**EXPEDIENTE: 017-02-2018-DEN** **RESOLUCION N° 187-2021**

**AGENCIA DE PROTECCIÓN DE DATOS DE LOS HABITANTES, DIRECCIÓN NACIONAL.** San José a las 12:00 horas del 01 de junio de 2021. Conoce la Agencia de Protección de Datos de los Habitantes denuncia formulada por **[NOMBRE1]** contra **COBRO E INVESTIGACIÓN CREDITICIA COINCRE S.A (COINCRE S.A.)**

## RESULTANDO:

**1-** Que mediante resolución final N° 03 de fecha veinte de setiembre de 2017 del expediente N°031-05-2017, se dispuso la apertura de oficio del procedimiento administrativo contra Cobro e Investigación Crediticia Coincre S.A. en adelante Coincre S.A, en favor de la señora **[NOMBRE1]**. (Visible a folios 41 al 45 del expediente administrativo 031-05-2017-DEN).
**2-** Que mediante oficio APD-DRABD-01-2018 de fecha veintiséis de enero de 2018, la Jefa del Departamento de Archivo y Registro de Bases de Datos; ordena iniciar de oficio, el procedimiento de protección de derechos contra Cobro e Investigación Crediticia Coincre S.A. de conformidad con la resolución N° 03 de fecha 20 de setiembre de 2017. (Visible a folios 01 al 04 del expediente administrativo).
**3-** Que mediante resolución N° 050-2018 de fecha dos de abril de 2018, se le da admisibilidad al procedimiento de protección de derechos. (Visible a folios 19 al 20 del expediente administrativo).
**4-** Que mediante resolución N°140-2018 del 16 de julio del 2018, se realiza el traslado de cargos a Coincre 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 14 de setiembre de 2018. (Visible a folios 21 al 24).
**5-** Que mediante oficio sin número y sin fecha, Coincre S.A., se refiere al traslado de cargos, el cual fue recibido en fecha diecinueve de setiembre de 2018, en las oficinas de la Prodhab. (Visible a folios 25 al 28).
**6-** 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 **[NOMBRE1]** fue cliente de TIGO STAR, la cual que fue desconectada, por falta de pago de sus obligaciones (Ver folio 08)

**2.** Que la gestión de cobro le fue trasladada a la empresa Coincre S.A. desde el 09 de diciembre de 2016 (Ver folios 06 y 10)
**3.** Que la señora **[NOMBRE1]** laboraba para la empresa LystoCard, cuando sucedieron los hechos (Ver folio 10)
**4.** Que la empresa Coincre S.A., envío un aviso de cobro al correo electrónico servicioalcliente@lystocard.com de la señora **[NOMBRE1]**, tomado de la red social Facebook. (Ver folio 10)

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

**III. EN CUANTO A LA CADUCIDAD:** Alega el denunciante que "*opone la Excepción de Caducidad del Procedimiento, reguladas en al artículo 340 inciso 1 de la Ley General de la Administración Pública, dado que en fecha 20 de setiembre del año 2017, se ordena iniciar de oficio un procedimiento administrativo contra mi representada y que posteriormente Prodhab mediante la resolución 140-2018 de las 8:45 horas del 16 de julio del 2018, procede a iniciar el procedimiento en contra de Coincre y que la misma fue notificada el 14 de septiembre del 2018, nótese que transcurrieron 10 meses entre la resolución que ordena la apertura del procedimiento de oficio y el momento en que formalmente inicia dicho proceso*". Es de gran importancia aclarar que la resolución que se menciona de fecha 20 de setiembre del año 2017, es de un expediente en el que el denunciado, no formaba parte en el proceso, la cual concluía con la denuncia tramitada en el expediente N° 031-05-2017-DEN. Que la apertura del procedimiento formal inició con la resolución N° 050-2018 de las ocho horas del dos de abril de 2018, que consta a folio 19 del expediente administrativo, en el que se da la admisibilidad del procedimiento de protección de derechos, de conformidad con el artículo 63 del Reglamento a la Ley N° 8968 y que posteriormente se le hace el traslado de cargos mediante resolución N° 140-2018 de fecha 16 de julio del 2018, la cual fue notificada efectivamente el 14 de setiembre de 2018, de forma personal dado que no se encontraba la dirección del denunciado. Una vez aclarado lo argumentado por el denunciante conviene indicar, que la Ley 6227 en los artículos 339 y 340 regula la figura de la caducidad del procedimiento, de la siguiente forma: *Artículo 339.- 1. Tanto el desistimiento como la renuncia han de hacerse por escrito. 2. La Administración aceptará de plano el desistimiento o la renuncia, salvo que, habiéndose apersonado otros interesados, instaren éstos la continuación en el plazo de diez días desde que fueron notificados de una y otra. 3. Si la cuestión suscitada por el expediente entrañare un interés general, o fuere conveniente sustanciarla para su definición y esclarecimiento, la Administración limitará los efectos del desistimiento o la renuncia a sus posibles consecuencias patrimoniales respecto del interesado, y seguirá el procedimiento en lo demás. Artículo 340.- 1) Cuando el procedimiento se paralice por más de seis meses en virtud de causa, imputable exclusivamente al interesado que lo haya promovido o a la Administración que lo haya iniciado, de oficio o por denuncia, se producirá la caducidad y se ordenará su archivo, a menos que se trate del caso previsto en el párrafo final del artículo 339 de este Código. 2) No procederá la caducidad del procedimiento iniciado a gestión de parte, cuando el interesado haya dejado de gestionar por haberse operado el silencio positivo o negativo, o cuando el expediente se encuentre listo para dictar el acto final. 3) La caducidad del procedimiento administrativo no extingue el derecho de las partes; pero los procedimientos se tienen por no seguidos, para los efectos de interrumpir la prescripción. (Así reformado por el artículo 200, incido 10) de la Ley N° 8508 de 28 de abril de 2006, Código Procesal Contencioso-Administrativo).*" El artículo 340 supra transcrito, es claro en establecer los requisitos que deben examinarse para que opere la caducidad del procedimiento,

