



EXPEDIENTE: 078-04-2021-DEN

RESOLUCION N° 729-2023

AGENCIA DE PROTECCIÓN DE DATOS DE LOS HABITANTES, San José a las 08:50 horas del 05 de setiembre de 2023. Conoce la Agencia de Protección de Datos de los Habitantes denuncia formulada por [NOMBRE 1] contra **BANCO PROMERICA**.

RESULTANDO

1- Que mediante escrito presentado en fecha 29 de abril de 2021, suscrito por el señor [NOMBRE 1] se presentó formal denuncia contra **BANCO PROMERICA**, donde ha indicado el mismo que: *“El pasado 22 de abril un ejecutivo de Cobro de dicha institución Bancaria envió un correo masivo a 91 personas incluyéndome, con el asunto (Cobro Judicial del Banco Promerica le notifica). En dicho correo se envía copia abierta a los 91 afectados a su correo personal mostrando mi dirección de correo a terceros sin mi autorización, dicho correo indica el siguiente texto. La Ley faculta al banco a proceder con lo correspondiente para la recuperación del saldo que nos adeuda, ya que a pesar de que le hemos ofrecido diferentes opciones para normalizarla no hemos obtenido respuesta positiva a ninguna de ellas que le ayude a saldar su cuenta. La única conciliación con la que cuenta para evitar la Gestión Judicial que mantiene usted, es que realice el pago mínimo adeudado a hoy (comunicarlo al asesor del área legal para ingresarlo antes que realice el pago). De lo contrario procederemos con el proceso judicial correspondiente. Quedo a la espera de su respuesta. (...)”* y cuya pretensión es: *“Deseo que se sancione al banco según corresponda y establece la ley, también que el Banco Promerica me indemnice según lo que corresponda e indique la Ley, por haber hecho pública mi situación crediticia en un correo abierto, infringiendo así la normativa de secreto bancario y seguridad de la información.”*. (Visible a folios 01 al 06 del Expediente Administrativo).

2- Que mediante resolución N°269-2021 de las 08:00 horas del 05 de julio de 2021, se declara admisible la denuncia y se ordena el traslado de cargos al denunciado, a efecto de que brinde informe sobre la veracidad de los cargos y aporte las pruebas que estime pertinentes. Dicha resolución fue notificada Banco Promerica en fecha 13 de julio de 2021. (Visible a folios 07 y 09 del Expediente Administrativo).

3- Que, mediante documento recibido en esta Agencia, en fecha 16 de julio de 2021, el señor [NOMBRE 2] en su condición de Apoderado Generalísimo de Banco Promerica de Costa Rica S.A. contesta el traslado de cargos, cumpliendo así en tiempo y forma con lo prevenido mediante la resolución N°269-2021 supra indicada. (Visible a folios 10 al 18 del Expediente Administrativo).

4- 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 queja presentada y los autos de expediente, de relevancia para la resolución del presente asunto se consideran los siguientes hechos:

1- Que Banco Promerica remitió un correo electrónico donde se observan varios correos electrónicos personales ajenos al denunciante. (Visible a folios 04 y 05 del Expediente Administrativo).



II. HECHOS NO PROBADOS: Por carecer de sustento probatorio, se tienen cómo hechos no probados:

1. Que el correo electrónico personal del señor [NOMBRE 1] haya sido utilizado de manera inadecuada por el Banco Promerica.

III. SOBRE EL FONDO DE LA PRESENTE DENUNCIA: Expone el señor [NOMBRE 1] en su escrito: *“El pasado 22 de abril un ejecutivo de Cobro de dicha institución Bancaria envió un correo masivo a 91 personas incluyéndome, con el asunto (Cobro Judicial del Banco Promerica le notifica). En dicho correo se envía copia abierta a los 91 afectados a su correo personal mostrando mi dirección de correo a terceros sin mi autorización, dicho correo indica el siguiente texto. La Ley faculta al banco a proceder con lo correspondiente para la recuperación del saldo que nos adeuda, ya que a pesar de que le hemos ofrecido diferentes opciones para normalizarla no hemos obtenido respuesta positiva a ninguna de ellas que le ayude a saldar su cuenta. La única conciliación con la que cuenta para evitar la Gestión Judicial que mantiene usted, es que realice el pago mínimo adeudado a hoy (comunicarlo al asesor del área legal para ingresarlo antes que realice el pago). De lo contrario procederemos con el proceso judicial correspondiente. Quedo a la espera de su respuesta. (...)”*

