



EXPEDIENTE: 036-03-2019-DEN

RESOLUCIÓN N° 471-2023

AGENCIA DE PROTECCIÓN DE DATOS DE LOS HABITANTES, DIRECCIÓN NACIONAL. San José, a las 13:33 horas del 01 de junio de 2023. Conoce la Agencia de Protección de Datos de los Habitantes, Recurso de Reconsideración interpuesto por el señor **[NOMBRE 2]**, Representante legal de **SCOTIABANK DE COSTA RICA S.A.** (en adelante Scotiabank), sobre los términos de la resolución N° 280-2022 de las 12:00 horas del 28 de junio de 2022, dictada dentro del presente Procedimiento de Protección de Derechos, según denuncia interpuesta por el señor **[NOMBRE 1]**.

RESULTANDO

1. Que mediante Oficio No. PACO-DAC-OF-027-2019, del 25 de enero de 2019, enviado a esta Agencia mediante correo electrónico del 25 de enero de 2019, por el Departamento de Apoyo al Consumidor del Ministerio de Economía, Industria y Comercio, el señor **[NOMBRE 1]**, presentó formal denuncia contra **SCOTIABANK DE COSTA RICA S.A.**, en el que indica que desde el año 2017 viene recibiendo correos no solicitados sobre promociones que ofrece dicha entidad, sin haber sido cliente anteriormente ni haber autorizado el envío de misivas comerciales a su correo electrónico, que ha solicitado al banco en múltiples ocasiones externando su disconformidad, por medio de servicio al cliente, quienes le han indicado su compromiso de dar de baja a sus datos (marzo 2018), pero esto no ha sucedido y le continúan enviando correos de este tipo, razón por la cual solicita que no le envíen más información de este tipo y se eliminen sus datos personales de la base de datos de la denunciada. (Visible a folios 01 al 10 del Expediente Administrativo).
2. Que mediante resolución N° **280-2022** de las 12:00 horas del 28 de junio de 2022, esta Agencia emitió la Resolución Final del Procedimiento de Protección de Derechos incoado, declarando con lugar la misma. Dicha resolución fue notificada a las partes el 01 de febrero de 2023, a los medios electrónicos señalados para tal efecto. (Visible a folios 22 al 26 del Expediente Administrativo).
3. Que, a través de escrito recibido en esta Agencia, vía correo electrónico del día 06 de febrero de 2023, la entidad denunciada presentó, en tiempo y forma, recurso de reconsideración contra dicha resolución final. (Visible a folios 27 al 31 del Expediente Administrativo).

CONSIDERANDO

I. SOBRE LA ADMISIBILIDAD DEL RECURSO: La etapa recursiva del Procedimiento de Protección de Derechos, se encuentra regulada en el artículo 27 de la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, Ley N° 8968, así como en su respectivo Reglamento. El artículo 1 del citado Reglamento establece: "**ARTÍCULO 1°.** - *Refórmense los artículos 56, 57, 63, 71 y 72 del Decreto Ejecutivo N°37554-JP, del 30 de octubre de 2012, denominado: "Reglamento a Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales" publicado en el Alcance 42 al Diario Oficial La Gaceta N°45 del 5 de marzo de 2013, para que en adelante se lean de la siguiente manera: "(...) Artículo 71. Medios de impugnación. Contra el acto final del procedimiento procede dentro del tercer día hábil a partir*



de la respectiva notificación la interposición ante la Agencia del recurso ordinario de reconsideración. (...)” (Lo subrayado y destacado no corresponde al original). Según lo expuesto supra, contra la resolución final del Procedimiento de Protección de Derechos, cabe el Recurso de Reconsideración. En el presente caso, la denuncia fue resuelta a través de Resolución No. 280-2022 de las 12:00 horas del 28 de junio de 2022, la cual se declaró con lugar. Dicha resolución fue notificada a las partes en fecha 01 de febrero de 2023, a los medios electrónicos señalados para tal efecto, otorgando un plazo de 3 días hábiles para la presentación de recursos, cuyo plazo vencía el 07 de febrero de 2023. Posteriormente, mediante escrito recibido en esta Agencia, en fecha 06 de febrero de 2023, el señor [NOMBRE 2], Representante legal de Scotiabank, presentó en tiempo y forma, Recurso de Reconsideración contra la Resolución Final, por lo tanto, el mismo resulta admisible y será resuelto lo que en derecho corresponde.

