VISTO:

El trámite nº **27762/20,** iniciado de oficio por esta Defensoría del Pueblo, a raíz del notorio incremento de consultas y reclamos recibido por casos de presunta comisión de ciberdelitos, especialmente relacionados con la captura ilegal de datos personales y fraudes bancarios, mediante el acceso ilegal a las cuentas de usuarios/as del sistema bancario.

Y CONSIDERANDO QUE:

I. Desde hace muchos años la vida cotidiana se encuentra interpelada y atravesada por la utilización, cada vez más frecuente, de medios informáticos para poder concretar múltiples tareas tan necesarias como habituales. En efecto, el acceso a internet y a distintos canales informáticos resultan casi ineludibles, pues a través de ellos podemos, por ejemplo, percibir el cobro de haberes u honorarios, realizar transferencias, pago de servicios, solicitud de créditos, etc., así como todo tipo de control sobre nuestras cuentas bancarizadas; también para formular consultas, trámites o reclamos de toda índole, tanto ante las administraciones u organismos públicos (a nivel nacional, provincial y/o municipal) como frente a entidades privadas (bancos, comercios, compañías de seguro, etc); además, efectuar compras, adquisiciones o contrataciones de bienes, productos y servicios (algunos de ellos de carácter esencial); y el acceso a noticias o transmisión de información de todo tipo (periodísticas, de estudio, documentales, personales, etc.).

Esta omnipresencia de la conectividad en nuestras vidas, se ha visto particularmente acentuada y acelerada con motivo de las medidas de aislamiento/distanciamiento social, preventivo y obligatorio, adoptadas para enfrentar la emergencia sanitaria por la aparición de la pandemia por el virus del Covid-19. Como consecuencia de ello, muchas actividades que antes podían realizarse de manera presencial, se tornaron casi exclusivamente de forma virtual.

La Organización de Naciones Unidas (ONU) elaboró un informe para nuestro país, en el cual señala que: *"... La epidemia causada por el virus COVID-19 tendrá en la Argentina un impacto multidimensional. Afectará al total de la ciudadanía, a los distintos sectores de la economía y actores de la vida del país, al ambiente y los recursos naturales (...) La crisis de COVID-19 ha exacerbado la vulnerabilidad y la discriminación hacia los y las menos protegidos/as de la sociedad, destacando profundas desigualdades económicas y sociales que requieren atención urgente..."*[1]. Siendo, en especial los/as consumidores/as o usuarios /as, quienes resultan ser sujetos pasibles de aprovechamientos y/o estafas.

II. En este contexto, desde el comienzo del aislamiento/distanciamiento social, preventivo y obligatorio, esta Defensoría del Pueblo, ha recibido una creciente cantidad de consultas y reclamos referidos a la comisión de los denominados "ciberdelitos", particularmente fraudes o estafas bancarias y robo de datos. La casi "obligada" inclinación al uso del entorno digital produjo, paralelamente, un incremento de los delitos o contravenciones informáticos, de aquellos/as que tienen como objetivo la identidad, la propiedad, el patrimonio y la seguridad de las personas, pero además de aquellos/as otros que tienen como objetivo atacar, destruir y dañar activos, sistemas de información y otros sistemas de computadoras, utilizando medios electrónicos y/o redes de Internet.

Las estafas cibernéticas, se cometen mediante el uso de un tipo de ingeniería social que se caracteriza por intentar adquirir información confidencial de forma fraudulenta. El/la estafador /a se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial sea electrónica, por correo electrónico, o algún sistema de mensajería instantánea, red social, llamadas telefónicas o combinando dos o más de estas vías[2].

De los reclamos recibidos se observa que la mayoría alude a distintas formas de robo de datos personales, a partir de lo cual los/as ciberdelincuentes acceden de manera ilícita a las cuentas bancarias o a los sistemas de "Home Banking" de las personas, y en pocos minutos pueden efectuar transferencias, realizar compras, incluso, gestionar créditos personales automáticos o pre-otorgados por las entidades bancarias. Es decir, la criminalidad informática tiene un alcance mayor y puede incluir delitos tradicionales como el fraude, el robo, la falsificación, entre otros; en los cuales los ordenadores y redes son utilizados como

medio. Con el desarrollo de la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados.

