de la SIC el día 22 de abril de 2021 en la franja entre 9 am y 11 am, y a la cual se abstuvo de presentarse.

Se le suma a lo anterior que, en el radicado 18 – 127153 – 135 del 22 de abril de 2021, por medio del cual presentaron alegatos de conclusión, CLARO indicó en la sección segunda de su escrito que la SIC violó el derecho al debido proceso por imposibilidad de acceso oportuno al expediente toda vez que: (i) la sociedad solo obtuvo acceso al expediente hasta el 20 de

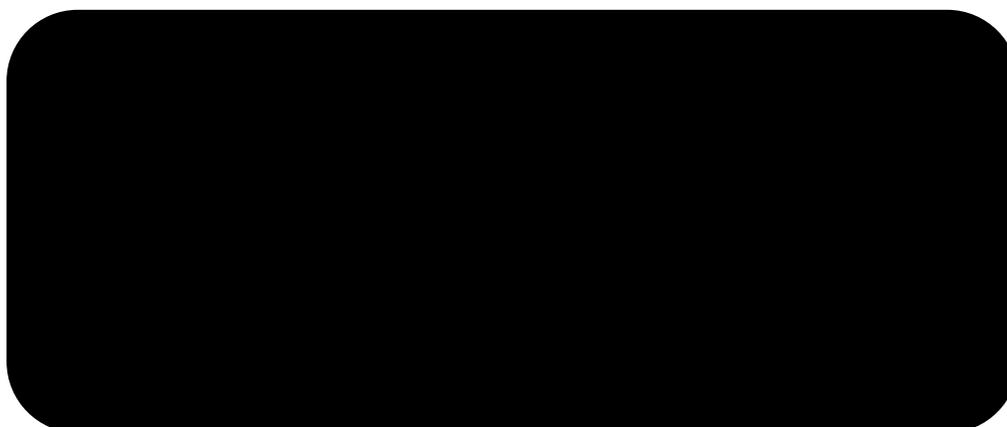
“Por la cual se impone una sanción y se imparte órdenes administrativas”

abril de 2021 a pesar de las múltiples solicitudes de acceso al expediente digital y físico, por lo que dejan constancia de la radicación de la solicitud del 8 de abril de 2021, donde se solicitó el acceso para el Representante Legal de la sociedad, y cuya respuesta fue obviada por parte de la SIC en la respuesta del 12 de abril de 2021 a pesar de haber cumplido los requisitos para el acceso de forma previa; (ii) La SIC advirtió que CLARO tenía acceso al expediente digital a través del correo de notificaciones de CLARO, notificacionesclaromovil@claro.com.co; sin embargo, también se intentó el ingreso con este correo y no fue posible realizar la revisión del expediente, y (iii) debido a esta imposibilidad, solicitó urgente acceso al expediente a través del correo del representante legal, y cita presencial en las instalaciones de la Superintendencia el 22 de abril de 2021, siendo que los alegatos de conclusión debían presentarse máximo el 21 de abril de 2021, lo cual le parece una grave transgresión al debido proceso que le asiste a CLARO como investigada.

De todo lo anteriormente expuesto, lleva a concluir que la SIC, teniendo en cuenta las circunstancias especiales creadas por el COVID-19, garantizó el derecho al acceso al expediente de la investigada CLARO en tanto, en cumplimiento de sus deberes constitucionales y legales, prestó los medios -físicos y electrónicos- necesarios para que ésta pudiera ejercer su derecho al acceso al expediente, y por ende de contradicción desde el radicado 18 – 127153 - - 54 del 3 de agosto de 2020, permitiendo el acceso a la totalidad del expediente a través del drive Google de la entidad, así como a través de visita a las instalaciones de la SIC el día 5 de agosto de 2020, a la cual asistió uno de los abogados del área jurídica de CLARO, y el cual saco copia integral del expediente físico, con el fin de poder ejercer el derecho de contradicción a pesar de la habilitación dada a través del Google Drive de la Entidad²³, así como el 22 de abril de 2021, a la cual se abstuvo de presentarse.

Este derecho al acceso al expediente se vio extendido, una vez la Entidad fijó las pautas definitivas de acceso a la plataforma digital, para que de forma permanente y en tiempo real los investigados tuvieran acceso a cada actuación administrativa que se iba surtiendo, sin perjuicio de aquellas que se debían hacer por notificación personal, aviso o comunicación; lo cual, en el caso del presente, se vio concretizado a través radicado 18-127153 - - 109 del 14 de octubre de 2020, con lo cual, como ya se indicó arriba, se permitió el acceso al expediente, pero sujeto al registro por parte de CLARO, y los terceros intervinientes; lo cual no ocurrió en el caso de CLARO, y la solicitud efectiva solo ocurrió, bien como la manifestó CLARO en sus alegatos de conclusión, el día 8 de abril de 2021 para el Representante Legal de la sociedad, Fernando Andrés Perdomo Córdoba, a través de su correo corporativo; razón por la cual el 12 de abril de 2021, se les recordó el procedimiento de acceso, y se les reiteró que también tenían acceso al expediente a través del drive de Google de la entidad. Cabe destacar que, contraria a las manifestaciones de CLARO, no se reportó solicitud de acceso a este medio en ninguna etapa del proceso del proceso, con excepción de aquel solicitado por parte de la encargada de la gestión del correo de notificaciones de CLARO.

De este modo, en virtud de la solicitud hecha el 16 de abril de 2021, y sin cumplir con el lleno de los requisitos establecidos para el acceso al expediente digital, el 20 de abril se le dio acceso al expediente al correo del representante legal, así como la asignación de la visita el día 22 de abril de 2021, en estricta observancia de las normas de bioseguridad, visita a la cual se abstuvo de presentarse. A continuación, se deja constancia de que se dio acceso al expediente digital al representante legal de la sociedad desde el 19 de abril de 2021:



²³ Debe resaltarse los siguientes puntos importantes referente al acceso al a través del Google: (1) se le envió la autorización de ingreso al correo de notificaciones de Claro; (2) la persona encargada de la gestión del correo solicitó el acceso a su correo personal y se le concedió; (3) Claro no solicitó jamás acceso a través del correo de notificaciones durante ninguna de las etapas del proceso.

“Por la cual se impone una sanción y se imparte órdenes administrativas”

De esta forma, se evidencia que la SIC, en el transcurso de la actuación²⁴ administrativa garantizó el derecho al debido proceso de CLARO como investigada, el acceso al expediente, dejando claro que fue deber de esta realizar la consultas a través de los mecanismos dispuestos por parte de la entidad²⁵, y lo cual se abstuvo de realizar sino hasta entrada la etapa de alegatos de conclusión.

Por lo tanto, teniendo en cuenta la importancia que tiene la cláusula del debido proceso dentro de las actuaciones administrativas, en especial lo referente al derecho de contradicción, que incluye la posibilidad de conocer el expediente, se le garantizó a los ciudadanos/investigados de la presente actuación, el acceso al expediente a través de dos mecanismos de consulta: (1) consulta a través del aplicativo de consulta en línea condicionado al registro a la base de datos de la SIC para efectos de autorización, y; (2) visita programada para revisión del expediente. Estos elementos fueron advertidos en cada una de las etapas. Frente a la primera, se le informó a través de los siguientes radicados: (i) 18-127153 - - 54 del 3 de agosto de 2020; (ii) 18 - 127153 - - 108 del 14 de octubre de 2020; (iii) 18 - 127153 - - 107 a 110 del 14 de octubre de 2020; (iv) R.64874/20; (v) 18-128153 - - 126 del 7 de abril de 2021; (vi) 18 -127153 - - 130 del 12 de abril de 2020, y (vii) 18-127153 - - 133 del 20 de abril de 2020, lo cual incluyó un acceso al expediente digitalizado a través del drive de Google de la entidad. En relación con los accesos, se requirió a la mesa de ayuda de la SIC información si existió solicitud de acceso remoto distintos a los solicitados por parte del Representante legal, siendo la respuesta negativa; por lo que el único acceso solicitado fue aquel realizado por el Representante Legal de la sociedad, el 8 de abril de 2021 y 16 de abril de 2021. Frente al segundo, se le permitió el acceso al expediente, teniendo en cuenta las circunstancias especiales creadas por el COVID-19, en las siguientes fechas por solicitud propia de CLARO: (i) 5 de agosto de 2020 (Rad. 18 - 127153 - - 54 del 3 de agosto de 2020), y; (ii) 22 de abril de 2022 (Rad. 18 - 127 153 - - 133 del 20 de abril de 2021) a la cual no asistió. Aún sí Claro presentó sus alegatos de conclusión contravirtiendo los cargos presentados, y utilizando las pruebas decretadas por el Despacho como parte de su defensa.

En suma, se advierte que la SIC, dentro de la actuación 18-127153, tomó las medidas necesarias para garantizar el derecho al debido proceso, incluyendo el de contradicción, a través del acceso al expediente mediante los mecanismos arriba descritos, y fue deber de CLARO tomar las medidas necesarias para poder hacer la revisión del expediente a través de dichos mecanismos habilitados en virtud del COVID-19 y las medidas tomadas por parte del Gobierno Nacional para evitar su propagación en las actividades administrativas, incluyendo, pero sin limitarse, a las sancionatorias. Lo anterior debe entenderse como la materialización expresa del mandado legal establecido por parte del C.P.A.C.A. en relación con el deber de la administración de habilitar el espacio idóneo para la consulta del expediente y documento, lo cual, en el caso presente, siempre se garantizó a CLARO, como a los terceros interesados, los cuales tuvieron acceso al expediente en las mismas condiciones sin que se hayan manifestado en ninguna etapa de la actuación imposibilidad en el acceso al expediente.

7.3. Adecuación típica

El artículo 19 de la Ley 1581 de 2012 establece la función de vigilancia que le corresponde a la Superintendencia de Industria y Comercio para garantizar que en el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la mencionada Ley.

La Corte Constitucional, mediante sentencia C-748 de 2011²⁶, estableció lo siguiente en relación con el principio de tipicidad en el derecho administrativo sancionatorio:

“En relación con el principio de tipicidad, encuentra la Sala que pese a la generalidad de la ley, es determinable la infracción administrativa en la medida en que se señala que la constituye el incumplimiento de las disposiciones de la ley, esto es, en términos específicos, la regulación que hacen los artículos 17 y

²⁴ Para acceso al expediente se debió agotar el siguiente procedimiento: *“(1) Enviar un correo electrónico a contactenos@sic.gov.co o habeasdata@sic.gov.co, solicitando el acceso al expediente a través de la plataforma servicios en línea, indicando: número de radicado, nombre completo de la persona que va a consultar el expediente, número de identificación y correo electrónico autorizado; (2) Una vez reciba respuesta positiva respecto de la solicitud de acceso, la sociedad debe registrarse en servicios en línea link <https://servicioslinea.sic.gov.co/servilinea/ServiLinea/Portada.php> y a través del mismo link posteriormente al registro puede consultar el expediente de manera digital.”*

²⁵ Los radicados y actos administrativos donde se les manifestó expresamente los mecanismos de acceso al expediente a CLARO fueron los siguientes, a saber: (i) 18-127153 - - 54 del 3 de agosto de 2020; (ii) 18 - 127153 - - 108 del 14 de octubre de 2020; (iii) 18 - 127153 - - 107 a 110 del 14 de octubre de 2020; (iv) R.64874/20; (v) 18-128153 - - 126 del 7 de abril de 2021; (vi) 18 -127153 - - 130 del 12 de abril de 2020, y (vii) 18-127153 - - 133 del 20 de abril de 2020.

²⁶ Corte Constitucional [C.C.] Sentencia C-748/11, M.P. Jorge Ignacio Pretelt Chaljub, Gaceta de la Corte Constitucional [G. C. C.] (Vol. n/d, p. 5) (Colom.).

“Por la cual se impone una sanción y se imparte órdenes administrativas”

18 del proyecto de ley, en los que se señalan los deberes de los responsables y encargados del tratamiento del dato”.

Atendiendo los parámetros indicados por la citada jurisprudencia, para el caso específico se tiene que:

- (i) El artículo 17 de la Ley 1581 de 2012 establece los deberes que les asisten a los responsables del tratamiento respecto del tratamiento de los datos personales de los titulares. El incumplimiento de tales deberes dará lugar a la aplicación de cualquiera de las sanciones definidas en el artículo 23 de la Ley 1581 de 2012;
- (ii) De conformidad con los hechos enunciados, que dieron lugar a la apertura de la presente investigación, y de la preponderancia de la evidencia obrante dentro del expediente, se puede indicar que la conducta desplegada por parte de la sociedad investigada, como responsable, se concreta la vulneración de:
 - Del principio de finalidad (Ley 1581 de 2012, artículo 4, literal (b)) y el deber de informar de forma debida sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada (Ley 1581 de 2012, artículo 17, literal (c)).
 - Del principio de libertad (Ley 1581 de 2012, artículo 4, literal (c)) y el deber de solicitar y conservar copia de la respectiva autorización otorgada por el Titular en los términos establecidos por la ley (Ley 1581 de 2012, artículos 9 y 17, literal (b), Decreto 1377 de 2013, artículos 5, 7, y 8 -incorporado en el Decreto Único Reglamentario 1074 de 2015).

