EXPEDIENTE: 032-02-2019-DEN **RESOLUCION N° 188-2021**

AGENCIA DE PROTECCIÓN DE DATOS DE LOS HABITANTES, DIRECCIÓN NACIONAL. San José a las 13:30 horas del 01 de junio de 2021. Conoce la Agencia de Protección de Datos de los Habitantes denuncia formulada por **[NOMBRE 1]** contra **ICOLLECT S.A.**

RESULTANDO:

1- Que en fecha 23 de abril de 2019, la señora **[NOMBRE 1]** presentó formal denuncia contra **Icollect S.A.,** cuya pretensión indica que: "(…) *Esta empresa ha estado enviando correos a un correo de mi trabajo la cual tienen acceso varios compañeros menos yo, revelando información personal mía y haciendo mal uso de mi información. Tengo entendido que son la gestionadora de crédito de Gollo, con quienes tuve una cuenta que desgraciadamente no pude cumplir junto con otras* (…)" (Visible a folios 01 al 11 del expediente administrativo).
2- Que mediante resolución N° 079-2019 de fecha 12 de marzo de 2019, se le da admisibilidad al procedimiento de protección de derechos. (Visible a folios 12 y 13).
3- Que mediante resolución N°147-2019 del 01 de abril del 2019, se realiza el traslado de cargos a Icollect S.A., a efecto de que se brinde informe sobre la veracidad de los cargos y aporten las pruebas que estimen pertinentes; la cual fue debidamente notificada el 10 de abril de 2019. (Visible a folios 14 al 16).
4- Que mediante oficio sin número y sin fecha, la empresa Icollect S.A., se refiere al traslado de cargos, el cual fue recibido en fecha 23 de abril de 2019, en las oficinas de la Prodhab. (Visible a folios 17 al 20).
5- Que se han analizado los aspectos de forma y fondo de este expediente y se han realizado las diligencias útiles y necesarias para el dictado de la presente Resolución Administrativa.

CONSIDERANDO:

I- HECHOS PROBADOS: Concluido el análisis de la denuncia presentada y los autos del expediente, de relevancia para la resolución del presente asunto se consideran los siguientes hechos:

1. Que la señora **[NOMBRE 1]** cuenta con una deuda con Gollo, cuya gestión de cobro la realiza la empresa Icollect S.A. (Ver folios 01 y 17)
2. Que la empresa Icollect S.A. envío un aviso de cobro al correo electrónico "información Brunca" que pertenece a la empresa para la que labora la señora **[NOMBRE 1]** y en el mismo indica: "Necesitamos de carácter urgente nos ayude con la entrega de esta notificación adjunta" (Ver folios 04 y 05)
3. Que en dicho aviso se hace referencia en su encabezado a la empresa Fiduciaria Brunca Sociedad Anónima, para la que trabaja la señora **[NOMBRE 1]** (Ver folio 05)

II- HECHOS NO PROBADOS: Ninguno de relevancia para la resolución del presente procedimiento.