Por su parte ha señalado Banco Promerica en su informe que rechaza los hechos denunciados, ya que no ha compartido su información personal con ninguna tercera persona por ningún medio. Expone que por un error operativo uno de sus funcionarios desde su dirección electrónica de trabajo envió un correo electrónico dirigido a otra dirección electrónica de la misma empresa, donde se indicaba de forma general que la Ley faculta al Banco a realizar gestión de recuperación de adeudos. Indica que, por un error humano del funcionario, puso en copia a varias direcciones electrónicas sin identificación de nombres y apellidos, aclara que el correo no iba dirigido a ninguno de los copiados, sino que fue enviado a la dirección [CORREO 1] como destinatario principal. Resalta que, si bien existió un error humano y operativo en la digitación por parte del colaborador, en dicho correo únicamente se indica en forma general que: *“la Ley faculta al Banco a realizar gestión de recuperación de saldos adeudados, y que para evitar el inicio de un proceso de gestión judicial es necesario realizar el pago mínimo adeudado”*, y que en dicho correo no se revela información determinada y específica de ninguna persona, ya que de los correos electrónicos no se puede extraer ningún tipo de identificación como: nombres, apellidos, cédula de identidad, residencia o pasaporte, números telefónicos, números de cuentas bancarias, direcciones físicas, nombre de productos bancarios, estados de cuentas, nivel de mora, saldo adeudado, o en general, cualquier dato relativo que permita que una persona sea identificada o identificable. Recalca que procedió a verificar sus sistemas internos y se constató que entre el señor [NOMBRE 1] y el banco existe una relación crediticia, donde el denunciado aportó de manera voluntaria como medio de contacto electrónico la dirección [CORREO 2], por lo que tuvo acceso al correo electrónico mencionado.

Revisada que ha sido la prueba que consta dentro del expediente administrativo, la misma no es clara al atribuir algún tipo de responsabilidad al aquí denunciado, esto en razón de que no se logra desprender de la misma que se haya utilizado el correo electrónico del denunciante en un correo masivo. Por lo que debe de indicársele al denunciante que quién procure que se tengan como ciertos



los hechos fundamentados debe demostrarlos, no basta con la simple evocación de los mismos, si no que existe la obligación determinada por Ley de comprobarlos, sobre este menester el Reglamento a la Ley No.8968, señala expresamente, en su artículo 67, lo siguiente: *“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.**”* (resaltado no es del original). De igual manera la Ley General de Administración Pública, señala en su Capítulo Segundo, específicamente en los artículos 293 y 298 lo referente a la prueba en los que indica expresamente lo siguiente: *“**Artículo 293.- 1. Con la presentación a que se refiere el artículo 285, los interesados acompañarán toda la documentación pertinente o, si no la tuvieren, indicarán dónde se encuentra. 2. Deberán, además, ofrecer todas las otras pruebas que consideren procedentes.**”* *“**Artículo 298.- 1. Los medios de prueba podrán ser todos los que estén permitidos por el derecho público, aunque no sean admisibles por el derecho común. 2. Salvo disposición en contrario, las pruebas serán apreciadas de conformidad con las reglas de la sana crítica.**”* Por lo anteriormente expuesto, no puede esta Agencia endilgar algún tipo de responsabilidad al denunciado por un tratamiento inadecuado de los datos personales del denunciante.

Sin embargo, de oficio se le indica al banco denunciado que el poner en copia varios correos electrónicos de varias personas físicas, de manera visible para todos los involucrados, aunque se trate de un error humano, se convierte en una vulneración a los datos personales de estas personas afectadas, ya que debe de aclararse de que el correo electrónico personal se trata de un dato personal de carácter restringido, por lo que resulta adecuado indicar al denunciado que para evitar que se den este tipo de errores se deben contar con protocolos de actuación, regulados en el artículo 12 de la Ley No.8968 que indican *“**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.** (...)”*. Además, indica el Reglamento a la Ley de repetida cita en su artículo 32, las especificaciones mínimas que deben incluir estos protocolos de actuación: *“**Artículo 32. De los protocolos mínimos de actuación. Los responsables deberán confeccionar un protocolo mínimo de actuación, el cual deberá ser transmitido al encargado para su fiel cumplimiento y donde al menos, se deberá especificar lo siguiente: a) Elaborar políticas y manuales de privacidad obligatorios y exigibles al interior de la organización del responsable; b) Poner en práctica un manual de capacitación, actualización y concientización del personal sobre las obligaciones en materia de protección de datos personales; c) Establecer un procedimiento de control interno para el cumplimiento de las políticas de privacidad; Instaurar procedimientos ágiles, expeditos y gratuitos para recibir y responder dudas y quejas de los titulares de los datos personales o sus representantes, así como para acceder, rectificar, modificar, bloquear o suprimir la información contenida en la base de datos y revocar su consentimiento. e) Crear medidas y procedimientos técnicos que permitan mantener un historial de los datos personales durante su tratamiento. f) Constituir un mecanismo en el cual el responsable transmitente, le comunica al responsable receptor, las condiciones en las que el titular consintió la recolección, la transferencia y el tratamiento de sus datos. Estas medidas, así como sus posteriores modificaciones, deberán ser inscritas ante la Agencia como protocolos**”*