De esta manera, corresponde a este Despacho establecer si la conducta desplegada por la investigada dará lugar o no a la imposición de una sanción para lo cual se deberán tener en cuenta los hechos objeto de investigación, así como las razones de hecho y de derecho aducidas por la investigada en el escrito los alegatos de conclusión, así como el conjunto de pruebas allegadas al expediente, tal como pasará a analizarse a continuación:

7.3.1. Sobre el Principio de finalidad y el deber de informar por parte del responsable a los titulares sobre los derechos que le asisten en virtud de la autorización otorgada.

El artículo 4, literal (b) de la Ley 1581 de 2012, establece como principio orientativo de la actividad de recolección y tratamiento, el de finalidad, el cual obliga a los responsables a que *“El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley, la cual deberá ser informada al titular”*. De forma consecutiva, la misma norma en su artículo 17, literal (c), estableció el deber para el responsable del Tratamiento de los datos de: *“informar debidamente al titular sobre la finalidad de la recolección y de los derechos que le asisten por virtud de la autorización otorgada”*.

De este modo, la Corte Constitucional, en interpretación del principio y deber de finalidad, ha sido enfática en determinar que no es posible la recolección de datos sin un fin legal y legítimo claro, quedando proscrita la recolección de datos sin la clara especificación acerca de su finalidad, o bien, *“(. . .) el uso o divulgación de datos para una finalidad diferente a la inicialmente prevista”*.²⁷ Por tanto, debe entenderse que, en el período de recopilación y posterior tratamiento de los datos, queda prohibido: (i) la recopilación de información personal sin que se establezca el objetivo de su incorporación a la base de datos, y; (ii) la recolección, procesamiento y/o divulgación de la información personal para un propósito diferente al inicialmente previsto y autorizado por el titular de los datos.

A lo anterior debe aunársele que, la finalidad no solo debe ser legítima, sino que la información recolectada debe ser usada para para realizar los fines exclusivos para los cuales fue dada la autorización, previa y expresa, por parte del Titular, o bien, la habilitación legal para la recolección específica; por tanto, cualquier utilización distinta a la previamente indicada, deberá requerirse la autorización expresa por parte del Titular²⁸. En ese sentido, la Corte Constitucional estableció que existe la posibilidad de que sea dificultoso enunciar, de manera amplia y detallada, los usos de la información, dejando la posibilidad de que se realicen tratamientos no autorizados expresamente siempre que sean compatibles con la finalidad principal autorizada; es así como la Corte

²⁷ Corte Constitucional [C.C.] Sentencia T-729/02, M.P. Eduardo Montealegre Lynnett, Gaceta de la Corte Constitucional [G. C. C.] (Vol. n/d, p. 5) (Colom.)

²⁸ Corte Constitucional [C.C.] Sentencia C-748/11, M.P. Jorge Ignacio Pretelt Chaljub, Gaceta de la Corte Constitucional [G. C. C.] (Vol. n/d, p. 40) (Colom.) (Interpreta el principio de finalidad de la L. 1581/12, y establece su alcance en la sección 2.6.5.2.2.).

“Por la cual se impone una sanción y se imparte órdenes administrativas”

Constitucional determinó que *“(. . .) los datos personales deben ser procesados solo en la forma que la persona afectada pueda razonablemente prever. Si, con el tiempo, el uso de los datos personales cambia a formas que la persona razonablemente no espera, debe obtenerse el consentimiento del titular”*²⁹.

De este modo, teniendo en cuenta el principio de finalidad y el deber de informar los derechos que tienen los titulares los derechos que le asisten debido a la autorización otorgado, la finalidad de la base de datos de portabilidad numérica, de acuerdo con la Ley 1245 de 2008 y la C.R.C. Resolución 5050 de 2016, tienen como finalidad permitir la portabilidad numérica a los usuarios de telefonía celular de la totalidad de los proveedores de Redes y servicios de telecomunicaciones, bajo criterios estándar fijados por el Plan Nacional del Numeración y demás reglas aplicables, pero de limitado a la finalidad misma, puesto que la C.R.C. Resolución 5050 de 2016, artículo 2.6.7.3. regló de forma expresa que la información recolectada para los fines específicos de la portabilidad numérica, y la excepción contemplada por la C.R.C. Resolución 5050 de 2016, artículo 2.1.1.8., en relación con el intercambio de datos entre proveedores exclusivamente para efectos de la prevención y control de fraudes de comunicaciones. En todo caso, el mismo artículo reconoce expresamente que debido que en el proceso de portabilidad numérica si se hace recolección de datos personales, razón por la cual deberá requerirse la autorización.

En el caso en concreto de CLARO, a través de la Resolución 35890 de 2020 se realizó la imputación del cargo sobre el supuesto que la investigada estaba accediendo a los datos tratados en las bases de datos positiva y negativa de IMEI creada por la L.1453/11 y reglamentada por la C.R.C. Resolución 5050 de 2016, bajo la premisa de que la articulación o conexión entre CLARO, como PRSTM, y las bases de datos positiva y negativa se realizaba a través del aplicativo PORTANODE; sin embargo, una vez allegadas las repuestas a los requerimientos³⁰ de información realizados tanto a la C.R.C. como al Corte Inglés, se evidenció que PORTANODE es el aplicativo o programa que sirve Gateway o cliente entre la base de datos de portabilidad numérica -BDA- administrada por parte del Corte Inglés y la base de datos operativa administrada por parte de los PRSTM como CLARO, y que, en conjunto conforman la Base de Datos de Portabilidad Numérica (Ver sección 7.1.1. de la presente resolución). Los aplicativos o cliente que sirven como mecanismo de interacción entre las bases de datos positiva y negativa de IMEI y los PSRT son MobLystNode o SRTMNode (Ver sección 7.1.2. de la presente resolución). En ese sentido, el Despacho evaluará, teniendo en cuenta la evidencia recolectada dentro del expediente, como CLARO accedió a través del aplicativo PORTANODE y sustrajo la información base de los números telefónicos de los titulares afiliados de otros operadores para procesos de tele mercadeo, contrariando la finalidad asignada por parte de la norma de creación de la base de datos, y no obtener, cuando les fue posible, el consentimiento de dichos titulares.

Frente al uso de PORTANODE, y el acceso a través de este a los datos contenidos en la base de portabilidad numérica, CLARO en sus descargos, presentados a través de los radicados 18-127153-56 a 102, indicó, y el Despacho acepta tal afirmación, (i) que el aplicativo PORTANODE no tiene relación alguna con la base de datos positiva y negativa, razón por la cual no sustrajo información personal de los titulares de esta; (ii) sin embargo, reconocen lo siguiente en relación con el uso de PORTANODE para *“(. . .) la recolección de datos (. . .) a través de diversos pasos, entre ellos el ‘Cruce de información de **clientes portados del Corte Inglés** para identificar clientes que se portaron para otra empresa’, se estaba haciendo alusión a la bases de datos administrada por El Corte Inglés en calidad de ADB en el proceso de portabilidad numérica, y no a las bases de datos relacionadas con control de IMEI (sic) de equipos terminales (. . .)”*; (iii) *“(. . .) las bases de datos no contienen (sic) datos personales de los cuales se requiera autorización previa, expresa e informada por parte del titular, sino que lo incorporado en la misma corresponde a un listado público de números que no identifican de manera personal a ningún usuario concreto. Una se establecen los contactos telefónicos, siempre se solicita autorización previa, expresa e informada para el tratamiento de datos personales que vaya a suministrar el titular de la línea.*

Esta línea argumentativa presentada por CLARO continua en los alegatos de conclusión presentados con el radicado 18 -127153 - - 135 del 22 de abril de 2021, donde argumentaron: (i) Citando al Corte Inglés indicaron que *“(. . .) los operadores móviles no tienen acceso directo (a) (sic) la totalidad de la información almacenada en la base de datos del ABD, ya que si interacción dentro de la misma es solo para envío de transacciones y consulta a través de protocolos seguros.”*³¹; (ii) *“Cuando se afirmo que por parte de la Compañía que el procedimiento de recolección de datos se realizaba a través de*

²⁹ Ibidem.

³⁰ Radicados 18 – 127153. - - 121 del 23 de noviembre de 200 y 18 – 127153 - - 126 del 12 de febrero de 2021.

³¹ Radicado 18-127153 - - 134 del 21 de abril de 2021, p. 12.

“Por la cual se impone una sanción y se imparte órdenes administrativas”

diversos pasos, entre ellos el ‘Cruce de información de clientes portados del Corte Inglés para identificar clientes que se portaron a otra empresa’, se estaba haciendo alusión a las bases de datos administrada por El Corte Inglés en calidad de ABD en el proceso de portabilidad numérica, y no a las bases de datos relacionadas con la actividad de control de IMEIS de equipos terminales (. . .)”³²; (iii) “. . .) las bases de datos de portabilidad numérica no contienen datos personales respecto de los cuales se requiera contar con autorización previa, expresa e informada por parte del titular, sino que lo incorporado en la misma corresponde a un listado público de números que no identifican de manera a ningún usuario concreto.”³³

A lo anterior se le suma lo dicho por parte de CLARO mediante el radicado 18 – 127153 - - 9 del 17 de octubre de 2018, en relación a la formación de la lista de mercadeo que es remitida por el Departamento de Inteligencia de los Negocios al Departamento de Tele mercadeo, y este a los Call Center contratos por parte de CLARO “. . .) indicó que los listados de números aleatorios se van creando a partir de los prefijos de la numeración pública, Estos listados aleatorios son cotejados con los archivos que publica el Corte Inglés para consulta de los operadores, **los cuales se descargan desde el Corte inglés y posteriormente se actualiza el operador al que respectivamente pertenece cada uno de los números telefónicos, así mismo señaló dentro de los listados se envían cerca de 100.000 números mensuales por operador los cuales pueden varias de acuerdo con la contactibilidad**” (negrillas fuera del texto); y lo cual fue confirmado posteriormente por parte de CLARO nuevamente a través de los radicados 18 – 127153 31 – 33 del 4 de junio de 2020, en los cuales se le dio respuesta al requerimiento de información realizado por parte de este Despacho mediante radicado 18- 127153 - -25 del 19 de mayo de 2020³⁴, así:

- (a) Las listas de números para tele-mercadeo para migración pre-pago y pos-pago se forman de las bases de datos internas de clientes actuales de CLARO; las cuales se generan para su uso durante un mes determinado y se mantienen disponibles por dos meses, y solo se usa para contactar a los clientes para la campana de migración del mes y hacer seguimiento a las ventas que se realizaron, así como para aplicar las exclusiones de las nuevas listas, por tanto fue posible la remisión de la base de datos para los periodos solicitados. Aun así, remitieron un cuadro explicativo de como se forma la base de datos de migración pre-pago y pos-pago de clientes propios:

PROCESO PARA GENERACION DE LISTAS DE MIGRACION PREPAGO A POSTPAGO



Fuente: 2Anexo 2 del radicado 18 - 127153 - - 31

- (b) En relación con la formación a la lista de clientes no CLARO, el RESPONSABLE indicó el procedimiento de recolección se realiza a través de diversos pasos, entre ellos el “Cruce de información de clientes portados del Corte inglés para identificar clientes que se portaron a otra empresa”, tal como explican en el siguiente Cuadro:

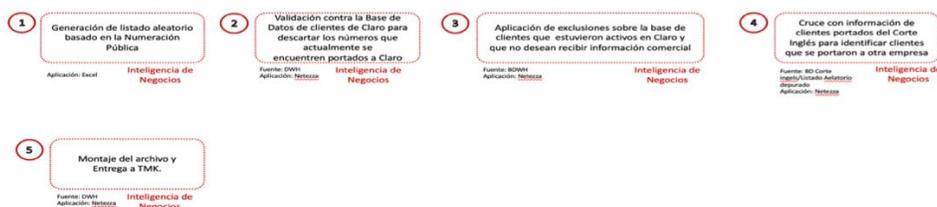
³² Ibidem, p. 13.

³³ Op. Cit. p. 13 -14.

³⁴ En respuesta a las preguntas 1 al 3 del cuestionario presentado ante CLARO: (1) De acuerdo con lo expresado por parte de la señora María Verónica Trujillo, la entonces gerente de inteligencia de negocios, las listas de números para tele mercadeo para migración pre-pago y pos-pago se forman de las bases de datos internas de Claro S.A. De acuerdo con lo anterior, informar detalladamente que bases de datos propias de Claro S.A. y procedimiento alimentan la formación de las listas de números para tele-mercadeo para migración pre-pago y pos-pago. Así mismo, remitir: (i) copia de dichas bases de datos; (ii) copia del aplicativo para realizar el tratamiento en cuestión junto con su código fuente y las instrucciones de funcionamiento; (2) De acuerdo con lo expresado por parte de la señora María Verónica Trujillo, la entonces gerente de inteligencia de negocios, la lista de número para afiliación de terceros no clientes de Claro S.A. se forma aleatoriamente de los prefijos de numeración pública, la cual es comparada con el listado arrojado por parte del Corte Inglés. De acuerdo con lo anterior, por favor explicar de forma detallada el procedimiento por medio del cual se hace la comparación del listado aleatorio con la lista del Corte Inglés; (3) De acuerdo con lo expresado por parte del señor Germán Lopera, el entonces gerente de desarrollo facturación, Claro S.A. desarrolló un aplicativo para gestionar el proceso de portabilidad llamado Portanode que descarga las bases de datos del ABD (Corte Inglés) a través del uso de VPN y las credenciales asignadas por parte de la Comisión de Regulación de Comunicación. De acuerdo con lo anterior, remitir: (i) copia del programa denominado Portanode junto con su código fuente e instrucciones de uso; (ii) copia del acuerdo o condiciones de uso remitidas por parte de la C.R.C, o quien haga de sus veces, para la utilización del usuario y clave de acceso a la base de datos del Corte Inglés.