III- SOBRE EL FONDO DE LA PRESENTE DENUNCIA: Señala la denunciante que *"Esta empresa ha estado enviando correos a un correo de mi trabajo la cual tienen acceso varios compañeros menos yo, revelando información personal mía y haciendo mal uso de mi información. Tengo entendido que son la gestionadora de crédito de Gollo, con quienes tuve una cuenta que desgraciadamente no pude cumplir junto con otras, por ello para honrar mis obligaciones tuve que abrir un proceso de insolvencia expediente* **[VALOR 1]** *(...)".* Por su parte el denunciado señala en su informe lo siguiente: *"Mi representada realiza acciones de cobro en nombre de diferentes empresas crediticias y son las empresas que nos facilitan la información de localización de sus clientes. Que en el registro de la gestión de cobro realizada a la deuda de la señora* **[NOMBRE 1]**, *no constan que se realizaran acciones de acoso agresivo a la denunciante. "(...) Mi representada rechaza haber realizado cualquier tipo de gestión acosadora o de cualquier otro tipo a la recurrente (...)".* Una vez valorado el expediente administrativo y las pruebas que constan en el mismo, se procede al análisis por el fondo desde los principios que contempla nuestra ley como lo son: el Autodeterminación Informativa, el consentimiento informado, adecuación al fin, el de calidad de la información, así como el tratamiento que se le debe de dar a los datos de acuerdo a su categoría. Ley No. 8968 de Protección de la Persona Frente al Tratamiento de sus Datos Personales, establece el Derecho Fundamental de Autodeterminación Informativa, el cual abarca el conjunto de principios y garantías relativas al legítimo tratamiento de los datos personales, con el objeto de controlar el flujo de informaciones que concierne a cada persona, derivado del derecho a la privacidad. Es por esta razón, que debe acatarse de forma obligatoria lo que establece dicha normativa, para realizar un tratamiento de datos personales de forma licita, a saber los artículos 3 y 5 de Ley N° 8968, como se detalla a continuación: ***"Artículo 3.- Definiciones****. Para los efectos de la presente ley se define lo siguiente:* ***a)*** *Base de datos: cualquier archivo, fichero, registro u otro conjunto estructurado de datos personales, que sean objeto de tratamiento o procesamiento, automatizado o manuales, cualquiera que sea la modalidad de su elaboración, organización o acceso***. *b) Datos personales: cualquier dato relativo a una persona física identificada o identificable. c) Datos personales de acceso irrestricto: los contenidos en bases de datos públicas de acceso general, según dispongan leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados. d) Datos personales de acceso restringido: los que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública. e) Datos sensibles: información relativa al fuero íntimo de la persona, como por ejemplo los que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros. f) Deber de confidencialidad: obligación de los responsables de bases de datos, personal a su cargo y del personal de la Agencia de Protección de Datos de los Habitantes (Prodhab), de guardar la confidencialidad con ocasión del ejercicio de las facultades dadas por esta ley, principalmente cuando se acceda a información sobre datos personales y sensibles. Esta obligación perdurará aun después de finalizada la relación con la base de datos. g) Interesado: persona física, titular de los datos que sean objeto del tratamiento automatizado o manual. h) Responsable de la base de datos: persona física o jurídica que administre, gerencie o se encargue de la base de datos, ya sea esta una entidad pública o privada, competente, con arreglo a la ley, para decidir cuál es la finalidad de la base de datos, cuáles categorías de datos de carácter personal deberán registrase y qué tipo de tratamiento se les aplicarán. i) Tratamiento de datos personales: cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o manuales y aplicadas a datos personales, tales como la recolección, el registro, la*