Dentro de esta generalidad, la mayor cantidad de consultas y/o reclamos recibidos, giran en torno a las comúnmente denominadas “estafas bancarias”. Éstas se generan mediante el “PHISHING”, que es un método que se utiliza para engañar a el/la usuario/a desprevenido/a, y así conseguir que revele información personal, como contraseñas, claves, datos de tarjetas de crédito o de la seguridad social con sus códigos de seguridad y números de cuentas bancarias, entre otros. Así como también, el acceso indebido se produce por la vulneración de la seguridad de los sistemas informáticos o del hackeo del sistema directamente.

Cabe mencionar sobre este punto, que la Ley Nacional nº 25.326[3] -y modificatorias- de Protección de los Datos Personales, en su art. 9º establece que: *“... 1. El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. 2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad”.*

III. Frente a esta creciente problemática, las distintas asociaciones que nuclean a los bancos públicos y privados que operan en el país, lanzaron una campaña conjunta de información dirigida a los/as usuarios/as de servicios financieros para prevenir las estafas virtuales, a través de una serie de recomendaciones de seguridad que publicaron y difundieron en medios digitales y redes sociales.

En un comunicado conjunto, de fecha 7 de octubre de 2020, las entidades agrupadas en la Asociación de Bancos de la Argentina (ABA), la Asociación de Bancos Públicos y Privados de la República Argentina (ABAPPRA), la Asociación de la Banca Especializada (ABE), la Asociación de Bancos Argentinos (ADEBA), señalaron que: *“... Con el objetivo de advertir a*

la sociedad ante nuevas modalidades delictivas, los bancos públicos, privados, de capital nacional e internacional con operaciones en el país realizarán a partir de la fecha y por las próximas tres semanas una campaña de ciberseguridad para difundir mensajes simples a toda la población: No compartir claves ni datos personales y entrar en contacto únicamente a través de los canales oficiales de atención de los bancos. Todos los bancos del sistema financiero difundirán las publicaciones en diferentes medios digitales, con un concepto creativo simple y una estética unificada. Para redes sociales los hashtags serán #CuidateDeLasEstafas y #ProtegeTuInformacion. Para el conjunto de entidades resulta imprescindible que todas las personas recuerden que no deben compartir información personal y financiera en redes sociales. En ese sentido, reiteramos las recomendaciones anteriormente difundidas: - Nunca un empleado de un banco va a solicitar: – Nombre de usuario. – Contraseña de homebanking o cajero automático. – Número de token de seguridad. – Transferencias de efectivo a cambio de un beneficio. Su banco nunca solicitará por mails, SMS, whatsapp, teléfono o por redes sociales: – Claves bancarias. – Número de tarjeta de crédito. – Token de seguridad. – Tarjeta de coordenadas. – Número de cuenta bancaria CBU o Alias. No comparta nunca su nombre de usuario, clave o número de token. No importa el motivo que le argumenten. No acceda a las páginas de los bancos por buscadores de internet. Si el mensaje que recibe por redes sociales, teléfono o correo electrónico le genera dudas, no responda por ese medio. Los bancos y las cámaras que los representan, consideran fundamental que todos los usuarios sigan estas recomendaciones para mejorar la seguridad y así evitar estafas, a la vez que agradecen la difusión de estos mensajes"[4].

Atento a tal iniciativa, esta Defensoría del Pueblo organizó un encuentro virtual con los principales representantes de las mencionadas asociaciones bancarias, a fin de transmitirles la preocupación por el crecimiento de los casos y reclamos de estas modalidades delictivas e interiorizarse de los alcances de la campaña, de los problemas detectados y demás medidas adoptadas por los bancos[5].

Con posterioridad, se mantuvo una videoconferencia con el doctor Horacio Azzolin, titular de la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) del Ministerio Publico Fiscal de la Nación, con el objetivo de coordinar y articular un trabajo conjunto con esta Defensoría del Pueblo, que permita intensificar las medidas de prevención e información a los/as usuarios

/as en general y, de corresponder, canalizar aquellos casos que requieran la promoción de acciones investigativas en el ámbito judicial por la existencia de hechos delictuales[6].