II. SOBRE EL FONDO DEL RECURSO: De relevancia para la resolución de este recurso, la entidad denunciada señala en su escrito, lo siguiente: “(...) *Es correcto que el pasado mes de abril del 2019 se envió la nota OGG419-19 firmada por el Lic. [NOMBRE 2], en donde se indicaba que la información personal del señor [NOMBRE 1], no se encuentra en nuestra base de datos, y que se marcaría su nombre e información para que no sea contactado por ningún ejecutivo del banco en el futuro. Según el análisis e investigación realizada, se confirma que la ejecutiva de ventas que envió el correo ofreciéndola (sic) un producto, en mayo 2019, mantenía, sin nuestro consentimiento ni autorización coma la información del señor [NOMBRE 1], de manera personal, y sin autorización procedió a enviarle el correo electrónico, en contra del procedimiento establecido, violentando las políticas vigentes del banco para búsqueda de prospectos, las cuales se detallan más adelante. Cabe indicar que dicha ejecutiva no labora en el banco en estos momentos, y que nunca ha existido autorizado (sic) del banco, para tener bases de datos personales. Todas nuestras Fuerzas de Ventas toman la información de las bases de datos establecidas por el banco, las mismas son digitales y todo cliente debe brindar el consentimiento correspondiente para el manejo de sus datos, según lo establecido en la regulación. Lo indicado en la nota firmada por el [NOMBRE 2], era correcto, pues la información personal del señor Rodríguez Sánchez no se encontraba en nuestras bases de datos digitales y lo ocurrido fue producto de una negligencia por parte de una persona que fue empleada del banco. (...) (...) Lo ocurrido en mayo del 2019, fue a un lamentable comportamiento, no autorizado coma de una ex funcionaria que se había saltado los protocolos establecidos. (...)*”. Más adelante, en síntesis, señala que Scotiabank cuenta con los protocolos mínimos de actuación, políticas internas, estándares de protección de información, manuales de privacidad, códigos de conducta, procedimientos de control interno y una intranet, para el adecuado uso, manejo y tratamiento de la información y privacidad de los datos personales, según lo exigido por la Ley No. 8968. Además, manifiesta que esa empresa pone en práctica un manual de capacitación, actualización y concientización del personal sobre las obligaciones en materia de Protección de Datos personales lo cual se certifica anualmente mediante la ventana de cumplimiento que establece el área de Recursos Humanos. Asimismo, declara que se estableció el rol y responsabilidad de un Delegado de Privacidad por Unidad de Negocio y Sucursales con el propósito de contar con una adecuada gestión del riesgo de privacidad que contiene las principales responsabilidades con las que deben contar los funcionarios designados como oficiales de privacidad en su respectiva unidad de



negocio, detallando a su vez, las funciones y actividades de cada uno de estos responsables. Señala que el Área de Cumplimiento-Protección de Datos y Privacidad, anualmente desarrolla un programa de capacitación en materia de privacidad, confidencialidad y seguridad de la información abordando los principales controles establecidos en las políticas y procedimientos señalados en párrafos anteriores, dirigidos a dichos Delegados de Privacidad, quienes a su vez están en la obligación de bajar esa información a cada colaborador de su área de trabajo. Finalmente, alega que se envían comunicados a todo el personal recordando la importancia del cumplimiento de las políticas y procedimientos en materia de privacidad y confidencialidad de la información como un proceso de concientización de todo el personal. Por tal motivo, consideran que ese Banco, cumplió con lo requerido por el denunciante, realizando la supresión de sus datos personales desde el año 2019, y que conforme lo explicado detalladamente en este escrito recursivo, esa entidad cuenta con políticas y procedimientos internos referentes a la protección de datos personales. Por otro lado, solicitan reconsiderar dejar sin efecto lo dispuesto en el punto 3 del “Por Tanto” de la resolución recurrida, en el cual se ordena testimoniar piezas del presente procedimiento de protección de derechos ante el Ministerio Público, por las inconsistencias detectadas, en cuanto al informe rendido bajo fe de juramento por el señor [NOMBRE 2], en su condición de Apoderado y Sub Gerente y Director Regional Legal de Scotiabank de Costa Rica S.A.