organización, la conservación, la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a estos, el cotejo o la interconexión, así como su bloqueo, supresión o destrucción, entre otros. (Subrayado y resaltado no es del original). ***"Artículo 5.-*** *Principio de consentimiento informado. 1.- Obligación de informar…Quien recopile datos personales deberá obtener el consentimiento expreso de la persona titular de los datos o de su representante. Este consentimiento deberá constar por escrito, ya sea en un documento físico o electrónico, el cual podrá ser revocado de la misma forma, sin efecto retroactivo. No será necesario el consentimiento expreso cuando: a) Exista orden fundamentada, dictada por autoridad judicial competente o acuerdo adoptado por una comisión especial de investigación de la Asamblea Legislativa en el ejercicio de su cargo. b) Se trate de datos personales de acceso irrestricto, obtenidos de fuentes de acceso público general. c) Los datos deban ser entregados por disposición constitucional o legal. Se prohíbe el acopio de datos sin el consentimiento informado de la persona, o bien, adquiridos por medios fraudulentos, desleales o ilícitos."* (Subrayado y resaltado no es del original). Así las cosas y en estricto apego a dicha normativa, quien requiera hacer tratamiento de datos personales; deberá obtener de su titular el consentimiento informado, con excepción de aquellas situaciones en las que no se requiera según se indica en el numeral citado anteriormente. Sobre el caso en particular el denunciado indica en sus alegatos de descargo que: *"Mi representada realiza acciones de cobro en nombre de diferentes empresas crediticias y son las empresas que nos facilitan la información de localización de sus clientes (…)".* De los argumentos antes expuestos, se puede comprobar que se están trasmitiendo datos personales de una empresa a otra sin el consentimiento del titular y utilizándose para un fin distinto al que fue consentido inicialmente, lo cual incumple con lo establecido en el artículo 6 de Ley N° 8968 inciso 4. Para dar tratamiento a datos personales implica que se cuente con las medidas y regulaciones necesarias para el resguardo de los datos personales y no se llegue a vulneraciones como las que se visualizan del presente caso. Sobre el particular la Procuraduría General de la República, se refirió a este tema en el dictamen C-090-2013 de fecha 28 de mayo, 2013, el cual cita en lo que nos interesa lo siguiente: *"Aunado a lo anterior, al responsable de la base de datos se le impone un deber de adoptar las medidas de índole técnica y de organización necesarias con el objeto de garantizar la seguridad de los datos personales y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado, así como cualquier otra acción contraria a la Ley en mención, contemplando como mínimo dentro de esas medidas, los mecanismos de seguridad física y lógica más adecuados acordes con el desarrollo tecnológico que impere en el momento dado. Asimismo, sobre dichos responsables y quienes participen en cualquier fase del proceso de tratamiento de datos personales, recae en correspondencia con esa información, un deber de confidencialidad sea por su condición profesional o funcional (artículo 11 LPData). Disposiciones todas que responden a la jurisprudencia constitucional. En efecto, la Sala sistematizó los principios a que se sujeta la autodeterminación informativa. Así, en la resolución 910-2009 de 13:36 hrs. de 23 de enero de 2009, dicho Tribunal manifestó: "La ampliación del ámbito protector del derecho a la intimidad surge como una respuesta al ambiente global de fluidez informativa actual, ambiente que ha puesto en entredicho las fórmulas tradicionales de protección a los datos personales, para evolucionar en atención a la necesidad de utilizar nuevas herramientas que permitan garantizar el derecho fundamental de los ciudadanos a decidir quién, cuándo, dónde y bajo qué y cuáles circunstancias tiene contacto con sus datos. Es reconocido así el derecho fundamental de toda persona física o jurídica a conocer lo que conste sobre ella, sus bienes o derechos en cualquier registro o archivo, de toda naturaleza, incluso mecánica, electrónica o informatizada, sea pública o privada; así como la finalidad a que esa información se destine y a que sea empleada únicamente para dicho fin, el cual dependerá de la naturaleza del registro en cuestión. Da derecho también a que la información sea rectificada, actualizada, complementada o suprimida, cuando la misma sea incorrecta*

