



EXPEDIENTE: 108-10-2018-DEN

RESOLUCIÓN N° 193-2021

AGENCIA DE PROTECCIÓN DE DATOS DE LOS HABITANTES, DIRECCIÓN NACIONAL.

San José a las 15:45 horas del 01 de junio de 2021. Conoce la Agencia de Protección de Datos de los Habitantes denuncia formulada por [NOMBRE 1] contra **INSTACREDIT S.A.**

RESULTANDO:

- 1- Que en fecha 23 de octubre de 2018, la señora [NOMBRE 1] presentó formal denuncia contra **Instacredit S.A.**, cuya pretensión indica que: *“Adquirió una deuda y que por su estabilidad laboral se atrasó y que debido a ello esta entidad ha llegado a métodos extremos para la gestión de cobranza de dicha deuda exponiendo públicamente mi situación financiera a terceras. personas (Visible a folios 01 al 10 del expediente administrativo).*
- 2- Que mediante resolución N° **298-2018** de fecha 01 de noviembre de 2018, se le da admisibilidad al procedimiento de protección de derechos. (Visible a folios 11 y 12).
- 3- Que mediante resolución N° **115-2019** del 22 de marzo del 2019, se realiza el traslado de cargos a **Instacredit 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 22 de marzo de 2019. (Visible a folios 13 al 15).
- 4- Que mediante oficio sin número y sin fecha, la empresa **Instacredit S.A.**, se refiere al traslado de cargos, el cual fue recibido en fecha 22 de marzo de 2019, en las oficinas de la Prodhab. (Visible a folios 16 al 19).
- 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 Instacredit S.A. (Ver folios 01 y 16).
2. Que la empresa Instacredit S.A., envió avisos de cobro a las cuentas de correo electrónico tanto de Capital Humano como a info@lapiedad.co.cr (Ver folios 04 al 10).

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

SOBRE EL FONDO DE LA PRESENTE DENUNCIA: Señala la denunciante que *“Adquirió una deuda y que por su estabilidad laboral se atrasó y que debido a ello esta entidad ha llegado a métodos extremos para la gestión de cobranza de dicha deuda exponiendo públicamente su situación financiera a terceras personas de la siguiente manera: “Que el 05 de setiembre llegaron a mi lugar de trabajo y entregaron una certificación prejudicial a una de mis compañeras. El 12 de setiembre llegaron a mi trabajo, esta vez me entregaron la notificación a mí, pero no conformes con eso enviaron la misma notificación al Departamento de Recursos Humanos... En ese momento no había completado mi periodo de prueba en dicha empresa y yo laboro para el área financiera por lo que es sumamente delicado que a uno lo expongan de esa manera. El 09 de octubre del 2018, nuevamente vuelven a enviar un comunicado a mi empresa esta vez lo enviaron a los correos de Recursos Humanos y también a*



info@lapiedad.co.cr, este correo está en la página web, el mismo le llega a varias personas de la empresa y los asistentes de Gerencia se lo hicieron llegar a mi jefatura directa con copia a mi persona y al departamento de recursos humanos, no puedo explicar lo mal que me hicieron sentir. Por su parte el denunciado señala en su informe lo siguiente: (...) Efectivamente la señora **[NOMBRE 1]** tiene un crédito vigente y en mora con mi representada 2. No es cierto que el personal de mi representada actué de esta forma para cobrar las deudas que tienen nuestros clientes con Instacredit S.A.3. No nos consta que lo aduce (sic) la señora **[NOMBRE 1]**, ella indica días específicos de visitas a su trabajo, departamentos que se visitaron y hasta afirma de correos que se enviaron a algunos departamentos de la empresa, también se refiere a pagos que realizó a la empresa Instacredit, además habla de otros puntos que desconocemos por ser únicamente manifestaciones de la señora **[NOMBRE 1]** que no tenemos conocimiento, ni se pueden comprobar. Nuevamente la señora **[NOMBRE 1]** aduce que se le envían mensajes de cobro en fechas determinadas a departamentos de su empresa, lo cual desconocemos y no se respalda con documentación idónea que haga constar que los representantes de la empresa Instacredit S.A. ". Una vez valorado el expediente administrativo y las pruebas que constan en el mismo, es de importancia indicar Ley 8968 de Protección de la Persona Frente al Tratamiento de sus Datos Personales, establece el artículo 4, de dicha ley se establece el Derecho Fundamental de Autodeterminación Informativa, el cual abarca el conjunto de principios y garantías relativas al legítimo tratamiento de los datos personales de la persona física, 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 lícita. En este sentido, es deber de esta Agencia manifestar, que, para poder dar tratamiento a un dato personal, se debe contar con un fin para la solicitud de datos personales, y el consentimiento informado del titular de los datos, siendo necesario el mismo, si lo que se va a dar tratamiento a datos sensibles, según lo que establece los artículos 3 y 5 de Ley N° 8968. 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: "1. No es cierto que el personal de mi representada actúe de esta forma para cobrar las deudas que tienen nuestros clientes con Instacredit S.A. 2. No nos consta que lo aduce (sic) la señora **[NOMBRE 1]**, ella indica días específicos de visitas a su trabajo, departamentos que se visitaron y hasta afirma de correos que se enviaron a algunos departamentos de la empresa (...) ". El principio del consentimiento informado, contenido en la Ley No. 8968 supra indicada, señala que 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 controlar quién está realizando tratamiento de sus datos personales y con qué finalidad. 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 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 a los autorizados, 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 folios 01 y 02, en el que se indica: “(...)El 09 de octubre del 2018, nuevamente vuelven a enviar un comunicado a mi empresa esta vez lo enviaron a los correos de Recursos Humanos y también a info@lapiedad.co.cr, este correo está en la página web, el mismo le llega a varias personas de la empresa y los asistentes de Gerencia se lo hicieron llegar a mi jefatura directa con copia a mi persona y al departamento de recursos humanos, no puedo explicar lo mal que me hicieron sentir (...)”. Se evidencia que efectivamente se están utilizando datos personales sin el consentimiento del titular, violentando el principio de la 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. Así las cosas, la forma de cobro que realiza la empresa Instacredit S.A. como consta a folios 04 al 09, 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, antes indicados. El tratamiento de 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 en el 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 rectificadora, 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 (...)"