“Por la cual se impone una sanción y se imparte órdenes administrativas”

PROCESO PARA GENERACION DE LISTADOS PARA PORTACIÓN



Fuente: 3 Anexo 3 del radicado 18 - 127153 - - 31

Se hace énfasis en el recuadro 4 del anexo 3 donde manifestaron de forma expresa que se utilizó la base de portabilidad numérica “Fuente: BD Corte Inglés/listado aleatorio depurado” para procesos de mercadeo tal como expone el recuadro 5, sumado a que se trata de la formación de una lista de clientes NO-CLARO.

Lo anteriormente expuesto confirma la teoría del caso creada por el Despacho sobre el uso que le da CLARO al doble acceso que tienen los PRSTM a la base de datos de portabilidad numérica: (i) a través del proceso de portabilidad numérica donde si se recolecta información personal³⁵ de los titulares (C.R.C. Resolución 5050 de 2016, art. 2.6.4.1.), y; (ii) el acceso que los demás PSRTM tienen a la base de datos BDA/BDO donde reposa los números de cada uno de los titulares como información base (Resolución 5050 de 2016, arts. 2.6.3.3.2.6. y 2.6.11.4.)³⁶, para formar una base de datos de alrededor de 100.000 números mensuales para ser remitida a los call center contratados por parte de CLARO, lo cual contraría la finalidad específica establecida por la Ley 1245 de 2008 y la C.R.C. Resolución 5050 de 2016, a la base de datos de portabilidad numérica, sin tener en cuenta la extrapolación con las llamadas a cabo a millones de usuarios de otros PRSTM.

En relación con la ausencia de afectación real a los titulares, tal como lo expuso CLARO en sus Descargos y Alegatos de Conclusión, esto no resulta cierto, puesto que reconocieron expresamente que la formación de las listas para efectos de tele mercadeo están compuestas por al menos 100.000 números de cada operador, lo cual contrasta negativamente con lo enunciado por parte de TIGO en sus diversas intervenciones en la presente actuación administrativa así: *[D]el seguimiento periódico realizado por la compañía para el análisis de tráfico de usuarios, se detectó la siguiente información, la cual contiene el detalle de las 10 líneas de Claro con más llamadas hacia Tigo, con un total de 1,6 millones de llamadas durante el mes de diciembre de 2018 en los cuales se contactó a 641 mil usuarios de nuestra base de datos*³⁷:

³⁵ C.R.C. R.5050/16, art. 2.6.4.3.: El Proceso de Portación se inicia con la entrega de la Solicitud de Portación por parte del Usuario al Proveedor Receptor. La Solicitud de Portación puede hacerse por escrito, personalmente o a través de la línea telefónica de atención al cliente, o por cualquier otro medio que determine o convalide la Comisión. En la Solicitud de Portación, el Usuario deberá proveer únicamente la siguiente información:

2.6.4.3.1. Para las personas naturales:

2.6.4.3.1.1. Nombre completo.

2.6.4.3.1.2. Número del documento de identidad.

2.6.4.3.1.3. Autorización del suscriptor del contrato de servicios de telecomunicaciones tratándose de servicios en la modalidad de pospago, y copia del documento de identidad, en caso de que la solicitud no sea presentada por el mismo.

2.6.4.3.1.4. Número(s) telefónico(s) asociado(s) a la portación solicitada.

2.6.4.3.1.5. Proveedor Donante.

2.6.4.3.1.6. NIP de Confirmación para los Usuarios de Servicios Móviles, el cual ha sido enviado previamente por el ABD al Usuario a través de un mensaje corto de texto (SMS).

2.6.4.3.2. Para las personas jurídicas:

2.6.4.3.2.1. Razón social.

2.6.4.3.2.2. Número de Identificación Tributaria (NIT).

2.6.4.3.2.3. Copia del Certificado de Cámara de Comercio con fecha de expedición no superior a treinta (30) días.

2.6.4.3.2.4. Tratándose de servicios en la modalidad de pospago autorización del representante legal y copia del documento de identidad, en caso que la solicitud no sea presentada por el mismo.

2.6.4.3.2.5. Número(s) telefónico(s) asociado(s) a la portación solicitada.

2.6.4.3.2.6. Proveedor Donante.

³⁶ Ver Concepto 504753 del 25 de febrero de 2020 de la Comisión de Regulación de Comunicaciones (Hace referencia al funcionamiento básico de la base de datos de portabilidad numérica, y como los PSRMT deben dar acceso

³⁷ 18-127153 - - 16 del 21 de febrero de 2019, p. 2.

“Por la cual se impone una sanción y se imparte órdenes administrativas”

	3177946525	3224382226	3106895752
Llamadas	551.601	193.517	238.458
Usuarios contactados	160.836	92.359	73.510
Usuarios Pospago	93.421	36.981	34.044
Usuarios Prepago	67.415	55.378	39.486
Portaciones Efectivas	2.985	429	783
Portaciones Pospago	2.074	273	519
Portaciones Prepago	911	156	264
Efectividad (%)	1,90%	0,50%	1,10%
Efectividad Pospago(%)	2,20%	0,70%	1,50%
Efectividad Prepago(%)	1,40%	0,30%	0,70%
Usuarios Portados después de la llamada	2.967	425	766
Días Promedio de Portación después de la llamada	9	6	7

	3213721331	3112647933	3228484426	3204479072
Llamadas	153.240	121.534	96.309	73.765
Usuarios contactados	61.688	58.918	55.648	40.338
Usuarios Pospago	30.314	26.000	22.733	20.733
Usuarios Prepago	31.374	32.918	32.915	19.605
Portaciones Efectivas	228	263	652	86
Portaciones Pospago	158	164	318	60
Portaciones Prepago	70	99	334	26
Efectividad (%)	0,40%	0,40%	1,20%	0,20%
Efectividad Pospago(%)	0,50%	0,60%	1,40%	0,30%
Efectividad Prepago(%)	0,20%	0,30%	1,00%	0,10%
Usuarios Portados después de la llamada	226	251	640	83
Días Promedio de Portación después de la llamada	6	7	6	6

	3112661776	3204425124	3114874135	Total
Llamadas	87.711	41.467	75.223	1.637.625
Usuarios contactados	34.427	32.625	30.761	641.130
Usuarios Pospago	17.253	14.619	8.623	304.121
Usuarios Prepago	17.174	18.006	22.138	337.009
Portaciones Efectivas	159	188	102	5.875
Portaciones Pospago	109	114	39	3.828
Portaciones Prepago	50	74	63	2.047
Efectividad (%)	0,50%	0,60%	0,30%	0,90%
Efectividad Pospago(%)	0,60%	0,80%	0,50%	1,30%
Efectividad Prepago(%)	0,30%	0,40%	0,30%	0,60%
Usuarios Portados después de la llamada	153	164	98	5.795
Días Promedio de Portación después de la llamada	9	13	9	8

Por su parte, AVANTEL muestra en cifras el actuar negativo de CLARO en cuanto a la utilización de la base de datos de portabilidad numérica, en los siguientes términos: “(. . .) AVANTEL pudo probar que COMCEL realizó 1.794.006 llamadas a sus abonados entre el mes de enero hasta el 27 de julio de 2020, tal como se aprecia en la siguiente tabla:

Llamadas	Claro Movil
Ene	203.584
Feb	350.548
mar	322.222
Abr	205.576
may	202.642
Jun	291.687
Jul	217.747
Total general	1.794.006

Elaboración propia

Sin perjuicio de advertir a su Despacho que las conductas aquí denunciadas y desplegadas por la empresa denunciada, persisten y han tenido vocación de continuidad, tal y como se aprecia en el siguiente cuadro:

Llamadas	Claro Móvil
Ago	647.284
Sep	599.542
Oct	455.948
Nov	568.207
Dic	725.579
Ene	694.128
Feb	861.077
Marzo	874.629
Abril	232.426
Total General	5.658.820

Elaboración propia

Conforme al cuadro anterior, CLARO desde agosto de 2020 hasta la fecha de este memorial, ha realizado desde sus call centers 5.658.820 llamadas usuarios Avante³⁸. Por su parte, CLARO no presentó evidencia para refutar que estas llamadas no se realizaron mediante la utilización de una lista formada de números de la base de datos de portabilidad numérica, lo cual lleva concluir que efectivamente lo expuesto por parte del despacho en relación al uso de al menos los números contenidos en la base de datos de portabilidad numérica para armar listas propias para realizar más de 100.000 llamadas para efectos de tele-mercadeo, denotando que la afectación no fue sobre unos miles, sino millones de titulares.

³⁸ Radicado 18 -127153 - - 132 del 19 de abril de 2021, p. 2 – 3.

“Por la cual se impone una sanción y se imparte órdenes administrativas”

De esta manera nos encontramos con una flagrante vulneración al Régimen de Protección de Datos en cuanto el uso de los datos contenidos, si bien no del todo personales, si son privados, puesto que su uso permite la individualización de los titulares de la misma, y que en todo caso, su uso en actividades de tele-mercadeo resulta contraria al principio de finalidad en los términos establecidos por el artículo 4, literal (b) y el deber de informar la finalidad del tratamiento de conformidad con el artículo 17, literal (c) de la Ley 1581 de 2012, a lo cual se le suma que los audios de las llamadas allegados a la actuación, así como de las quejas remitidas por parte de algunos titulares a la SIC y a través de sus respectivos operadores, no evidenció que estas incluyeran la solicitud de un nuevo consentimiento, salvo aquellas donde se realizó la portación efectiva, ni como tampoco una explicación, dentro del espectro de los posibles usos razonables de la información de acuerdo con la autorización inicialmente otorgada y vinculada con la finalidad específica dada por la ley, la cual, en el presente caso, de la razón por la cual fueron los titulares contactados para llamadas de tele-mercadeo por parte de CLARO.

Bien como indicó la Corte Constitucional en relación con el principio de finalidad y el deber de informar la finalidad a los titulares, CLARO realizó una recolección de datos sin un fin legal y legítimo, utilizando la base de datos de portabilidad numérica³⁹ para (. . .) *una finalidad diferente a la inicialmente prevista*⁴⁰, contrariando también las prohibiciones expresas dadas por la C.R.C. Resolución 5050 de 2016, artículos 2.1.1.8. y 2.6.7.3., los cuales, respectivamente, (i) indican que, por existir tratamiento de datos personales, se requerirá autorización expresa de los titulares, pues el número telefónico es uno de ellos, y; (ii) los datos incluidos dentro de la base de datos portabilidad numérica, incluyendo la BDO y la BDA, son de confidenciales y reservados, y solo pudiendo utilizar esta para fines de la portabilidad numérica en el esquema presentado por la C.R.C. Resolución 5050 de 2016.

En suma, CLARO realizó la recolección y tratamiento de información contenida en la base de datos de portabilidad numérica con el propósito de poder adelantar procesos de tele-mercadeo no contemplados por la finalidad asignada por la norma que le dio origen, afectando a millones de titulares al ser sujetos de llamadas a sus números personales y sobre las cuales no prestaron su autorización previa, y CLARO no procuró obtenerla en la mayoría de las llamadas, lo cual es una clara vulneración al Régimen de Protección de Datos que da lugar a la imposición de una sanción y la orden de abstenerse de continuar utilizando la base de datos de portabilidad numérica para generar listados de números para efectos de campañas de tele-mercadeo para la captación masiva de clientes de otros operadores.

7.3.2. Sobre el Principio de libertad y el deber de solicitar y conservar la copia de la autorización de la respectiva autorización otorgada por los titulares en los términos establecidos en la ley.

De conformidad con el artículo 4, literal (c) de la Ley 1581 de 2012, el principio de libertad erige para el responsable el deber de que *“El tratamiento solo puede ejercerse con el consentimiento, previo, expreso e informado del titular. Los datos personales no podrán ser obtenidos (...) sin previa autorización (...)”*; por su parte, y lo cual debe ser leído en conjunto con lo anteriormente expuesto, el artículo 9 de la Ley 1581 de 2012 estableció que *“Sin perjuicio de las excepciones previstas en la ley, en el tratamiento se requiere la autorización previa e informada del titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior”*

Así mismo, el artículo 17, literal (b) de la ley 1581 de 2012, erigió el deber para el responsable de: *“Solicitar y conservar (. . .) copia de la respectiva autorización otorgada por el titular”*; lo cual fue reglamento por parte del Decreto 1377 del 2013, artículo 5, incorporado al Decreto único Reglamentario 1074 del 2015, artículo 2.2.2.25.2.2., así:

“El responsable del tratamiento deberá adoptar procedimiento para la solicitar el tratamiento de los mismos e informarle los datos personales que serán recolectados, así como todas las finalidades específicas del tratamiento para las cuales se obtiene el consentimiento.