La UFECI fue creada por Resolución PGN nº 3743/15, a fin de *"... robustecer la capacidad de respuesta del organismo en materia de detección, persecución y represión de la criminalidad organizada y de los delitos que más menoscaban la seguridad ciudadana. Así la UFECI podrá entender en casos de ilícitos constituidos por ataques a sistemas informáticos, o cuando el medio comisivo principal o accesorio de una conducta delictiva incluya la utilización de sistemas informáticos, con especial atención en el ámbito de la criminalidad organizada, y crímenes en los que sea necesario realizar investigaciones en entornos digitales –aun cuando no hayan sido cometidos contra o mediante un sistema informático..."* [7].

En nuestro país, mediante la Ley Nacional nº 26.388[8] -y modificatorias- se modificó el Código Penal, a fin de incorporar diversos delitos informáticos, tales como la distribución y tenencia con fines de distribución de pornografía infantil, violación de correo electrónico, acceso ilegítimo a sistemas informáticos, daño informático y distribución de virus, daño informático agravado e interrupción de comunicaciones.

Por su parte, esta Defensoría del Pueblo también se sumó a la campaña de prevención, mediante una solicitada publicada con fecha 9 de noviembre de 2020, en los principales diarios nacionales, bajo el lema: "EVITÁ EL ROBO DE LAS CUENTAS BANCARIAS Y TUS DATOS PERSONALES. SEGUÍ LAS RECOMENDACIONES DE LA DEFENSORÍA"[9], y con el siguiente texto: *"Si operás con homebanking y necesitás realizar una consulta o reclamo a tu banco hacelo en lo posible por correo-e escribiendo a la casilla que indica la entidad en su página web. Es más seguro.* ***Si lo hacés por alguna red social:*** *-Asegurate de que sea una cuenta oficial/VERIFICADA del banco (debe tener un tilde azul a continuación del nombre de usuario). -No envíes por mensaje privado ningún dato personal ni de tu cuenta bancaria, correo electrónico o número de teléfono alguno. Los bancos NUNCA piden esa información.* ***Si luego de la consulta/reclamo te llaman por teléfono afirmando ser del banco:*** *-Exigí que te contacten al correo-e que está registrado en el banco y NO CONTINÚES LA*

CONVERSACIÓN. -Consultá inmediatamente tu cuenta desde el homebanking. Controlá que no aparezcan transferencias hacia otras cuentas que no hayas realizado y que no tengas algún crédito depositado que no hayas solicitado. -Si encontrás alguna o ambas irregularidades hacé una captura de pantalla y comunicate con el banco por correo-e para desconocerlas. Exigí número de reclamo. ***Si se bloquea la clave, el usuario o el token de seguridad de tu homebanking:*** *– Es preferible que consultes a través del correo-e que brinda tu banco en su página web. Evitá hacerlo por teléfono. – Si lo hacés a través de las redes sociales, asegurate de que sea la cuenta oficial/verificada del banco (debe tener un tilde azul a continuación del nombre de usuario). No brindes ningún tipo de información por mensaje privado. Pedí que te envíen las instrucciones al correo-e que la entidad tiene registrado. – Consultá el estado de tu cuenta y de los últimos movimientos desde un cajero automático y guardá el ticket impreso. Hacé la consulta al menos durante dos días seguidos. – Controlá que no aparezcan transferencias hacia otras cuentas que no hayas realizado y/o que no tengas algún crédito depositado que no hayas solicitado. Buscá más consejos en www.defensoria.org.ar.* ***La Defensoría del Pueblo trabaja junto a la Asociación de Bancos Argentinos (ADEBA), la Asociación de Bancos Públicos y Privados (ABAPPRA), la Asociación de Bancos de la Argentina (ABA), la Asociación de la Banca Especializada (ABE) y la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) para ayudarte****".*

IV. Conforme lo hasta aquí señalado, resulta claro que la principal medida para intentar disminuir este tipo de modalidades delictivas debe ser la información amplia y masiva, brindada de manera veraz, adecuada, oportuna y suficiente a través de medidas elementales de prevención, para que cada usuario/a las conozca a fin de no caer en la trampa de los/as ciberdelincuentes. Se presume así, que cuanto mayor sea el conocimiento de los/as usuarios /as para operar en forma segura, menor será la posibilidad de resultar víctimas de tales delitos. Desde ese punto de vista, la decisión de las entidades bancarias de desarrollar una campaña de divulgación de métodos de prevención, parece acertada y plausible.