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, en sus artículos 10, 11 y 12. Los cuales señalan: **“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. En cuanto a lo argumentado por el denunciado referente a la prueba aportada, debe de indicarse que el artículo 60 del Reglamento a la Ley No. 8968, señala: **Artículo 60. Requisitos de la denuncia.** *La solicitud de protección de datos deberá contener lo siguiente: a) Nombres, apellidos y calidades del titular o denunciante; b) Nombre del dueño o responsable o de la base de datos o bien cualquier elemento que permita identificar al denunciado; c) Hechos en que se funde la denuncia expuestos uno por uno, enumerados y bien especificados, en forma clara y precisa; d) Copia de la solicitud del ejercicio de derechos que corresponda, así como copia de los documentos anexos para cada una de las partes, de ser el caso; e) Documento en que conste la respuesta a su gestión, de ser el caso; f) En el supuesto en que impugne la falta de respuesta, deberá acompañar una copia en la que conste el acuse o constancia de recepción de la solicitud del ejercicio de derechos; g) Las pruebas documentales o pertinentes; h) Pretensión que formule; i) Señalamiento de medios para recibir notificaciones; j) Cualquier otro documento que considere procedente someter a juicio de la Agencia. Por otra parte, establece esta misma ley: Artículo 68. Medios de prueba. Los medios de prueba serán los siguientes: a. Documental físico o electrónico; b. El resultado de un estudio pericial; c. Declaraciones juradas de los testigos, debidamente autenticadas; Las pruebas de cargo y de descargo deberán ser presentadas junto con la denuncia o la contestación, según corresponda.* Nótese que el único requisito formal que ordena la ley, es que en caso de que haya declaraciones de testigos, éstas deben ser debidamente autenticadas (cuando el denunciante lo quiera aportar como prueba), y esto cobra sentido cuando vemos que, al tratarse de un proceso sumario, no se consideran en estos procedimientos la celebración de audiencias de recepción de prueba. Además, debe tenerse en cuenta que nos encontramos ante un procedimiento de naturaleza administrativa, mismos que se encuentran regulados por una serie de principios, entre ellos el informalismo, mismo que pretende que no existan rigurosidades formales que tiendan a entorpecer, suspender o paralizar el procedimiento, y más bien que se impongan reglas de celeridad y simplicidad, los cuales tienden a evitar trámites lentos, costosos y complejos que impidan el desenvolvimiento del procedimiento administrativo, por lo que el trámite del expediente debe hacerse de forma rápida, simple, célere y eficiente, siempre acorde con el ordenamiento jurídico y la eventual afectación al encausado. Asimismo, implica una elasticidad e interpretación informal de las normas del procedimiento en tanto beneficien al administrado. Todo lo anterior se encuentra regulado en los artículos 221, 222, 224, 225, 260, 269, 292 y 304 de la LGAP. 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 y acoger la denuncia interpuesta, siendo que se logra demostrar efectivamente que la empresa Instacredit S.A. no les 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 hacer 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, dado la gran cantidad de denuncias que contra esta misma empresa se tramitan en esta Agencia, lo cual denota desconocimiento de los alcances de la Ley No. 8968



PRODHAB
AGENCIA DE PROTECCIÓN DE
DATOS DE LOS HABITANTES
MINISTERIO DE JUSTICIA Y PAZ

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 **Instacredit S.A.**, y se ordena a la empresa denunciada abstenerse de realizar gestiones de cobros por medios no autorizados por su titular.
- 2- 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