Los datos personales que se encuentren en fuentes de acceso público, con independencia del medio por el cual se tenga acceso, entendiéndose por tales aquellos datos o bases de datos que se encuentran a disposición del público,

³⁹ Cuya finalidad es permitir la portabilidad numérica a los usuarios de telefonía celular de la totalidad de los proveedores de Redes y servicios de telecomunicaciones, bajo criterios estándar fijados por el Plan Nacional del Numeración y demás reglas aplicables,

⁴⁰ Corte Constitucional [C.C.] Sentencia T-729/02, M.P. Eduardo Montealegre Lynnett, Gaceta de la Corte Constitucional [G. C. C.] (Vol. n/d, p. 5) (Colom.)

“Por la cual se impone una sanción y se imparte órdenes administrativas”

pueden ser tratados por cualquier persona y cuando, por su naturaleza, sean datos públicos (. . .)”.

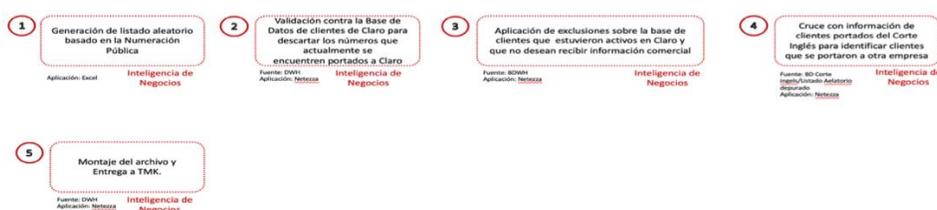
Para lograr lo anterior, artículo 7 del Decreto 1377 del 2013, incorporado al Decreto único Reglamentario 1074 del 2015, artículo 2.2.2.25.2.3., estableció el mecanismo para obtener la autorización:

“Para efectos de dar cumplimiento a lo dispuesto en el artículo 9 de la Ley 1581 de 2012, los Responsables del tratamiento de datos personales establecerán mecanismos para obtener la autorización de los titulares o de quien se encuentra legitimado (. . .) que garanticen su consulta. Estos mecanismos podrán ser predeterminados a través de medios técnicos que faciliten al titular su manifestación automatizada. Se entenderá que la autorización cumple con estos requisitos cuando se manifieste (i) por escrito, (ii) de forma oral o (iii) mediante conductas inequívocas del Titular permitan concluir de forma razonable que otorgó la autorización. En ningún caso, el silencio podrá asimilarse a una conducta inequívoca.”

Una vez obtenida la autorización *“Los responsables deberán conservar prueba de la autorización otorgada por los titulares de datos personales para el tratamiento de los mismos.”*⁴¹

En el caso en concreto de Claro, se evidenció que utilizó la base de datos de portabilidad numérica para generar base de datos propias o listados propios de números que era remitidas por parte del Departamento de Inteligencia de los Negocios al Departamento de Tele-mercadeo y de esta a los Call Center contratados CLARO, *“(. . .) los listados de números aleatorios se van creando a partir de los prefijos de la numeración pública, Estos listados aleatorios son cotejados con los archivos que publica el Corte Inglés para consulta de los operadores, los cuales se descargan desde el Corte inglés y posteriormente se actualiza el operador al que respectivamente pertenece cada uno de los números telefónicos, así mismo señaló dentro de los listados se envían cerca de 100.000 números mensuales por operador los cuales pueden varias de acuerdo con la contactibilidad”* (negrillas fuera del texto); esto se ve reflejado en el cuadro -Anexo 3- remitido por parte de CLARO a través del radicado 18 -127153 - - 31, donde se manifestó -recuadro 4- la sustracción de datos de la base denominada el Corte Inglés -base de datos de portabilidad numérica-, para realizar llamadas de tele-mercadeo para la captación de clientes de otros operadores, contrariando la finalidad propia de dicha base de datos, la consecución exclusiva de la portabilidad numérica.

PROCESO PARA GENERACION DE LISTADOS PARA PORTACIÓN



Fuente: 4 Anexo 3 del radicado 18 - 127153 - - 31

De igual forma, Claro ignoró los dos mecanismos establecidos por parte de la C.R.C. R. 5050/16 que limitan el uso de la información que es recolectada por parte de los PRSTM: (i) la información no fue utilizada para efectos de la prevención y control de fraudes de comunicación y el cumplimiento de la actividad regulatoria, como tampoco, por tratarse de información personal, se solicitó la autorización de expresa de los titulares (C.R.C. Resolución 5050 de 2016, art. 2.1.1.8.) cuyos números telefónicos estaba registrados obligatoriamente en los BDO de los operadores tales como TIGO y AVANTEL, sin perjuicio de aquellos PRSTM y usuarios que hayan podido ser afectados por esta misma práctica; (ii) utilización de la base de datos, y los datos allí contenido para efectos específicos de la portabilidad numérica (C.R.C. Resolución 5050 de 2016, art. 2.6.7.3.).

Esta ausencia de solicitud de autorización, en los términos prescritos por el Régimen de Protección de Datos, se ve reflejada en las quejas y grabaciones de llamadas remitidas al Despacho así:

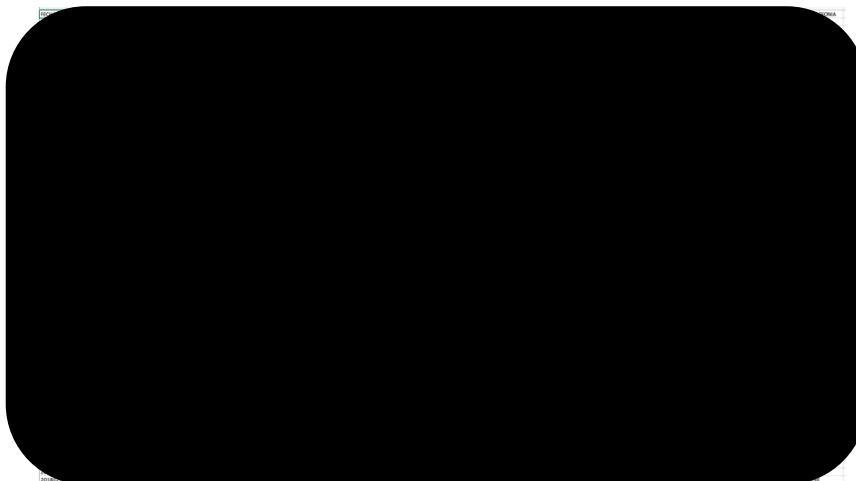
(a) Queja presentada por la señora Sandy de la Ossa, donde indicó lo siguiente: *“(. . .) al preguntarles porque tenían acceso a mi información, el asesor manifestó que tenían una base*

⁴¹ D.1377/13, art. 8.

“Por la cual se impone una sanción y se imparte órdenes administrativas”

de datos de los todos los clientes de todos los operadores (. . .)”⁴², de donde se sustrae el uso de la información de la base de datos de portabilidad numérica, y no se solicitó la autorización exigida por el Régimen de Protección de Datos y la C.R.C. Resolución 5050 de 2016.

- (b) Queja presentada por [REDACTED], donde indicó lo siguiente: *“Me dirijo a ustedes para manifestarles mi inconformidad (. . .) al recibir varias llamadas del Operador Claro donde se evidencia que poseen toda la información personal de la línea (. . .) incluyendo mi número y mis datos personales, tal como si fuera un asesor de Tigo. (. . .) me ofrecieron el proceso de portación informando que ‘ellos’ se encargaban de toda la papelería (. . .)”*⁴³ de donde también se sustrae el uso de la información de la base de datos de portabilidad numérica, y no se solicitó la autorización exigida por el Régimen de Protección de Datos y la C.R.C. Resolución 5050 de 2016
- (c) Queja presentada por [REDACTED], donde indicó lo siguiente: *Me dirijo a ustedes para manifestarles mi inconformidad (. . .) al recibir varias llamadas del Operador Claro donde se evidencia que poseen toda la información personal de la línea (. . .) hago referencia a (sic) que conocen la tarifa que manejo, los recursos asignados, el valor del cargo básico, mi número de línea, y mis datos personales, tal como si fueran un asesor de Tigo (. . .) me ofrecieron el proceso de portación con los mismos recursos de portación con los mismos recursos y un cargo inferior (. . .)”* de lo cual se entiende el uso de la información de la base de datos de portabilidad numérica, y no se solicitó la autorización exigida por el Régimen de Protección de Datos y la C.R.C. Resolución 5050 de 2016.
- (d) De igual forma, TIGO realizó el seguimiento de llamadas recibidas de los siguientes números de CLARO ([REDACTED]), evidenciando que realizó 1279 llamada a distintos números TIGO, sin que haya presentado prueba sumaria por parte de CLARO de haber solicitado la autorización expresa a los titulares de estas líneas, ni explicación sumaria de donde sustrajeron los datos -números- para el contacto. A continuación, se adjunta cuadro de muestra de algunas de las llamadas realizadas por parte de CLARO números TIGO:



- (e) Mediante el radicado 18-127153 - - 12 del 22 de noviembre de 2018, TIGO remitió audio de la llamada realizada [REDACTED], en la cual, dentro del minuto 0:40 a 0:44 el señor Díaz preguntó a la agente comercial de dónde obtuvieron su número telefónico, a lo cual ella replicó de que se trataba de una base de Datos que proporcionaba la Superintendencia, sin especificar cual. Se denota de tal llamada la ausencia de explicación razonable de donde obtuvieron el número de teléfono, como tampoco que se solicitó la autorización en los términos establecidos por el Régimen de Protección de Datos.
- (f) Mediante radicado 18 – 127153 - - 15 del 27 de noviembre de 2019, se radicado la grabación a [REDACTED], en la cual se puede evidenciar que la agente comercial de CLARO no pudo justificar el origen de la base de datos, solo indicando que el poseían el número, así como tampoco con la autorización por parte de la señora Lastre para realizar la llamada;

⁴² Radicado 18-127153 - - 00 del 24 de abril de 2020.

⁴³ Radicado 18-127153 - - 00 del 24 de abril de 2020.

"Por la cual se impone una sanción y se imparte órdenes administrativas"

- (g) Mediante radicado 18 – 127153 - - 19 del 21 de octubre de 2019, se radicó por parte de TIGO el audio de la llamada realizada [REDACTED], en la cual se le informó desde el minuto 4:40, una vez este le preguntó si sus datos estaban en una base de datos VIP, que poseían solo su número, pero que ellos llamaban de forma constante a los clientes de otros operadores tales como TIGO, MOVISTAR para brindarle las propuestas que maneja CLARO. Las bases de datos son brindadas directamente por CLARO de números de otros operadores a los cuales tiene acceso. Nuevamente, se evidencia la utilización de la base de datos de portabilidad numérica, única en la cual se encuentra, como información básica, los números de la totalidad de los operadores en Colombia para una finalidad distinta a la portabilidad numérica, y en todo caso, sin requerir la autorización previa, expresa e informada requerida por la ley para darle un tratamiento.
- (h) A través del radicado 18-225775 - - 00 del 7 de septiembre de 2018, AVANTEL radicó la transcripción de las siguientes llamadas en las cuales se evidencia la ausencia de autorización para realizar la llamada:

(i) Llamada 6:

Usuario: pero, pero un momento porque tienen mi número?...
 Claro: porque su número esta todas las bases de datos a nivel nacional según el ministerio de transporte y comunicaciones ...
 Usuario: ósea que claro llama a todos los operadores a ofrecerles promociones?
 Asesor comercial: si señor ...
 Usuario: y eso si es legal?
 ...
 Usuario: ... ósea usted tiene una base de datos del ministerio del transporte ...
 Asesor comercial: ... yo no, esto es una central telefónica.
 Usuario: si no es que me preocupa, porque pues tengan mi número y me estén llamando para ofrecerme promociones ...

(ii) Llamada 7:

"Asesor comercial: ... el motivo de mi llamada como tal, ... la compañía de claro pues estamos en aniversario y el día de hoy queremos realizarle a usted una excelente oferta, para que realice la portabilidad directamente con nosotros ...
 Usuario: ... pero ven yo te hago una pregunta, tu como obtuviste mi número?
 Asesor comercial: Como tenemos tu numero de teléfono?
 Usuario: Sí.
 Asesor comercial: Bueno señor sí, lo que pasa es que a través del servicio de lo que sería la protección de datos personales, pasa una ... directamente con el número de teléfonos de los clientes preferenciales para llamar, pero a nosotros nos cargan los clientes pero no nos cargan directamente los datos personales de los clientes

... solamente los números de teléfono que están en otras compañías compañía ...

“Por la cual se impone una sanción y se imparte órdenes administrativas”

(iii) Llamada 9:

...

Claro: ... La razón de mi llamada es porque queremos hacerle un ofrecimiento para traer su línea celular 350 de Avantel traerla a claro.

...

Usuario: No entiendo es como la tiene.

Asesor comercial: porque pues quedan registradas en la base de datos como líneas de otro operador, lo que queremos simplemente es traerlas ...

Usuario: ... pero ustedes pueden simplemente porque paso una llamada por sus bases de datos contactarlo a uno sin que yo les haya autorizado habeas data.