Al respecto, es importante reiterar a esa empresa que, tal y como se le ha indicado en diferentes resoluciones, lo dispuesto en la Ley No. 8968 y su Reglamento, deber ser de conocimiento y acatamiento obligatorio, para toda persona física o jurídica, empresa o entidad pública o privada, quienes tienen el deber de protección al derecho constitucional a la autodeterminación informativa, regulado en el artículo 12 del Reglamento a la Ley N° 8968, el cual indica: “(...) **Artículo 12. Autodeterminación informativa.** Es el derecho fundamental de toda persona física, a conocer lo que conste sobre ella, sus bienes o derechos en cualquier base de datos, de toda naturaleza, pública o privada, el fin para el cual está siendo utilizada o recabada su información personal, así como exigir que sea rectificadas, actualizada, complementada o suprimida, cuando la misma sea incorrecta o inexacta, o esté siendo empleada para un fin distinto del autorizado o del que legítimamente puede cumplir. (...)” (Lo destacado y subrayado no corresponde al original), lo cual fue requerido por el denunciante en su momento y no se cumplió por parte de Scotiabank; al ser así, de manera proactiva y como co-responsables, tienen el deber legal y la obligación de verificar el actuar de cada uno de los involucrados en el uso, manejo, y/o tratamiento de los datos personales, entendiéndose tratamiento como: “(...) 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.”, según la definición contenida en el inciso i) del artículo 3 de la Ley No. 8968, cuya regulación debe ser conocida y aplicada por esa empresa y sus colaboradores, en observancia y cumplimiento del principio constitucional de que “Nadie puede alegar ignorancia del ordenamiento jurídico”, por tal motivo, cada una de las partes intervinientes, en este caso, tanto los empleados de esa entidad, como en sí todo el banco, deben observar y aplicar las medidas de seguridad y protocolos mínimos de actuación necesarios para salvaguardar y proteger los datos personales de sus clientes, situación que en este caso evidentemente no sucedió y es confirmado



por la misma entidad denunciada en su escrito recursivo, por lo tanto, no es de recibo la justificación dada por el señor [NOMBRE 2], Representante Legal de Scotiabank, en la que manifiesta que la situación irregular presentada, se debe a una negligencia en la actuación de una ex funcionaria de ese Banco que se saltó los protocolos, pues precisamente esta actuación, denota una falta de controles y una evidente vulneración a las políticas y procedimientos internos del banco, siendo esa entidad la responsable de velar y capacitar a su personal respecto a la protección de los datos personales de sus clientes, y de que cada uno de éstos cumpla con dicha labor. Por otra parte, sorprende a esta instancia que se realicen tales manifestaciones, pues precisamente el mismo señor [NOMBRE 2], en su informe rendido en fecha 22 de abril de 2019, indicó que la situación presentada se debía a la integración entre Scotiabank Transformandose y Scotiabank de Costa Rica S.A., y que, el único correo que recibió el señor [NOMBRE 1], por parte de su representada, fue en diciembre de 2018 (folio 17 vuelto), sin embargo, tal como se constata en el presente expediente administrativo, así como lo confirma el mismo señor [NOMBRE 2], en su escrito recursivo de fecha 06 de febrero de 2023, posteriormente el 07 de mayo de 2019, se vuelve a enviar correo electrónico al denunciante, por parte de una ex colaboradora de Scotiabank, que inobservó las políticas internas del banco, lo cual hace ver una clara contradicción entre los argumentos vertidos en ambos escritos.