No obstante, deviene igualmente necesario avanzar en otras medidas adicionales -más allá de las preventivas- que contribuyan a reducir y, en lo posible evitar, la proliferación de estas

maniobras delictivas. Pues, en definitiva, se deben extremar los esfuerzos para revestir de mayores niveles de protección a quienes son los/as principales perjudicados/as: los/as usuarios/as de servicios financieros.

Frente a la realidad que impuso la pandemia, muchas personas que antes del aislamiento /distanciamiento social, preventivo y obligatorio, no disponían, no usaban, o no tenían acceso a medios electrónicos, ni conocimiento adecuado de estas herramientas, se vieron compelidos a usarlas dado que de otra manera no podían realizar operaciones cotidianas y necesarias. Ello colocó en una situación de mayor indefensión y vulnerabilidad a estos/as usuarios/as "nuevos/as" o inexpertos/as (adultos/as mayores, personas no bancarizadas, etc.) que resultaron presas fáciles para estas maniobras delictivas.

V. En términos de protección de derechos, no se debe soslayar que la Constitución Nacional ha reconocido expresamente que todos/as los/as consumidores/as y usuarios/as (entre ellos, claro está, los/as usuarios/as de servicios financieros) tienen derecho, en la relación de consumo, a la protección de su salud, seguridad e intereses económicos; a una información adecuada y veraz; a la libertad de elección; y a condiciones de trato equitativo y digno, a cuyo respecto las autoridades públicas deben proveer a la protección de esos derechos (art. 42).

Desde esa perspectiva, resulta innegable que la relación que se entabla entre los/as usuarios/as de servicios financieros y las entidades bancarias, constituye una típica relación de consumo y, por consiguiente, está abarcada por el régimen de tutela especial de toda la normativa de defensa del consumidor.

Así se ha dicho que *"... la relación de consumo –con anclaje y reconocimiento constitucional en el art. 42 CN- es un concepto más amplio y abarcativo que la típica relación contractual. En los términos de la LDC, la relación de consumo es el vínculo jurídico –y no sólo contractual- que se entabla entre el consumidor y los proveedores de bienes y servicios. Lo que caracteriza al derecho del consumidor es el principio de protección al débil jurídico en el marco de una relación que se presenta como estructuralmente desigual y asimétrica a la que*

la ley pretende equilibrar. De un lado, se ubica el consumidor que es el sujeto que requiere de especial tutela, y del otro, los proveedores de bienes y servicios, que son los sujetos particularmente obligados, por su carácter de profesionales o expertos. La relación de consumo es entonces, el elemento que decide el ámbito de aplicación del derecho del consumidor, por consiguiente debe comprender todas las situaciones posibles en las que el consumidor –como débil jurídico- debe ser protegido, ya sea antes durante y después de contratar, o cuando es dañado por un ilícito extracontractual, o cuando es sometido a una práctica de mercado, o cuando actúa individualmente o cuando lo hace colectivamente. La doctrina y la jurisprudencia han subrayado que 'el propio art. 42, CN. adopta esta expresión de relación de consumo para evitar circunscribirse a lo contractual y referirse con una visión más amplia a todas las circunstancias que rodean o se refieren o constituyen un antecedente o son una consecuencia de la actividad encaminada a satisfacer la demanda de bienes y servicios para destino final de consumidores y usuarios…"[10].

La doctrina especializada no duda en afirmar que, en general, buena parte de la actividad de las entidades bancarias queda sujeta a la normativa especial de defensa del consumidor. Al respecto, Chamatrópulos sostiene que: *"... hoy en día prácticamente ya no existen voces que pongan en tela de juicio la sumisión de las entidades bancarias al Estatuto del Consumidor..."*. Por otra parte, nunca debe olvidarse que la función que cumplen estas entidades en la comunidad es de una importancia tal que su conducta **"debe ajustarse a un standard de responsabilidad agravada, distinta de la que le cabría a una simple persona"**. Esto se debe a que estamos ante *"... comerciantes profesionales colectores de fondos públicos y altamente especializados que ostentan una superioridad de tipo técnico sobre los usuarios. Su actuación puede resumirse en la expresión: 'a mayor responsabilidad, mayor diligencia'..."* pues *"... los bancos no sólo son proveedores en los términos de la LDC sino que **su conducta deberá ser apreciada con parámetros aún más exigentes que aquellos que se utilicen para evaluar el accionar de otros proveedores** también regidos por el Estatuto del Consumidor, pero que no se encuentran llamados a cumplir un rol en la sociedad tan preponderante como el de las entidades financieras..."*[11].