o inexacta, o esté siendo empleada para fin distinto del que legítimamente puede cumplir. Es la llamada protección a la autodeterminación informativa de las personas, la cual rebasa su simple ámbito de intimidad. Se concede al ciudadano el derecho a estar informado del procesamiento de los datos y de los fines que con él se pretende alcanzar, junto con el derecho de acceso, corrección o eliminación en caso el que se le cause un perjuicio ilegítimo. El derecho de autodeterminación informativa tiene como base los siguientes principios: el de transparencia sobre el tipo, dimensión o fines del procesamiento de los datos guardados; el de correspondencia entre los fines y el uso del almacenamiento y empleo de la información; el de exactitud, veracidad, actualidad y plena identificación de los datos guardados; de prohibición del procesamiento de datos relativos a la esfera íntima del ciudadano (raza, creencias religiosas, afinidad política, preferencias sexuales, entre otras) por parte de entidades no expresamente autorizadas para ello; y de todos modos, el uso que la información se haga debe acorde con lo que con ella se persigue; la destrucción de datos personales una vez que haya sido cumplidos el fin para el que fueron recopilados; entre otros. La esfera privada ya no se reduce al domicilio o a las comunicaciones, sino que es factible preguntarse si es comprensible incluir "la protección de la información" para reconocerle al ciudadano una tutela a la intimidad que implique la posibilidad de controlar la información que lo pueda afectar. ...La tutela a la intimidad implica, la posibilidad real y efectiva para el ciudadano de saber cuáles datos suyos están siendo tratados, con qué fines, por cuáles personas, bajo qué circunstancias, para que pueda ejercer el control correspondiente sobre la información que se distribuye y que lo afecta (artículos 24 de la Constitución Política y 13 inciso 1 de la Convención Americana de Derechos Humanos). En resumen, se deduce entonces que la autodeterminación informativa es una ampliación del derecho a la intimidad y que su protección surge a partir del desarrollo de mecanismos informáticos y tecnológicos globales que manejan bases de datos que contienen información de las personas. Respecto de la delimitación del contenido del derecho de autodeterminación informativa es importante acotar que para que la información sea almacenada de forma legítima, debe cumplir al menos con los siguientes requisitos: primero no debe versar sobre información de carácter estrictamente privado o de la esfera íntima de las personas; segundo debe ser información exacta y veraz (v. sentencia #2000-1119 de las 18:51 horas del 1° de febrero de 2000) y tercero la persona tiene el derecho de conocer la información y exigir que sea rectificada, actualizada, complementada o suprimida, cuando sea incorrecta o inexacta, o esté siendo empleada para fin distinto del que legítimamente puede cumplir (v. sentencias #2007-6793 de las 11:24 horas del 18 de mayo del 2007 y #2008-10114 de las 19:18 horas del 17 de junio de 2008) (...)". Por otra parte, es responsabilidad de quienes realizan tratamiento de datos, llámese responsable o encargado de la base de datos, conocer y aplicar en el manejo de datos personales los principios establecidos en la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, de allí que establecen los artículos 10, 11 y 12 de la misma lo siguiente: ***"Artículo 10.- Seguridad de los datos****. El responsable de la base de datos deberá adoptar las medidas de índole técnica y de organización necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado, así como cualquier otra acción contraria a esta ley. Dichas medidas deberán incluir, al menos, los mecanismos de seguridad física y lógica más adecuados de acuerdo con el desarrollo tecnológico actual, para garantizar la protección de la información almacenada. No se registrarán datos personales en bases de datos que no reúnan las condiciones que garanticen plenamente su seguridad e integridad, así como la de los centros de tratamiento, equipos, sistemas y programas. Por vía de reglamento se establecerán los requisitos y las condiciones que deban reunir las bases de datos automatizadas y manuales, y de las personas que intervengan en el acopio,*

almacenamiento y uso de los datos." ***"Artículo 11.- Deber de confidencialidad****. La persona responsable y quienes intervengan en cualquier fase del tratamiento de datos personales están obligadas al secreto profesional o funcional, aun después de finalizada su relación con la base de datos. La persona obligada podrá ser relevado del deber de secreto por decisión judicial en lo estrictamente necesario y dentro de la causa que conoce."* ***"Artículo 12.- Protocolos de actuación****. Las personas físicas y jurídicas, públicas y privadas, que tengan entre sus funciones la recolección, el almacenamiento y el uso de datos personales, podrán emitir un protocolo de actuación en el cual establecerán los pasos que deberán seguir en la recolección, el almacenamiento y el manejo de los datos personales, de conformidad con las reglas previstas en esta ley..."* (Subrayado y resaltado no es del original). Los aspectos antes citados, son de indispensable cumplimiento por aquellas empresas que realizan tratamiento de datos personales entre sus funciones; en un escenario ideal no debería de presentarse usos no autorizados de datos personales sensibles, menos aún si no se tiene claridad de su actualidad, veracidad, exactitud o inadecuación al fin, ya que es el responsable de las bases de datos a quien corresponde adecuar sus bases al cumplimiento de la ley. Así mismo, es importante aclarar que una base de datos, puede ser cualquier archivo, fichero registro u otro conjunto estructurado de datos personales que sean objeto de tratamiento o procesamiento automatizado o manuales, cualquiera que sea la modalidad de su colaboración, organización o acceso, por lo que al indicar la empresa Icollect S.A., lo siguiente: "(…) *realiza acciones de cobro en nombre de diferentes empresas crediticias y son las empresas que nos facilitan la información de localización de sus clientes* se pude determinar que se dio una transmisión de datos, recolección y almacenamiento de datos sin el consentimiento informado de la señora **[NOMBRE 1]** , para poder realizar la gestión de cobro. En cuanto a lo alegado por el denunciado con respecto a que*:* "*Que en el registro de la gestión de cobro realizada a la deuda de la señora* **[NOMBRE 1]**, *no constan que se realizaran acciones de acoso agresivo a la denunciante.* Según lo antes expuesto, y acorde con lo argumentado por la denunciante, téngase en cuenta el principio calidad de la información, contemplado en el artículo 6 de Ley 8968, el cual indica que solo podrán ser recolectados, almacenados o empleados datos de carácter personal, para su tratamiento automatizado o manual cuando tales datos sean actuales, veraces exactos y adecuados al fin para el que fueron recolectados. Es por lo antes expuesto, que nos es de importancia explicar el concepto de consentimiento informado, el cual es el derecho que tiene los ciudadanos a que se les comunique sobre los tratamientos que se les darán a sus datos personales, el cual tiene una relación directa con el derecho a la intimidad y con el derecho de la autodeterminación informativa. Con la protección de estos derechos lo que se busca es garantizarle al ciudadano, el control sobre el manejo de sus datos personales. Control que constituye a su vez una garantía de libertad individual al otorgarle al individuo la posibilidad de fiscalizar quién está haciendo un tratamiento de sus datos personales y con qué objetivo se realiza el referido tratamiento. Pero, además, son derechos dirigidos a proteger la identidad de las personas ya que no sólo otorga la posibilidad de conocer los datos personales que ostenten terceros, sino de "traer" esos datos, de corregirlos o rectificarlos en el caso de que sean incorrectos o de solicitar su eliminación en caso de que no sean necesarios para los fines para los cuales fueron recabados inicialmente. El respeto a los derechos antes mencionados, se fundamentan en el consentimiento del individuo, como regla general, para que determinada información sea recabada y se garantice que la información que conste en diferentes archivos o bases de datos no se utilice con fines diferentes y que estos sean legítimos y lícitos. Es por lo anterior, que el enviar información sensible al correo electrónico de la empresa para la que labora la señora **[NOMBRE 1]**, cuya cuenta no es administrada, ni fue consentida por la denunciante para que se le remitiera información; como puede evidenciarse a folio 01, en el que se indica: *"(…) Esta empresa ha estado enviando correos a un correo*