Asesor comercial: Tenga en cuenta que la ley de habeas data aplica para lo que es nombre y cedula, el número celular no es un dato sensible.

(iv) Llamada 13:

Asesor comercial: si señora como yo le estoy explicando señora, le estoy diciendo que hubo alguien que hizo la portabilidad y nos dio a usted como referente.

Usuario: ... entiendo que es mi amigo y mi familiar y dice mi nombre y mi número, pero de dónde sacan un número sin un nombre asociado, porque usted no sabe cómo me llamo yo.

...

Usuario: ósea usted no tiene la autorización para hacer el tratamiento de mis datos personales.

Asesor comercial: porque no me la ha dado señora, si me da la autorización claro que si tengo la autorización de tener sus datos, de hacer tratamiento de sus datos ...

(Comillas, cursiva, negrilla y subrayado fuera del texto original)

De acuerdo con lo anteriormente expuesto, TIGO y AVANTEL en los radicados 18-127153 - - 134 el 21 de abril de 2021 y 18 – 127153 - - 132 del 19 de abril de 2021, respectivamente, indicaron que: (i) CLARO “(. . .) *no solo ha venido utilizando datos personales con fines distintos a los manifestados en la ley que da origen a la base de datos, sino que además no cuenta con los consentimientos de los titulares de la información para este efecto, ni para ningún otro tipo de tratamiento que pudiera equipararse a las finalidades de la base de datos o ser previsto por los afectados.*”⁴⁴; (ii) la actuación de CLARO deja de manifiesto que “(. . .) *obtuvo de forma irregular dichos datos personales, y en total oposición al deber de tutela que respecto al derecho fundamental le compete, decidió además disponer de los mismos con fines explotativos, anteponiendo su ánimo de lucro a los derechos fundamentales de los ciudadanos contactados irregularmente y ejerciendo, aún en perjuicio de los ciudadanos y competidores, un ejercicio abiertamente abusivo de su posición de dominio en los servicios de Voz y datos móviles. (. . .) desde agosto de 2020 hasta la fecha de este memorial, ha realizado desde sus call centers 5.658.820 llamadas usuarios Avantel. Si se tiene en cuenta que Avantel al tercer trimestre de 2020 (. . .) contaba con 1.4 millones de líneas móviles, se concluye que en promedio, durante los últimos 9 meses, CLARO realizó en promedio 5 intentos de contacto por cada usuario de servicios de la base total de usuarios Avantel (. . .)*”⁴⁵.

Por su parte, CLARO a través del radicado 18 – 127153 - - 56 al 102 del 12 de agosto de 2020, solicitó que se tuvieran en cuenta 25 llamadas realizadas entre 2019 y 2020, de las cuales se

⁴⁴ 18-127153 - - 134 el 21 de abril de 2021, p. 6.

⁴⁵ 18 – 127153 - - 132 del 19 de abril de 2021, p. 4 – 5.

“Por la cual se impone una sanción y se imparte órdenes administrativas”

concluye, teniendo en cuenta los siguientes audios: 2019-93057368921.mp3, 2019 – 93002505497.mp3, 2019-93167386432-A.mp3, y 2020-93165341982.mp3, y el guion de venta de servicios móviles V2 adjunto: (i) la autorización, en los términos prescritos por el Régimen de Protección de Datos, solo se requiere para aquellos titulares que muestren interés real en realizar el proceso de portabilidad, por lo que los audios son de casos de portabilidad exitosos; (ii) no se les informa de donde se adquirió o se sustrajo su número telefónico para efectos de dicha llamada, y (iii) se condicionaba al titular de la línea a la dar su autorización para efectos de solo entregar la información relacionada con los planes ofrecidos por CLARO, lo que en suma demuestra un actuar contrario al Régimen de Protección de Datos, y una utilización indebida de la información contenida en la base de portabilidad numérica.

CLARO, con excepción de los casos donde adquirió la autorización de los titulares que decidieron portarse a otro PRSTM, realizó el tratamiento de la información sin la autorización previa que requiere el Régimen, no estando tampoco los datos dentro de las excepciones contempladas por el artículo 10 de Ley 1581 de 2012, toda vez que, como se indicó, si bien la base de datos de portabilidad numérica es una base de datos de creación legal para beneficio del público, su acceso es de finalidad y acceso restringida -solo es posible a través del aplicativo PORTANODE-, por lo que no recae tampoco en la excepción establecida por el Decreto Único Reglamentario 1074/14, artículo 2.2.2.25.2.2.⁴⁶; nunca se buscó, en los términos del artículo 17, literal (b) de la Ley 1581 de 2012, solicitar y conservar copia de la respectiva autorización, ya que de los audios se evidencia también una ausencia, al menos para aquellos donde no hay interés de realizar la portabilidad numérica, de mecanismos técnicos que permitieran prestar su autorización por parte del titular ya sea (i) *por escrito*, (ii) *de forma oral* o (iii) *mediante conductas inequívocas*, teniendo en cuenta que el silencio nunca podrá ser signo de aceptación. A lo cual se debe adicionar que actuó en expresa contradicción de prohibición de utilizar los datos de portabilidad, los cuales incluyen, pero no se limitan a, los números dentro de los BDO de cada PSRTM, y aquellos que componen la BDA de administrada por el BDA.

En conclusión, se evidenció de forma contundente del acervo probatorio, y ausencia de pruebas de actos contrarios por parte de CLARO, que esta realizó el tratamiento de la información sustraída de la base de datos de portabilidad numérica para efectos de realizar campañas de tele-mercadeo sin la autorización previa, expresa e informada, de los titulares, razón por la cual se ve la necesidad de imponer una sanción y la orden de abstenerse de continuar el uso de la base de datos para efectos o finalidades distintas que la misma portabilidad numérica en las condiciones prescritas por la C.R.C. Resolución 5050 de 2016.

OCTAVO: Imposición y graduación de la sanción

La Ley 1581 de 2012 le confirió a la Superintendencia de Industria y Comercio una potestad sancionatoria que se concreta en el artículo 23 de la Ley 1581 de 2012, el cual señala lo siguiente:

“ARTÍCULO 23. SANCIONES. *La Superintendencia de Industria y Comercio podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:*

a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;

Texto del Proyecto de Ley Anterior

b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicaran los correctivos que se deberán adoptar;

c) Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio;

d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles;

(...).”

⁴⁶ D.U.R. 1074/15, art. 2.2.2.25.2.2.: (. . .): *Los datos personales que se encuentren en fuentes de acceso público, con independencia del medio por el cual se tenga acceso, entendiéndose por tales aquellos datos o bases de datos que se encuentran a disposición del público, pueden ser tratados por cualquier persona y cuando, por su naturaleza, sean datos públicos (. . .).”*

“Por la cual se impone una sanción y se imparte órdenes administrativas”

Por su parte, la Corte Constitucional a través de sentencia C-557 de 2000, señaló que la ley aprobatoria del Plan Nacional de Desarrollo tiene la siguiente naturaleza:

“Partiendo de la concepción que entiende la planeación como el instrumento fundamental para el manejo económico del Estado, y con base en lo dispuesto por el inciso tercero del artículo 341 de la Constitución Política según el cual “(e)l Plan Nacional de Inversiones se expedirá mediante una ley que tendrá prelación sobre las demás leyes”, y que “sus mandatos constituirán mecanismos idóneos para su ejecución y suplirán los existentes sin necesidad de la expedición de leyes posteriores”, la jurisprudencia ha destacado que la Ley del Plan de Desarrollo, que debe expedirse en cada período presidencial, determina el contenido de las leyes anuales de presupuesto, de otras leyes que tocan el tema económico, social o ambiental (...)”

El Plan Nacional de Desarrollo por ser una ley de iniciativa gubernamental y de un amplio consenso -tanto en la elaboración del proyecto de Ley como en su trámite legislativo- su cumplimiento debe hacerse de manera inmediata por parte de todas las entidades de orden nacional⁴⁷. Su cumplimiento se mide en la ejecución que se haga del Plan Nacional de Desarrollo dentro las competencias que le sean propias a cada una de las entidades del orden nacional observando los criterios de concurrencia, complementariedad y subsidiariedad. En consecuencia, cualquier norma que se incluya dentro del Plan Nacional de Desarrollo debe ser de obligatorio cumplimiento por las entidades que conforman la rama ejecutiva del nivel nacional a través del respectivo plan de acción institucional como lo establece el inciso 1 del artículo 26 de la ley 152 de 1994.

En ese orden de ideas, el artículo 49 de la Ley 1955 de 2019, mediante la cual se expide el Plan Nacional de Desarrollo 2018-2022, establece lo siguiente:

“ART. 49. —Cálculo de valores en UVT. A partir del 1o de enero de 2020, todos los cobros, sanciones, multas, tasas, tarifas y estampillas, actualmente denominados y establecidos con base en el salario mínimo mensual legal vigente, SMMLV, deberán ser calculados con base en su equivalencia en términos de la unidad de valor tributario, UVT. En adelante, las actualizaciones de estos valores también se harán con base en el valor de la UVT vigente.

PAR. —Los cobros, sanciones, multas, tasas, tarifas y estampillas, que se encuentren ejecutoriados con anterioridad al 1o de enero de 2020 se mantendrán determinados en SMMLV.”

De esta manera y de conformidad con la norma antes señalada, si el valor de los cobros, sanciones o multas se encuentran establecidos en salarios mínimos, estos deberán ser calculados con base en su equivalencia en términos de la unidad de valor tributario UVT. Por lo cual, las multas de carácter personal e institucional dispuestas en la Ley 1581 de 2012, serán determinadas de la siguiente manera:

$$\frac{SMMLV}{UVT \text{ vigente } 2021} = SMMLV \text{ expresado en UVT}' S$$

$$SMMLV \text{ expresado en UVT}' S * \text{Número de SMMLV a convertir} = \text{Sanción expresada en UVT}' S$$

De otra parte, la ley 1581 de 2012 en su artículo 24 señala los criterios de graduación de las sanciones de los cuales este Despacho entrará a determinar cuales se deben tener en cuenta en caso concreto, así:

De otra parte, dentro del marco de la Ley 1581 de 2012, con relación a la imposición de la sanción, el artículo 24 de la misma norma establece unos criterios de graduación que permiten garantizar el respeto de las garantías del artículo 29 Constitucional⁴⁸ y que, por lo tanto, esta Dirección deberá analizar para el caso concreto y así determinar cuales debe tener en cuenta. Esos criterios, según la sentencia C-748 de 2012, hacen referencia a cinco circunstancias de agravación, entre los literales

⁴⁷ Las entidades territoriales tienen sus propios Planes de Desarrollo, artículos 31 y ss., de la Ley 152 de 1994. Sin perjuicio, a la participación que éstas tienen en la elaboración del PND.

⁴⁸ Artículo 29. El debido proceso se aplicará a toda clase de actuaciones judiciales y **administrativas**. (...) (negrita añadida)

“Por la cual se impone una sanción y se imparte órdenes administrativas”

(a) y (e), y a una circunstancia de atenuación o disminución de la sanción, correspondiente al literal (f).

De igual forma, respecto a las sanciones que se imponen por la infracción al Régimen de Protección de Datos, debe precisarse que conforme al principio de proporcionalidad que orienta el derecho administrativo sancionador, esta Superintendencia debe ejercer su potestad sancionatoria de forma razonable y proporcionada, de modo que logre el equilibrio entre la sanción y la finalidad que la norma vulnerada que establezca, así como la proporcionalidad entre la gravedad de la infracción y la sanción aplicada. Sobre la aplicación de este principio, la Corte Constitucional ha señalado:

“En cuanto al principio de proporcionalidad en materia sancionatoria administrativa, éste exige que tanto la falta descrita como la sanción correspondiente a las mismas que resulten adecuadas a los fines de la norma, esto es, a la realización de los principios que gobiernan la función pública. Respecto de la sanción administrativa, la proporcionalidad implica también que ella no resulte excesiva en rigidez frente a la gravedad de la conducta, ni tampoco carente de importancia frente a esa misma gravedad”⁴⁹

Siendo así, para la correcta adecuación de los hechos y la sanción aplicable, el operador jurídico en materia de protección de datos personales debe analizar todos los criterios de graduación del artículo 24 de la Ley 1581 de 2012 con la finalidad de establecer como se aplican al caso concreto y, de esa forma, seleccionar y graduar la sanción que se impondrá. Para esta finalidad, también se pueden tener en cuenta para la dosificación de la sanción, el tamaño de la empresa, sus ingresos operacionales, patrimonio y, en general, su información financiera, como también su rol dentro del cumplimiento la Ley de habeas data financiero, de tal forma que la sanción resulte disuasoria más no confiscatoria.