-mismos que son de aplicación restrictiva-, los cuales son: que el procedimiento se haya paralizado por más de 6 meses en virtud de causas imputables exclusivamente al interesado que lo haya promovido o a la Administración que lo haya iniciado, de oficio o por denuncia. No obstante, en el párrafo final del inciso 1) del artículo 340, se establece la excepción a esa regla, que refiere a lo dispuesto en el párrafo final del artículo 339 LGAP, el que indica que, si existiere un interés general de por medio, o fuere conveniente sustanciarlo para su definición y esclarecimiento, no operaría la caducidad del procedimiento, aunque hubiesen transcurrido los 6 meses de inactividad contados a partir del inicio del mismo. En términos, la Ley No. 8968 de Protección de la Persona frente a tratamiento de sus Datos personales, tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes. Del análisis de estas circunstancias, se desprende que el bien jurídico tutelado por dicha ley, reviste particular importancia, al tratarse derechos fundamentales como lo es el derecho a la intimidad y o el de autodeterminación informativa, entre otros. No obstante, lo anterior se debe aclarar que de la Ley N° 8968, misma que reconoce la potestad de la Agencia de resolver los reclamos por infracción a las normas sobre protección de los datos personales, la posibilidad de ordenar la supresión, rectificación, adición o restricción de la información contenida en los archivos y las bases de datos y, la potestad de imponer las sanciones a las personas físicas o jurídicas, públicas o privadas, que infrinjan las normas sobre protección de los datos. Ambas potestades están reguladas en dos procedimientos diferentes, el primero es un proceso sumario, pues el legislador consideró que la violación al derecho de autodeterminación informativa de los ciudadanos merece una tutela más inmediata, y posteriormente, en caso de haber incurrido una infracción, procede la vía ordinara, en la cual el denunciado tiene mayores garantías procesales. Dado lo anterior y en atención a lo dispuesto en los artículos 340 inciso 1) y 339 párrafo final de la Ley 6227, aún en caso de haber transcurrido más de 6 meses de inactividad desde la apertura del procedimiento, a criterio de esta agencia, no operaría la caducidad del procedimiento, en aplicación de la excepción a la regla de la caducidad. De conformidad con lo anterior se procede el rechazo de la excepción de caducidad del procedimiento interpuesta por el denunciado.

**IV. SOBRE EL FONDO DE LA PRESENTE DENUNCIA**: Señala la denunciante que *"yo laboro para la empresa Soluciones de Pago MB (Lystocard), cuando una persona ingresa al Link y da click en la palabra Lystocard lo dirige a la página de la empresa www.lystocard.com, en esa página se encuentra el correo de servicio al cliente, el cual es información pública, pero no obstante no es mi correo electrónico personal en la empresa, ni tampoco es el correo que yo autoricé para que me envíen notificaciones. Al correo de Servicio al Cliente de la empresa para la cual trabajo llegó la notificación dirigida a mi nombre, con información sensible, ya que mencionan mi nombre completo y mi número de cédula, adicionalmente informan que se dará inicio a un proceso judicial, lo cual es causal de despido en la empresa y no era la notificación emitida por el juzgado".* Por su parte el denunciado señala en su informe lo siguiente: *"Que los hechos expuestos en la denuncia, los rechaza dado que la empresa Coincre, no se dedica a la recolección, almacenamiento o difusión de los datos de terceros relacionados con su cliente Tigo. "(...) que Coincre S.A, fue el canal de cobro que tramitó la cuenta de* **[NOMBRE1]**, *cuenta que fue asignada por nuestro cliente Tigo". (...) Que considerando que doña* **[NOMBRE1]** *ya no contestaba las llamadas de cobro que se le estaban realizando se procedió a envíale a su correo*