*mínimos de actuación.”, y medidas de seguridad suficientes para evitar incurrir en malos entendidos como ha sido en el presente caso. La Ley de marras indica con respecto a las medidas de seguridad que deben existir en las bases de datos en su artículo 10: “**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.”.*

Los protocolos mínimos de actuación, estará integrados por todas aquellas directrices, manuales, políticas y demás que se elaboren, con el objeto de regular el debido tratamiento de los datos personales, los cuales se encuentran regulados en los artículos del 10 seguridad de los datos que indica: “**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.”, 11 deber de confidencialidad el cual señala: “**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.”, y artículo 12 supra mencionado, todos de la Ley No.8968.

Al poseer los mecanismos suficientes para garantizar la seguridad de los datos personales de sus clientes, el banco no incurrirá en vulneraciones al derecho de autodeterminación informativa de los mismos, derecho contemplado en el artículo 4 de la Ley No. 8968 el cual indica: “**ARTÍCULO 4.- Autodeterminación informativa:** Toda persona tiene derecho a la autodeterminación informativa, la cual abarca el conjunto de principios y garantías relativas al legítimo tratamiento de sus datos personales reconocidos en esta sección. Se reconoce también la autodeterminación informativa como un derecho fundamental, con el objeto de controlar el flujo de informaciones que conciernen a cada persona, derivado del derecho a la privacidad, evitando que se propicien acciones discriminatorias.”.Por lo anteriormente expuesto, es procedente ordenar de oficio al Banco



Promerica, que en un plazo **DIEZ DÍAS HÁBILES**, presenten ante esta Agencia **UNA COPIA DE LOS PROTOCOLOS MÍNIMOS DE ACTUACIÓN** y **UNA DESCRIPCIÓN TÉCNICA DE LAS MEDIDAS DE SEGURIDAD**, que se tienen establecidos a lo interno para subsanar este tipo de errores.

Así las cosas, siendo que no se cuenta con prueba suficiente que logre demostrar que se ha realizado una vulneración a algún dato personal del denunciante lo procedente es declarar sin lugar el presente procedimiento de protección de derechos. Resolución debidamente firmada por la Licda. Karla Quesada Rodríguez, jefa del Departamento de Registro de Archivos de Bases de Datos, en razón de acuerdo N° **PRODHAB 1-2022**, del 26 de diciembre de 2022 de autorización de tramites de procesos sumarios. **NOTIFIQUESE.**

POR TANTO

Con fundamento en los numerales 1, 2, 4, 10, 11, 12, y 16 de la Ley N° 8968; 11, 12, 40, 58, 59 y 70 y concordantes del Reglamento a dicha Ley:

1. Se declara sin lugar la denuncia interpuesta por [NOMBRE 1] contra **BANCO PROMERICA.**
2. Se ordena de oficio al denunciado que en un plazo **DIEZ DÍAS HÁBILES**, presenten ante esta Agencia **UNA COPIA DE LOS PROTOCOLOS MÍNIMOS DE ACTUACIÓN** y **UNA DESCRIPCIÓN TÉCNICA DE LAS MEDIDAS DE SEGURIDAD**, que se tienen establecidos a lo interno para subsanar este tipo de errores.
3. Contra la presente resolución, de conformidad con los artículos 25 de la Ley No. 8968 y 71 de su reglamento, procede el recurso de reconsideración, mismo que deberá presentarse en un plazo de **tres días hábiles** a partir de la notificación de la misma. **NOTIFIQUESE.**

Licda. Karla Quesada Rodríguez
Departamento de Registro y Archivo de Bases de Datos
Agencia de Protección de Datos de los Habitantes

Elaborado: Licda. Alejandra López Mora