Es necesario precisar que las sanciones que se imponen dentro de procesos administrativos sancionatorios no constituyen ninguna cuantificación de perjuicios materiales o morales, es decir no se trata de la cuantificación de un daño subjetivo, como sucede en el régimen civil de responsabilidad. Por el contrario, las sanciones que impone esta Superintendencia, en virtud del artículo 23 y siguientes de la Ley 1581 de 2012, es una consecuencia negativa impuesta en contra de la persona natural o jurídica que viole las disposiciones de la Ley 1581 de 2012. Esta consecuencia negativa tiene como finalidad promover y garantizar el cumplimiento de la Ley de habeas data financiero y, de esa forma, proteger el derecho fundamental a la protección de datos personales, entre otros.⁵⁰

La imposición de sanciones por violación de la Ley 1581 de 2012 tiene como fin central proteger y promover el respeto del derecho fundamental a la protección de datos personales, derecho humano (universal, inalienable, indivisible, irrenunciable e imprescriptible) que fue positivado en el artículo 15 de la Constitución de 1991, y que en muchas ocasiones es conexo a otros derechos fundamentales de gran relevancia constitucional como la dignidad humana, el buen nombre, la intimidad, etc. Del mismo modo, la vulneración del derecho fundamental a la protección de datos personales no solo afecta los derechos de una persona en particular, sino que pone en riesgo los derechos fundamentales de toda la sociedad. Por eso, las sanciones de dichas conductas no pueden, ni deben tratarse, como una cuestión insignificante o de poca monta. La transgresión flagrante a los derechos humanos de un ciudadano es, por sí solo, un hecho muy grave que no necesita de forzosos razonamientos para evitar un desentendimiento de la importancia de lo sucedido.

Recuérdese que, según la Declaración Universal de los Derechos Humanos, *“el desconocimiento y el menosprecio de los derechos humanos han originado actos de barbarie ultrajantes para la conciencia de la humanidad”*⁵¹. Por eso, según dicho documento, se considera *“esencial que los derechos humanos sean protegidos por un régimen de Derecho”*. No debe olvidarse que el respeto de los derechos humanos es un elemento esencial de la democracia.⁵¹ La Ley 1581 de 2012 le confirió a la Superintendencia de Industria y Comercio potestad sancionatoria que se concreta en

⁴⁹ Corte Constitucional, Sala Plena, C-125 del 18 de febrero de 2003, Magistrado Ponente Marco Gerardo Monroy Cabra.

⁵⁰ Las sanciones impuestas en función del derecho administrativo sancionatorio pretenden asegurar el orden público y el correcto funcionamiento de la administración. Al respecto ver: Corte Constitucional, Sala Plena, C-703 de 2010, Magistrado Ponente Gabriel Eduardo Mendoza, Considerando 5; Corte Constitucional, Sala Plena, C-010-03, Magistrada Ponente Clara Inés Vargas.

⁵¹ Artículo 3 de la Carta Democrática Interamericana la cual se puede consultar en: http://www.oas.org/OASpage/esp/Documentos/Carta_Democratica.htm

“Por la cual se impone una sanción y se imparte órdenes administrativas”

el artículo 23 de la misma ley. Asimismo, el artículo 24 de la norma en mención indica los criterios a seguir para graduar las sanciones en los siguientes términos:

“ARTÍCULO 24. CRITERIOS PARA GRADUAR LAS SANCIONES. *Las sanciones por infracciones a las que se refieren el artículo anterior, se graduarán atendiendo los siguientes criterios, en cuanto resulten aplicables:*

- a) La dimensión del daño o peligro a los intereses jurídicos tutelados por la presente ley;*
- b) El beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción;*
- c) La reincidencia en la comisión de la infracción;*
- d) La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Superintendencia de Industria y Comercio;*
- e) La renuencia o desacato a cumplir las órdenes impartidas por la Superintendencia de Industria y Comercio;*
- f) El reconocimiento o aceptación expresas que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar.”*

Por lo tanto, atendiendo dichos criterios, este Despacho entrará a determinar cuales deberá tener en cuenta en el caso en concreto, así:

9.1.1. La dimensión del daño o peligro a los intereses jurídicos tutelados por la ley

De la lectura de la norma citada, resulta claro que para que haya lugar a la imposición de una sanción por parte de este Despacho, basta que la conducta desplegada por la investigada haya puesto en peligro los intereses jurídicos tutelados por la Ley 1581 de 2012.

Respecto a las sanciones que se imponen por la infracción al Régimen de Protección de Datos, debe precisarse que conforme al principio de proporcionalidad que orienta el derecho administrativo sancionador, la autoridad administrativa debe ejercer su potestad sancionatoria en forma razonable y proporcionada, de modo que logre el equilibrio entre la sanción y la finalidad de la norma que establezca, así como la proporcionalidad entre el hecho constitutivo de la infracción y la sanción aplicada. Sobre la aplicación de este principio, la Corte Constitucional ha señalado:

*“En cuanto al principio de proporcionalidad en materia sancionatoria administrativa, éste exige que tanto la falta descrita como la sanción correspondiente a las mismas que resulten adecuadas a los fines de la norma, esto es, a la realización de los principios que gobiernan la función pública. Respecto de la sanción administrativa, la proporcionalidad implica también que ella no resulte excesiva en rigidez frente a la gravedad de la conducta, ni tampoco carente de importancia frente a esa misma gravedad”*⁵²

También se tendrán en cuenta para la dosificación de la sanción, el tamaño de la empresa, sus ingresos operacionales, patrimonio y, en general, su información financiera, de tal forma que la sanción resulte disuasoria más no confiscatoria. Así como, la conducta de la investigada durante el trámite de la investigación administrativa. De esta forma, para la correcta adecuación de los hechos y la sanción aplicable, el operador jurídico en materia de protección de datos personales, debe en primera medida, analizar la dimensión del daño o peligro a los intereses jurídicos tutelados, así como el posible beneficio económico, para luego analizar otras circunstancias concurrentes de graduación, tales como la capacidad económica del investigado, la reiteración de la infracción, colaboración del investigado para esclarecer los hechos investigados.⁵³

También se tendrán en cuenta para la dosificación de la sanción, el tamaño de la empresa, sus ingresos operacionales, patrimonio y, en general, su información financiera, de tal forma que la

⁵² Corte Constitucional, Sala Plena, Sentencia C-125 del 18 de febrero de 2003, Exp. Rad. D-4059, Magistrado Ponente Dr. Marco Gerardo Monroy Cabra.

⁵³ L. 1581/12, art 23: *“La Superintendencia de Industria y Comercio podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:* a) *Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;* b) *Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar;* c) *Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio;* d) *Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles;* *Parágrafo. Las sanciones indicadas en el presente artículo sólo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva.”*

“Por la cual se impone una sanción y se imparte órdenes administrativas”

sanción resulte disuasoria más no confiscatoria. Así como, la conducta de la investigada durante el trámite de la investigación administrativa.

9.1.2. Dimensión de los daños a los intereses de los titulares y ganancia económica por parte de CLARO

Para proceder a la imposición de la multa, es necesario tener en dos elementos fácticos evidenciados dentro de la investigación por parte del CLARO: (i) Utilizó la bases de datos de portabilidad numérica, -cuya finalidad es exclusivamente para dichos efectos-, al tratar, clasifica, y remitir dicha información a sus call center -propios y contratados- para realizar llamadas masivas de tele mercadeo con el fin de captar un mayor número de titulares, sin que mediara tampoco la autorización previa de los titulares para estos efectos; (ii) Capitalizó la bases de datos de portabilidad numérica, gratuita para los titulares pero onerosa para los PRSTM, con el fin de recibir un beneficio económico de los clientes que migraron de otros operadores a este a través de las llamadas masivas realizadas para efectos de migrarlos a su servicio.

Para efectos del presente análisis, es necesario tener en cuenta lo establecido por la Ley 1581 de 2012, artículo 24, literales (a) y (b), los cuales hablan de los criterios de graduación, el literal (a) habla de la dimensión del daño, y literal (b), hace referencia al beneficio económico recibido por parte del infractor, frente a lo cual la Corte Constitucional estableció lo siguiente: *“(. . .) se ajusta a la Constitución, en la medida en que corresponde al legislador establecer parámetros para que las autoridades, al momento de aplicar determinada sanción, puedan hacer graduaciones dependiendo de factores o circunstancias del investigado o de su actuación (. . .)”*⁵⁴. En ese orden de ideas, en materia de vulneración al Régimen de Protección de Datos, es posible fijar la sanción con base en estos criterios y los factores subjetivos -hechos- del caso en concreto sobre los parámetros objetivos fijados por la norma para efectos de tasación de multas.

En el caso en concreto, frente al literal (a), tal como ya se indicó, la utilización de la bases de datos de portabilidad numérica con una finalidad distinta y sin la autorización de los titulares de los datos personales allí recolectados es una afectación grave, no solo para el Régimen de Protección de Datos, sino para los derechos fundamentales de los titulares como sujetos especiales de protección del Régimen, en tanto, como ya se advirtió en su momento, CLARO realizó para titulares inscritos en el operador AVANTEL, solo en el período de julio de 2020 hasta la fecha en que se presentaron los Descargos, 5.658.820 llamadas no autorizadas utilizando los datos contenidos en la base de datos de portabilidad numérica, y que se individualizan de la siguiente manera:

Llamadas	Claro Móvil
Ago	647.284
Sep	599.542
Oct	455.948
Nov	568.207
Dic	725.579
Ene	694.128
Feb	861.077
Marzo	874.629
Abril	232.426
Total General	5.658.820

Elaboración propia

Esta operación, como ya se indicó fue aceptada por parte del Claro al indicar que sustrajo del Corte Inglés -base de datos de portabilidad numérica – alrededor de 100.000 número mensuales para efectos de migración de operador, siendo muchos más de los finalmente reconocidos; lo que evidencia que la actuación vulneradora de Claro no se concretizó a un número reducido de titulares, sino a millones de titulares por operador. Ahora, dada la falta de datos exactos en cuanto a las llamadas realizadas por parte de Claro a otros operadores, y teniendo en cuenta su sistematicidad, se considera que el radio de llamadas debió ser el mismo reportado por AVANTEL, con lo que se estima una afectación del mismo número para otros operadores, a lo que se le debe sumar que los datos de estos están disponibles para otros efectos por parte de los Call Center propios y tercerizados, sin que haya certeza de cuales otras utilidades se les pudo haber dado .

⁵⁴ Corte Constitucional [C.C.] SentenciaC-748/11, M.P. Jorge Ignacio Pretelt Chaljub, Gaceta de la Corte Constitucional [G. C. C.] (Vol. n/d, p. 40) (Colom.)

“Por la cual se impone una sanción y se imparte órdenes administrativas”

Este tipo de actuaciones no solo afecta a los titulares cuyos datos se encuentran dentro de la base de datos, sino una transgresión grave y puesta en riesgo grave de los derechos fundamentales de la sociedad colombiana, lo cual es suficiente para entender la gravedad de la conducta, sin necesidad de acudir a forzosos razonamientos complicadas, a fin de desentender o negar una verdad inconcusa, cual es la del quebrantamiento de derechos constitucionales, razón por la cual este Despacho sin ninguna duda considera que la vulneración del Régimen de Protección de Datos, y su bien jurídico protegido, el derecho fundamental de habeas data de millones de Colombianos fue deliberadamente y sistemáticamente transgredido, así como un asalto en la fe pública en relación a actividad de administración de datos, en particular los datos contenidos en una base de datos de portabilidad numérica de finalidad específica.

En cuanto al literal (b), o la ganancia o beneficio económica generado por parte de Claro, es necesario recordar nuevamente que la portabilidad numérica para los titulares es gratuita, y no debe generar costos en su solicitud, ya sea por el operador receptor o el donante; pero si genera costos de implementación y funcionamiento para los operadores que no deben ser cargados a los titulares, y cuya finalidad, es solo para efectos de la portabilidad, por lo que no puede ser utilizada para otros efectos. Sin embargo, Claro generó, posiblemente buscando un retorno a la pérdida de clientes por el efecto de la posibilidad de la portabilidad y los costos de operatividad del ADB, un proceso de capitalización de la base de datos a través de la captación masiva de clientes a través de tele mercadeo, por lo que se generó mensualmente millones de llamadas desde el 2018.

Ahora, si se tiene en cuenta, solo para efectos de los titulares de Avantel, el promedio de llamadas mensual reportado para el mes de abril de 2021, esto es 232.426 llamadas, y el promedio de planes post-pago⁵⁵ más económicos ofrecidos por Claro, esto es \$55.900, y que tan solo el 5% de los titulares llamados, sin autorización expresa, esto es 11.621 titulares, hubiesen migrado, se tendría un ingreso operaciones mensual para Claro de \$649.630.670, suma la cual multiplicada por hasta la fecha de esta sanción le generaría, un ingreso total desde abril de 2021, de: \$2.598.522.680. Ahora, si se tiene en cuenta que, si la operación se hubiese realizado dentro del número de llamadas mensuales que Claro reportó, 100.000 llamadas al mes, y se le aplica la misma operación anteriormente expuesta, se tiene como ingresos operacionales mensual, con solo el 5% de éxito en la portabilidad, un valor correspondiente a \$279.500.000, lo cual multiplicado por el tiempo en que se ejecutó la conducta 2018 a 2021 -48 meses-, asciende a un total de \$13.416.000.000, en promedio; lo que resulta solo ser un estimado para los efectos económicos a favor de Claro desde 2018, año en que se reportó la operación ilegal.