*electrónico y al señalado en su perfil público de la red social Facebook un aviso de cobro, en este perfil, en el que se señala que labora en LystoCard y en este se indica el correo electrónico: servicioalcliente@lystocard.com. (…) Considero que es importante enfatizar que el correo al que le envió la nota de cobro forma parte del link presente en el perfil que ella ha hecho público en Facebook, la información que obtuvimos de ella fue accesando a una red a la cual el interesado puede graduar el nivel de publicidad que quiere que tenga su información. En este caso, doña* **[NOMBRE1]** *publica la información sin filtro, haciendo totalmente pública a cualquier persona su información señalando su lugar de trabajo y el correo de contacto en este lugar. Es de esa forma que logramos evidenciar el aviso de cobro En el aviso de cobro no se incluye información restringida o sensible de doña* **[NOMBRE1]**, *no se señalan montos, únicamente se señala que se mantiene en mora en su deuda y se le brindan los teléfonos de contacto. Que presenta la excepción de caducidad del procedimiento (…)".* 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 la Ley No. 8968 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. Así las cosas, el artículo 4 de dicha ley establece el Derecho Fundamental de Autodeterminación Informativa, el cual abarca el conjunto de principios y garantías relativas al legitimo 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, 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 (de conformidad con el artículo 3 antes citado, la recolección, el trasmitir o la extracción de datos de una plataforma); 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 *"Que los hechos expuestos en la denuncia, los rechaza dado que la empresa Coincre, no se dedica a la recolección, almacenamiento o difusión de los datos de terceros relacionados con su cliente Tigo (…)". "(…) que Coincre S.A, fue el canal de cobro que tramitó la cuenta de* **[NOMBRE1]**, *cuenta que fue asignada por nuestro cliente Tigo".* De los argumentos antes expuestos, se puede demostrar 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, cuando se solicitó la prestación del servicio, lo cual incumple con lo establecido en el artículo 6 de Ley N° 8968 inciso 4. Dar 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 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 el denunciado "*que la empresa Coincre, no se dedica a la recolección, almacenamiento o difusión de los datos de terceros"* no es de recibo, dado que del análisis de los argumentos tanto del denunciado como del denúnciate, se pude determinar que se dio una transmisión de datos, recolección y almacenamiento de datos sin el consentimiento informado, para poder realizar la gestión de cobro. En cuanto a lo alegado por el denunciante con respecto a que*:* "*Que considerando que doña* **[NOMBRE1]** *ya no contestaba las llamadas de cobro que se le estaban realizando se procedió a envíale a su correo electrónico y al señalado en su perfil público de la red social Facebook un aviso de cobro, en este perfil, en el que se señala que labora en LystoCard y en este se indica el correo electrónico: servicioalcliente@lystocard.com. (…) Considero que es importante enfatizar que el correo al que le envió la nota de cobro forma parte del link presente en el perfil que ella ha hecho público en Facebook, la información que obtuvimos de ella fue accesando a una red a la cual el interesado puede graduar el nivel de publicidad que quiere que tenga su información. En este caso, doña* **[NOMBRE1]** *publica la información sin filtro, haciendo totalmente pública a cualquier persona su información señalando su lugar de trabajo y el correo de contacto en este lugar. Es de esa forma que logramos evidenciar el aviso de cobro no se incluye información restringida o sensible de doña* **[NOMBRE1]**, *no se señalan montos, únicamente se señala que se mantiene en mora en su deuda y se le brindan los teléfonos de contacto.* Según lo antes expuesto, y acorde con lo argumentado por la denúnciate, resulta aplicable 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. En ese sentido, se tiene que un perfil de Facebook, es una cuenta personal, se utiliza para un fin no comercial y representa a individuos; es donde se agregan amigos y familiares y se comparte fotos personales, videos y actualizaciones de la vida y biografía de su titular. La información que se sube a dicha red social, se sube para compartir información con los miembros de esa red, para mantener contacto con personas, para enviar mensajes entre otros; lo cual no autoriza a que terceros puedan sustraer datos personales; aún más tratándose de datos como el correo electrónico del trabajo, que se configura en una herramienta de trabajo otorgada por su patrono, y, como es este caso, una cuenta que no es administrada por la señora **[NOMBRE1]**, como lo manifiesta la denunciante; dado que es la cuenta del servicio al cliente y no la autorizada por ella. 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. 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. Dado lo anterior, se debe de indicar que se desconoce el tratamiento que se le dio la empresa Coincre S.A., a los datos personales sensibles de la señora **[NOMBRE1]**, dado que los mismos fueron recopilados de la red social Facebook, independientemente del grado de privacidad del mismo, los cuales tenían un fin determinado, explícito y legítimo, utilizándose posteriormente los mismos para un destino diferentes a los consentidos por la denunciante, por lo que no se podría afirmar que dicha empresa, cumpliera el principio de calidad de la información, es decir que la información utilizada sea actual veraz, exacta y adecuada al fin, para los que fueron recolectados. 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 Coincre S.A., no les dio un adecuado uso a los datos personales de la denunciante, al no contar con el consentimiento informado y haber usado dicha información para un fin distinto al consentido por la señora **[NOMBRE1]**. Además, resulta imperante 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.

**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 rechaza la excepción de caducidad contra el procedimiento.
**2-** Se declara con lugar la denuncia interpuesta por **[NOMBRE1]** contra **Cobro e Investigación Crediticia COINCRE S.A.**
**3-** Se ordena **Cobro e Investigación Crediticia** a suprimir los datos personales señalados por señora **[NOMBRE1]**.

**4-** 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**