de mi trabajo la cual tienen acceso varios compañeros menos yo (...)". Así las cosas, la forma de cobro que realiza la empresa como consta a folios 05 y 06, contraviene lo establecido en el artículo 9 inciso 1 y 4 de la Ley 8968, dado que se da una evidente violación al derecho de la autodeterminación informativa, el principio de calidad de la información y el principio del consentimiento informado, los cuales fueron ampliamente desarrollados. Así las cosas y visto lo anterior, es deber de esta Agencia en su facultad otorgada por ley de garantizar el derecho a la Autodeterminación Informativa acoger la denuncia interpuesta, siendo que se logra demostrar efectivamente que la empresa Icollect S.A. no dio un adecuado uso a los datos personales, al no contar con el consentimiento informado de la denunciante y el haberse usado dicha información para un fin distinto al consentido por la señora **[NOMBRE 1]**. Aunado a lo anterior, resulta necesario hhacer un llamado de atención a esta empresa para que se cumpla con la aplicación de los principios y prerrogativas que establece la ley N° 8968, se proceda a revisar las políticas que se utilizan en su base de datos para que la recopilación y ulterior tratamiento de datos personales de sus clientes, se lleve a cabo en el marco de la legalidad y las mejores prácticas.

POR TANTO

Con fundamento en los numerales 4, 5, 6, 9,16 inciso e) de la Ley N° 8968; y los artículos 12, 58, siguientes y concordantes del Reglamento No. 37.554-JP a dicha Ley:

1- Se declara con lugar la denuncia interpuesta por **[NOMBRE 1]** contra **Icollect S.A**
2- Se ordena Icollect S.A. a suprimir los datos personales sensibles señalados por señora **[NOMBRE 1]**.
3- De conformidad con la Ley No. 8968, contra este acto procede el Recursos de Reconsideración mismo que deberá interponerse en el plazo de tres días hábiles a partir de la notificación, de la presente notificación. ***NOTIFIQUESE.***

Licda. Elizabeth Mora Elizondo
Directora Nacional
Agencia de Protección de Datos de los Habitantes
PRODHAB