Frente a lo anterior, debe tenerse en cuenta la posición de Claro dentro del mercado de telefonía celular en Colombia, al tener un numero de 33.461.107 de abonados activos para el 2021⁵⁶, lo cual lo cataloga como el PRSTM con mayor número de abonados en el territorio, y por ende con más ingresos operacionales en relación a los servicios que presta, lo cual le permite desplegar los medios humanos y tecnológicos para la capitalización de la base de portabilidad numérica, sin tener cuenta los efectos negativos que su actividad puede tener sobre los derechos de titulares, en especial los derechos fundamentales, los cuales no pueden ceder bajo ninguna circunstancia a los intereses económicos de particulares. En todo caso, no debe olvidarse que el respeto de los Derechos Humanos es un elemento esencial de la democracia, por lo que su violación, sin importar el mecanismo por el cual se ejecute, es una conducta gravísima que no solo atenta contra los intereses de un individuo en particular sino de la sociedad en general, y se torna más grave cuando se busca la generación de un ingreso económico en perjuicio de la colectividad.

En conclusión, es evidente que Claro, a través de la campañas masivas de tele mercadeo, y en concreta utilización ilegal de la base de datos de portabilidad numérica, genero una ganancia económica significativa durante el período de 2018 a 2021, pero en perjuicio de los derechos fundamentales de los titulares cuya información se encontraba resguardada y sobre la cual no se solicitó autorización previa para iniciar el contacto e ignorando, cuando es expresa, su finalidad específica y acceso restringido.

⁵⁵ No se puede tener en cuenta pre-pago dado que las cifras varían de usuario a usuario.

⁵⁶ Datos Abiertos, “Telefonía Móvil abonados por Categoría” (Ago. 27, 2021, 2:46 PM), En: <https://www.datos.gov.co/Ciencia-Tecnolog-a-e-Innovaci-n/Telefon-a-M-vil-abonados-por-categor-a/nrst-mwx4>.

“Por la cual se impone una sanción y se imparte órdenes administrativas”

De esta manera, quedó demostrado que la sociedad investigada, COMUNICACIÓN CELULAR S.A. - COMCEL S.A. con NIT. 800.153.993-7, incumplió con el Régimen de Protección de Datos, razón por la cual se le

impondrá una sanción equivalente a NOVECIENTOS CINCUENTA MILLONES DE PESOS (\$950,000,000) correspondientes a a 26,165.0325 Unidades de Valor Tributario (“UVT”).

9.1.3. Otros criterios de graduación

Por ultimo se aclara que los criterios de graduación de la sanción señalados en los literales (c), y (d) del artículo 24 de la Ley 1581 de 2008 no serán tenidos en cuenta debido a que: (i) no hubo reincidencia en la comisión de la infracción; (ii) no hubo resistencia, negativa u obstrucción a la acción investigadora de la SIC, y; (iii) o hubo renuencia o desacato a cumplir las ordenes e instrucciones del Despacho. En todo caso, si existió un daño a los intereses jurídicos tutelados por la L.1581/12 y se reportó un beneficio económico para CLARO en cuanto los datos que reposan en la base de datos de portabilidad numérica fueron utilizados para hacer campañas para afiliación masiva de clientes de otros operadores de telefonía celular.

Para efectos de la dosificación de la sanción, y teniendo en cuenta los criterios anteriormente citados, tanto en sus elementos objetivos y subjetivos, y que la multa máxima posible a imponer es de 2000 SMMLV, de acuerdo con el artículo 23, literal (a) de la Ley 1581 de 2012, solo se impuso el correspondiente al 52,25% del máximo permitido.

DÉCIMO: RESPONSABILIDAD DEMOSTRADA (ACCOUNTABILITY) EN EL TRATAMIENTO DE DATOS PERSONALES.

La regulación colombiana le impone al Responsable o al Encargado del Tratamiento, la responsabilidad de garantizar la eficacia de los derechos del titular del dato, la cual no puede ser simbólica, ni limitarse únicamente a la formalidad. Por el contrario, debe ser real y demostrable. Al respecto, nuestra jurisprudencia ha determinado que *“existe un deber constitucional de administrar correctamente y de proteger los archivos y bases de datos que contengan información personal o socialmente relevante”*.⁵⁷

Adicionalmente, es importante resaltar que los responsables o encargados del tratamiento de los datos, no se convierten en dueños de los mismos como consecuencia del almacenamiento en sus bases o archivos. En efecto, al ejercer únicamente la mera tenencia de la información, solo tienen a su cargo el deber de administrarla de manera correcta, apropiada y acertada. Por consiguiente, si los sujetos mencionados actúan con negligencia o dolo, la consecuencia directa sería la afectación de los derechos humanos y fundamentales de los titulares de los datos.

En virtud de lo anterior, el Capítulo III del Decreto 1377 de 27 de junio de 2013 -incorporado en el Decreto Único Reglamentario 1074 de 2015- reglamenta algunos aspectos relacionados con el principio de responsabilidad demostrada. Por su parte, el artículo 26⁵⁸ -*Demostración*- establece que, *“los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012”*. Así, resulta imposible ignorar la forma en que el Responsable o Encargado del Tratamiento debe probar poner en funcionamiento medidas adecuadas, útiles y eficaces para cumplir la regulación. Es decir, se reivindica que un administrador no puede utilizar cualquier tipo de políticas o herramientas para dicho efecto, sino solo aquellas que tengan como propósito lograr que los postulados legales sean realidades verificables, y no solo se limiten a creaciones teóricas e intelectuales. El artículo 27- *Políticas Internas Efectivas*-, exige que los responsables del tratamiento de datos implementen medidas efectivas y apropiadas que garanticen, entre otras: *“(…) 3. La adopción de procesos para la*

⁵⁷ Corte Constitucional [C.C.] Sentencia T-227/03, M.P. Eduardo Montealegre Lynett, Gaceta de la Corte Constitucional [G. C. C.] (Vol. n/d, p. 12) (Colom.).

⁵⁸ D.1377/13, art. 26: El texto completo del artículo 26 del Decreto 1377 de 2013 ordena: *“Demostración. Los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este decreto, en una manera que sea proporcional a lo siguiente: (1) La naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente. (2) La naturaleza de los datos personales objeto del tratamiento. (3) El tipo de Tratamiento (4) Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares. En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, los Responsables deberán suministrar a esta una descripción de los procedimientos usados para la recolección de los datos personales, como también la descripción de las finalidades para las cuales esta información es recolectada y una explicación sobre la relevancia de los datos personales en cada caso. En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, quienes efectúen el Tratamiento de los datos personales deberán suministrar a esta de las medidas de seguridad apropiadas evidencia sobre la implementación efectiva*

“Por la cual se impone una sanción y se imparte órdenes administrativas”

atención y respuesta a consultas, peticiones y reclamos de los titulares, con respecto a cualquier aspecto del tratamiento.”⁵⁹

Con el propósito de dar orientaciones sobre la materia, la Superintendencia de Industria y Comercio expidió el 28 de mayo de 2015 la *“Guía para implementación del principio de responsabilidad demostrada (accountability)”*. El término *“accountability”*, a pesar de tener diferentes significados, ha sido entendido en el campo de la protección de datos como el modo en que una organización debe cumplir (en la práctica) las regulaciones sobre el tema, y la manera en que debe demostrar que lo puesto en práctica es útil, pertinente y eficiente.

Conforme con ese análisis, las recomendaciones que trae la guía a los obligados a cumplir la Ley 1581 de 2012, son:

- (1) Diseñar y activar un programa integral de gestión de datos (en adelante PIGDP). Esto, exige compromisos y acciones concretas de los directivos de la organización. Igualmente requiere la implementación de controles de diversa naturaleza;
- (2) Desarrollar un plan de revisión, supervisión, evaluación y control del PIGDP, y;
- (3) Demostrar el debido cumplimiento de la regulación sobre tratamiento de datos personales.

El principio de responsabilidad demostrada –*accountability*– demanda implementar acciones de diversa naturaleza para garantizar el correcto cumplimiento de los deberes que imponen las regulaciones sobre tratamiento de datos personales. El mismo, exige que los responsables y encargados del tratamiento adopten medidas apropiadas, efectivas y verificables que le permitan evidenciar la observancia de las normas sobre la materia. Dichas acciones o medidas, deben ser objeto de revisión y evaluación permanente para medir su nivel de eficacia y el grado de protección de los datos personales.

El principio de responsabilidad precisa menos retórica y más acción en el cumplimiento de los deberes que imponen las regulaciones sobre tratamiento de datos personales. Requiere apremiar acciones concretas por parte de las organizaciones para garantizar el debido tratamiento de los datos personales. El éxito del mismo, dependerá del compromiso real de todos los miembros de una organización. Especialmente, de los directivos de las organizaciones, pues, sin su apoyo sincero y decidido, cualquier esfuerzo será insuficiente para diseñar, llevar a cabo, revisar, actualizar y/o evaluar los programas de gestión de datos. Adicionalmente, el reto de las organizaciones frente al principio de responsabilidad demostrada va mucho más allá de la mera expedición de documentos o redacción de políticas. Como se ha manifestado, exige que se demuestre el cumplimiento real y efectivo en la práctica de sus funciones.

En este sentido, desde el año 2006 la Red Iberoamericana de Protección de Datos (RIPD) ha puesto de presente que, *“la autorregulación sólo [sic] redundará en beneficio real de las personas en la medida que sea bien concebida, aplicada y cuente con mecanismos que garanticen su cumplimiento de manera que **no se constituyan en meras declaraciones simbólicas de buenas intenciones sin que produzcan efectos concretos en la persona cuyos derechos y libertades pueden ser lesionados o amenazados por el tratamiento indebido de sus datos personales**”*.⁶⁰ (Énfasis añadido)

El principio de responsabilidad demostrada busca que los mandatos constitucionales y legales sobre tratamiento de datos personales sean una realidad verificable y redunden en beneficio de la protección de los derechos de las personas. Por eso, es crucial que los administradores de las organizaciones sean proactivos respecto del tratamiento de la información. De manera que, por iniciativa propia, adopten medidas estratégicas, idóneas y suficientes, que permitan garantizar: (i) los

⁵⁹ D.1377/13, art. 27: *“Políticas internas efectivas. En cada caso, de acuerdo con las circunstancias mencionadas en los numerales 1, 2, 3 y 4 del artículo 26 anterior, las medidas efectivas y apropiadas implementadas por el Responsable deben ser consistentes con las instrucciones impartidas por la Superintendencia de Industria y Comercio. Dichas políticas deberán garantizar: 1. La existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del responsable para la adopción e implementación de políticas consistentes con la Ley 1581 de 2012 y este decreto. 2. La adopción de mecanismos internos para poner en práctica estas políticas incluyendo herramientas de implementación, entrenamiento y programas de educación. 3. La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los Titulares, con respecto a cualquier aspecto del tratamiento. La verificación por parte de la Superintendencia de Industria y Comercio de la existencia de medidas y políticas específicas para el manejo adecuado de los datos personales que administra un Responsable será tenida en cuenta al momento de evaluar la imposición de sanciones por violación a los deberes y obligaciones establecidos en la ley y en el presente decreto”*.

⁶⁰ Red Iberoamericana de Protección de Datos. Grupo de trabajo temporal sobre autorregulación y protección de datos personales. Mayo de 5 de 2006. En aquel entonces, la RIPD expidió un documento sobre autorregulación y protección de datos personales que guarda cercana relación con *“accountability”* en la medida que la materialización del mismo depende, en gran parte, de lo que internamente realicen las organizaciones y definan en sus políticas o regulaciones internas.

derechos de los titulares de los datos personales, y; (ii) una gestión respetuosa de los derechos humanos

DÉCIMO PRIMERO: SOBRE LA POSIBLE AFECTACIÓN A LA LIBRE COMPETENCIA INSINUADA POR PARTE DE LOS TERCEROS INTERESADOS INTERVENIENTES EN LA ACTUACIÓN ADMINISTRATIVA

La sociedad TIGO manifestó que la actuación puede tener efectos a la libre competencia toda vez que CLARO actuó abusando de su acceso a la base de datos de portabilidad numérica y de su posición dominante en el mercado para lanzar una campaña de tele mercadeo para captar de forma masiva clientes de otros operadores de telefonía celular, razón por la cual la SIC debía pronunciarse de fondo.

Frente a esta solicitud, se debe indicar que si bien la SIC, es la autoridad nacional de competencia, lo cierto es que esta Delegatura no tiene las facultades para determinar si el actuar de CLARO tiene efectos anticompetitivos por abuso de posición dominante o cualquiera de los actos que se consideran como sujetos de la accionar de la autoridad, dado que la Delegatura se limita al ejercicio de sus funciones en el marco dado por la Ley 1581 de 2012, Decreto 1377 de 2013, Decreto Único Reglamentario 1074 de 2015, y las especificadas dadas por el Decreto 4886 de 2011. Sin embargo, dentro de sus funciones se encuentra remitir a cualquier otra autoridad los casos que considere que son de su competencia.

En el caso en específico se evidenció que CLARO actuó en clara contradicción del Régimen de Protección de Datos al darle otra finalidad a los datos contenidos en la base de datos de portabilidad numérica creada reglada por la C.R.C. Resolución 5050 de 2016, la cual estableció, con relación a la base de datos de portabilidad numérica, en su artículo 2.6.9.1., lo siguiente en materia sancionatoria: (i) Las infracciones, incumplimientos, o violación de las disposiciones legales, reglamentarias o regulatorias en esta materia serán sancionadas de acuerdo con lo previsto en el título IX de la Ley 1341 de 2009, esto es por parte del Ministerio de Tecnologías de la Información y las Comunicaciones; (ii) sin perjuicio de las sanciones que por infracción a las normas de promoción de la Competencia y Protección al usuario que le corresponda a la Superintendencia de Industria y Comercio, y; (iii) y por la infracción a lo previsto en el artículo 22, numeral 19 de la Ley 1341 de 2009 le corresponda a la Comisión de Regulación de Comunicaciones.