Ahora bien, respecto a los protocolos mínimos de actuación y medidas de seguridad, se insiste en que, en cumplimiento de los principios y derechos fundamentales y constitucionalmente protegidos, como lo son el derecho a la intimidad y a la autodeterminación informativa, la citada Ley No. 8968 y su Reglamento, son sumamente claros en establecer y determinar la obligación de contar con las medidas de seguridad y protocolos mínimos de actuación para el uso, manejo y tratamiento de los datos personales, siendo el responsable y/o encargado de las bases de datos, a quienes les corresponde conocer y aplicarlos, de acuerdo a los principios establecidos en la referida ley, específicamente en sus artículos 10, 11 y 12, en concordancia con los numerales 37 al 41 de su respectivo Reglamento, los cuales señalan: Artículos de la Ley: “**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 (...)” (Lo subrayado no corresponde al original). Numerales más relevantes del citado Reglamento: “**Artículo 27. Procedimientos para el tratamiento.** El responsable establecerá y documentará procedimientos para la inclusión, conservación, modificación, bloqueo y supresión de los datos personales, en el sitio o en la nube, con base en los protocolos mínimos de actuación y las medidas de seguridad en el tratamiento de los datos personales. Además, deberá el responsable de la base de datos velar por la aplicación del principio de calidad de la información. (...) **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; d) 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. (...) **Artículo 34. De las medidas de seguridad en el tratamiento de datos personales.** El responsable, deberá establecer y mantener las medidas de seguridad administrativas, físicas y lógicas para la protección de los datos personales, con arreglo a lo dispuesto en la Ley y el presente Reglamento. Se entenderá por medidas de seguridad el control o grupo de controles para proteger los datos personales. Asimismo, el responsable deberá velar porque el encargado de la base de datos y el intermediario tecnológico cumplan con dichas medidas de seguridad, para el resguardo de la información. (...) **Artículo 41. Cumplimiento de los protocolos mínimos de actuación.** Las transferencias de datos personales por parte de los responsables, estarán supeditadas al fiel cumplimiento de los protocolos mínimos de actuación, debidamente inscritos ante la Agencia.”. (Lo subrayado y destacado no corresponde al original). Todos los aspectos antes citados, son de indispensable conocimiento y cumplimiento por parte de todas aquellas entidades que realizan tratamiento de datos personales; de manera que, en un escenario ideal no deberían presentarse usos no autorizados de datos personales, menos aún si no se tiene claridad de que se cuenta con el debido consentimiento informado y previo del titular, ya que, es al responsable de las bases de datos, a quien le corresponde adecuar sus bases al cumplimiento de la normativa vigente. El respeto a estos derechos, se fundamenta 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 veraces, lícitos, exactos y legítimos. De tal manera que, el mecanismo ideal para garantizar el ejercicio del derecho a la autodeterminación informativa, y que, debe emplear y utilizar cualquier persona física y/o jurídica**



que realice el tratamiento de datos personales, sería precisamente el consentimiento informado por parte del titular de los datos personales. En razón de que esa entidad menciona en su informe que cuenta con: protocolos mínimos de actuación, medidas de seguridad, políticas internas, estándares de protección de información, manuales de privacidad, códigos de conducta, procedimientos de control interno, una intranet, manual de capacitación, actualización y concientización del personal certificado anualmente por área de RRHH, un rol y responsabilidad de un Delegado de Privacidad por Unidad de Negocio y Sucursales con las funciones y actividades de cada uno de estos responsables, así como además, señala que el Área de Cumplimiento-Protección de Datos y Privacidad, anualmente desarrolla un programa de capacitación en materia de privacidad, confidencialidad y seguridad de la información abordando los principales controles establecidos en las políticas y procedimientos señalados en párrafos anteriores, dirigidos a dichos Delegados de Privacidad, quienes a su vez están en la obligación de bajar esa información a cada colaborador de su área de trabajo y que, se envían comunicados a todo el personal recordando la importancia del cumplimiento de las políticas y procedimientos en materia de privacidad, todo esto para el adecuado uso, manejo y tratamiento de la información y privacidad de los datos personales, según lo exigido por la Ley No. 8968, se ordena a la denunciada a presentar de **forma física**, en un plazo de **20 DÍAS HABILES**, contados a partir de la notificación de la presente resolución, toda la documentación detallada que compruebe y respalde dichos controles. Caso contrario, podrá ser objeto de la aplicación de las sanciones establecidas en el artículo 28 de la Ley No. 8968, previo cumplimiento del debido proceso.

Con relación a lo ordenado en la resolución N° 280-2022, respecto a testimoniar piezas ante el Ministerio Público, se le informa que esta orden quedará supeditada a la presentación de toda la documentación solicitada en la presente resolución por parte del Scotiabank, misma que será analizada por esta Agencia.

Finalmente, se tiene por satisfecha la pretensión del señor Rodríguez Sánchez, toda vez que la denunciada indica en su informe que no se cuenta con información del denunciante dentro de su base de datos, y que marcaría su nombre e información para que no sea contactado por ningún ejecutivo del banco a futuro.

POR TANTO

Con fundamento en los numerales 1, 2, 4, 16, 25 y 27 de la Ley N° 8968; artículos 56 y 71 del Reglamento No. 37554-JP a dicha Ley, se resuelve:

1.- Se declara sin lugar el recurso de reconsideración incoado contra la resolución N° 280-2022 de las 12:00 horas del 28 de junio de 2022.

2. Se ordena a **SCOTIABANK DE COSTA RICA S.A.**, presentar en un plazo de **20 DÍAS HABILES**, contados a partir de la notificación de la presente resolución, toda la documentación detallada que compruebe y respalde la existencia y aplicación de protocolos mínimos de actuación, medidas de seguridad, políticas internas, estándares de protección de información, manuales de privacidad, códigos de conducta, procedimientos de control interno, una intranet, manual de capacitación, actualización y concientización del personal certificado anualmente por área de RRHH, un rol y responsabilidad de un Delegado de Privacidad por Unidad de Negocio y Sucursales con las funciones y actividades de cada uno de estos responsables, así como además, señala que el



Área de Cumplimiento-Protección de Datos y Privacidad, anualmente desarrolla un programa de capacitación en materia de privacidad, confidencialidad y seguridad de la información abordando los principales controles establecidos en las políticas y procedimientos señalados en párrafos anteriores, dirigidos a dichos Delegados de Privacidad, quienes a su vez están en la obligación de bajar esa información a cada colaborador de su área de trabajo y que, se envían comunicados a todo el personal recordando la importancia del cumplimiento de las políticas y procedimientos en materia de privacidad, todo esto para el adecuado uso, manejo y tratamiento de la información y privacidad de los datos personales, según lo exigido por la Ley No. 8968. Caso contrario, podrá ser objeto de la aplicación de las sanciones establecidas en el artículo 28 de la Ley No. 8968, previo cumplimiento del debido proceso.

3.- Con relación a lo ordenado en la resolución N° 280-2022, respecto a testimoniar piezas ante el Ministerio Público, se le informa que esta orden quedará supeditada a la presentación de toda la documentación solicitada en la presente resolución por parte del Scotiabank, misma que será analizada por esta Agencia.

4.- Se tiene por satisfecha la pretensión del señor [NOMBRE 1], toda vez que la denunciada indica en su informe que no se cuenta con información del denunciante dentro de su base de datos, y que marcaría su nombre e información para que no sea contactado por ningún ejecutivo del banco a futuro. **NOTIFÍQUESE.**

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

Elaborada por: Licda. Judith Coronado García