En virtud de esta disposición, se procederá a compulsar copia de la presente resolución a las siguientes entidades para que aboquen conocimiento en lo que les competa dentro de las funciones otorgadas por la Ley:

- (1) Ministerio de Tecnologías de la Información y las Comunicaciones;
- (2) Dirección de Investigaciones de Protección de Usuarios de Servicios de Comunicaciones de la Delegatura de Protección al Consumidor de la Superintendencia de Industria y Comercio, y;
- (3) Comisión de Regulación de Comunicaciones.

En cuanto a la remisión de la presente resolución al Grupo de Competencia Desleal y Propiedad Intelectual de la Delegatura de Asuntos Jurisdiccionales de la SIC, esta no es posible toda vez que se trata una acción judicial de carácter particular que debe ser incoada directamente por la parte afectada, por lo que, de quererse una declaración judicial sobre el referente, los terceros intervinientes y otros afectados, deberán realizar la radicación del escrito de demanda de forma individual.

DÉCIMO SEGUNDO: CONCLUSIONES

Son las siguientes las conclusiones del Despacho en relación con el caso en concreto, a saber:

- (1) El Régimen de Protección de Datos estableció que las bases de datos, de creación legal o privada, deben tener una finalidad específica y el tratamiento de la información allí contenida debe sujetarse a dicha finalidad, siendo deber de los Responsables informar a los titulares la finalidad de la recolección y procurar la autorización respectiva;

“Por la cual se impone una sanción y se imparte órdenes administrativas”

- (2) En el caso de la base de datos portabilidad numérica, su finalidad específica es la de lograr, con la interacción de la totalidad de los operadores de telefonía celular, la consecución de la portabilidad numérica de acuerdo con el plan nacional de portabilidad bajo criterios técnicos estándar. Razón por la cual se creó una base de datos operativa y otra administrativa, pública de carácter restringido, cuyos datos básicos son la totalidad de los números telefónicos de los afiliados de los operadores de telefonía celular, y los cuales son accesibles a los demás operadores para su consulta a través del programa denominado Gateway;
- (3) CLARO aprovechó el acceso a los datos -números telefónicos- de millones de titulares para realizar una campaña masiva de captación de clientes, a los cuales, una vez fueron contactados: (i) no se les informaba la fuente de donde obtuvieron su respectivo número; (ii) no se les solicitó la autorización en los términos prescritos por la ley, y; (iii) la autorización solo se requirió para aquellos titulares que mostraban interés en realizar el proceso de portabilidad, condicionando, en algunas circunstancias, la entrega de la información sobre posibles planes previa la otorgación de la autorización.
- (4) CLARO trató la información contenida en la base de datos de portabilidad numérica como una base de datos públicos, cuya información puede ser utilizada libremente, cuando en la realidad es una base de datos pública, por su creación legal, de acceso restringido y finalidad específica, y cuya información es solo para efectos de la portabilidad numérica.
- (5) CLARO, con las actuaciones descritas, desconoce el principio de accountability o responsabilidad demostrada en materia de protección de datos, en cuanto sus medidas humanas, tecnológicas y administrativas no son las propicias para garantizar la protección de los datos personales de los titulares a nivel nacional.

DÉCIMO PRIMERO: Que, como consecuencia de la situación actual, y teniendo en cuenta el Estado de Emergencia Económica, Social y Ecológica decretado por el Gobierno Nacional, se ha restringido el ingreso a las instalaciones de la Superintendencia, en consecuencia, se establecieron las medidas pertinentes para permitir el acceso completo a los expedientes por medios digitales.

Al punto se precisa que, con el fin de garantizar los derechos fundamentales de la sociedad comercial **COMUNICACIÓN CELULAR S.A. - COMCEL S.A.** con NIT. 800.153.993-7, **esta Dirección ha concedido el acceso al presente Expediente digital a esta**, por intermedio de su representante legal al correo electrónico: notificacionesclaro@claro.com.co y fernando.perdomoc@claro.com.co quien debe registrarse en calidad de persona natural, exclusivamente con los datos en mención, en el enlace <https://servicioslinea.sic.gov.co/servilinea/ServiLinea/Portada.php>.

En caso de que la sociedad requiera un acceso adicional de consulta del Expediente, deberá dirigir su solicitud en tal sentido desde el correo electrónico de notificación judicial de la sociedad, a los correos electrónicos contactenos@sic.gov.co y habeasdata@sic.gov.co, indicando los nombres y números de identificación de las personas autorizadas, **acreditando para dicho efecto los debidos poderes y/o autorizaciones, según corresponda.**

Finalmente, precisando que la totalidad del Expediente se encuentra digitalizado para su consulta por medios virtuales, si la sociedad investigada considera estrictamente necesario el acceso del Expediente en físico, deberá enviar un correo electrónico a la dirección de correo contactenos@sic.gov.co y habeasdata@sic.gov.co, solicitando la asignación de una cita para revisión física del Expediente en las instalaciones de la Superintendencia de Industria y Comercio en la ciudad de Bogotá D.C., indicando su número de radicado. Lo anterior por cuanto se deben garantizar el ingreso a las instalaciones con las adecuadas medidas de bioseguridad.

En mérito de lo expuesto, este Despacho,

RESUELVE

ARTÍCULO PRIMERO: Imponer una sanción pecuniaria a la sociedad comercial **COMUNICACIÓN CELULAR S.A. - COMCEL S.A.** con NIT. 800.153.993-7, correspondiente a NOVECIENTOS CINCUENTA MILLONES DE PESOS (\$950,000,000) correspondientes a 26,165.0325 Unidades de Valor Tributario (“UVT”), por violación en lo dispuesto en:

“Por la cual se impone una sanción y se imparte órdenes administrativas”

- Del principio de finalidad (Ley 1581 de 2012, artículo 4, literal (b)) y el deber de informar de forma debida sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada (Ley 1581 de 2012, artículo 17, literal (c)).
- Del principio de libertad (Ley 1581 de 2012, artículo 4, literal (c)) y el deber de solicitar y conservar copia de la respectiva autorización otorgada por el Titular en los términos establecidos por la ley (Ley 1581 de 2012, artículos 9 y 17, literal (b), Decreto 1377 de 2013, artículos 5, 7, y 8 -incorporado en el Decreto Único Reglamentario 1074 de 2015).

PARÁGRAFO: El valor de la sanción pecuniaria que por esta resolución se impone, deberá consignarse en efectivo o cheque de gerencia en el Banco Popular, Cuenta No. 050000249, a nombre de Dirección del Tesoro Nacional – Fondos Comunes, Código Rentístico No. 350300, Nit. 899999090-2. En el recibo deberá indicarse el número del expediente y el número de la presente resolución. El pago deberá acreditarse ante la pagaduría de esta Superintendencia, con el original de la consignación, dentro de los cinco (5) días hábiles siguientes a la ejecutoria de esta resolución.

ARTÍCULO SEGUNDO: ORDENAR a la sociedad comercial **COMUNICACIÓN CELULAR S.A. - COMCEL S.A.** con NIT. 800.153.993-7, abstenerse de continuar utilizando los números telefónicos contenidos en la Base de Portabilidad Numérica (BDO – BDA) para realizar campañas de telemarketing para la captación masiva de clientes de otros operadores de telefonía celular, y reducir su utilización para efectos de la portabilidad numérica solicitada directamente por parte de los titulares de otros operadores en sujeción a lo ordenado expresamente por la C.R.C. R.5050/16, y demás normas que la adicionen, modifiquen o deroguen.

ARTÍCULO TERCERO: ORDENAR a la sociedad comercial **COMUNICACIÓN CELULAR S.A. - COMCEL S.A.** con NIT. 800.153.993-7, proceda a la destrucción y/o eliminación, en conjunto con las copias remitidas a sus call center propios y contratados, de las bases de datos sub-producto de los datos personales contenidos en la base de datos por portabilidad numérica.

ARTÍCULO CUARTO: ORDENAR a la sociedad comercial **COMUNICACIÓN CELULAR S.A. - COMCEL S.A.** con NIT. 800.153.993-7, tomar las medidas humanas, administrativas y tecnológicas con el fin de que cualquier recolección y tratamiento de información que esta compañía se sujete a una finalidad específica y en sujeción al Régimen de Protección de Datos de modo que implemente la “*responsabilidad demostrada*” en los términos de cumplimiento de los principios y deberes de la Ley Estatutaria 1581 de 2012, y sus decretos reglamentarios, en especial sujeción al uso de base de datos dentro del marco de las finalidades específicas asignadas a estas.

ARTÍCULO QUINTO: COMUNICACIÓN CELULAR S.A. - COMCEL S.A. deberá cumplir lo ordenado en el artículo tercero de esta resolución dentro de los noventa (90) días siguientes a la ejecutoria del presente acto administrativo.

PARÁGRAFO: Para demostrar el cumplimiento deberá remitir una certificación suscrita por el representante legal **COMUNICACIÓN CELULAR S.A. - COMCEL S.A.**, en su calidad de Responsable, con la cual se acredite y evidencie la implementación de las medidas ordenadas.

ARTÍCULO SEXTO: Notificar personalmente el contenido de la presente resolución a la sociedad comercial **COMUNICACIÓN CELULAR S.A. - COMCEL S.A.**, entregándole copia de la misma e informándole que contra ella procede recurso de reposición ante el Director de Investigación de Protección de Datos personales y el de apelación ante el Superintendente Delegado para la Protección de Datos Personales, dentro de los diez (10) días siguientes a la diligencia de notificación.

ARTÍCULO SÉPTIMO: Notificar personalmente el contenido de la presente resolución a la sociedad comercial **COLOMBIA MÓVIL S.A. - ESP**, entregándole copia de la misma e informándole que contra ella procede recurso de reposición ante el Director de Investigación de Protección de Datos personales y el de apelación ante el Superintendente Delegado para la Protección de Datos Personales, dentro de los diez (10) días siguientes a la diligencia de notificación.

ARTÍCULO OCTAVO: Notificar personalmente el contenido de la presente resolución a la sociedad comercial **AVANTEL S.A.S. -EN REORGANIZACIÓN-**, entregándole copia de la misma e informándole que contra ella procede recurso de reposición ante el Director de Investigación de Protección de Datos personales y el de apelación ante el Superintendente Delegado para la Protección de Datos Personales, dentro de los diez (10) días siguientes a la diligencia de notificación.

"Por la cual se impone una sanción y se imparte órdenes administrativas"

ARTÍCULO NOVENO: REMITIR COPIA de la presente actuación a las siguientes entidades para que avoquen conocimiento en los que les corresponda:

- Ministerio de Tecnologías de la Información y las Comunicaciones;
- Dirección de Investigaciones de Protección de Usuarios de Servicios de Comunicaciones de la Delegatura de Protección al Consumidor de la Superintendencia de Industria y Comercio, y;
- Comisión de Regulación de Comunicaciones.

ARTÍCULO DÉCIMO: La Superintendencia de Industria y Comercio se permite recordar que los canales habilitados para que los investigados ejerzan sus derechos, den respuesta a requerimientos, interpongan recursos, entre otros, son:

- Correo de la Superintendencia de Industria y Comercio: contactenos@sic.gov.co

- Sede Principal: Carrera 13 No. 27 - 00, Pisos 1 y 3 en la ciudad de Bogotá de lunes a viernes de 8:00 a.m a 4:30 p.m.

NOTIFÍQUESE Y CÚMPLASE

Dada en Bogotá D. C., 20 OCTUBRE 2021

El Director de Investigación de Protección de Datos Personales,

CARLOS ENRIQUE SALAZAR MUÑOZ

Proyectó: JATS
Revisó: CESM
Aprobó: CESM

NOTIFICACIÓN:

Investigada:

Entidad: **COMUNICACIÓN CELULAR S.A. - COMCEL S.A.**

NIT.: 800.153.993-7

Representante Legal: **Hilda María Pardo Hasche**

Identificación: C.C. 41.662.356

Dirección: Carrera 68 número 24b -10

Ciudad: Bogotá D.C. – Colombia

Correo electrónico: notificacionesclaro@claro.com.co

Terceros:

Sociedad: **COLOMBIA MÓVIL S.A. - ESP**

NIT.: 830.114.921-1

Representante Legal: **Carolina Raquel Bernal**

Identificación: C.E. 1.016.500

Dirección: Calle 26 número 92 -31, módulo G1

Ciudad: Bogotá D.C. – Colombia

Correo electrónico: notificacionesjudiciales@tigo.com.co

Sociedad: **AVANTEL S.A.S. - EN REORGANIZACIÓN**

NIT.: 830.016.046-1

Representante Legal: **Alexandra Turbay Arango**

Identificación: C.C. 33.334.398

Dirección: Carrera 11 número 93 - 92

Ciudad: Bogotá D.C. – Colombia

Correo electrónico: notificacionesjudiciales@avantel.com.co