En la misma línea, De Núñez señala que: *"... A estas alturas ya es inobjetable la irrupción de la LDC dentro de la actividad bancaria, aunque no se desconoce que su aplicación no debe ser automática sino luego de encontrarse verificadas las condiciones de su procedencia*

(arts. 1º y 2º LDC). Sin embargo, no cabe duda de que una vasta cantidad de sus relaciones jurídicas quedan comprendidas bajo este régimen protectorio. Muestra de ello es que el mismísimo Código Civil y Comercial dedica un parágrafo a los contratos bancarios con consumidores y usuarios (arts. 1384 a 1389 Cód. Civ. y Com.). Así pues, ***cualquier incumplimiento por parte del proveedor bancario dará lugar a responsabilidad objetiva*** *(...) Piénsese en extracciones de fondos por ventanilla realizadas por terceros no autorizados a tal efecto sobre cuentas bancarias consumeriles. La entrega de dinero a personas distintas a las habilitadas implica una prestación defectuosa del servicio por la cual el banco debe responder objetivamente, sin resultar atendible ningún argumento de defensa que no configure caso fortuito o fuerza mayor...".*

En materia de responsabilidad objetiva en determinadas relaciones bancarias y en cuanto al empleo de medios informáticos en la actividad bancaria, el antedicho autor señala que: *"... La recurrente comisión de fraudes vinculados con la prestación de servicios financieros que se valen de la informática (considérese, por ejemplo, las plataformas electrónicas de pagos, los cajeros automáticos, y los portales de home banking), así como las reiteradas fallas que aquejan a dichos mismos servicios, refleja con elocuencia el nivel considerable de exposición que acompaña a buena parte del negocio bancario actual. Es en base a tales circunstancias que se argumenta que* ***el oficio bancario, en tanto y en cuanto se encuentre atravesado por sistemas informáticos, se perfila como una actividad riesgosa.*** *Aun antes del dictado del Código Civil y Comercial (…) ya se afirmaba que* ***el sistema (software y hardware) que permite operar una red de cajeros automáticos podía ser calificado de cosa riesgosa y que en rigor esta calificación podía ser asignada, en este punto, al sistema informático que opera las transacciones remotas, sea mediante el denominado homebanking sea por el uso de cajeros automáticos*** *(…) Habida cuenta de que el sustrato de la prestación bancaria no siempre conlleva un peligro intrínseco, opinamos que la potencialidad dañosa deriva de la mismísima informatización, conformando, por ende, una actividad riesgosa a razón de los medios empleados (...) La presente temática goza de plena vigencia dado el sostenido avance de la tecnología sobre la industria (siendo inminente el lanzamiento del primer banco 100% digital de la Argentina) y el creciente número de ardides sustentados en las 'posibilidades' que ofrece la masificación de la operatoria electrónica bancaria, llegándose incluso a decir que 'la actividad financiera en sí misma constituye un foco de atención para la delincuencia'; a resultas de lo cual, concluye que si bien frente a este fenómeno 'los bancos establecen y perfeccionan medidas*

tendientes a fortalecer la seguridad de sus servicios' no es ocioso destacar que 'su sola puesta en marcha no trae aparejada eximición alguna dado que, en principio, las entidades financieras continuarán siendo responsables si tales hechos lesivos no logran ser neutralizados. Sucede que, al tratarse de actividades riesgosas, únicamente podrán desentenderse comprobando causa ajena..."[12].

La jurisprudencia también se ha pronunciado al respecto. En un fallo reciente, la Cámara de Apelaciones en lo Civil y Comercial - Sala I - de La Plata, confirmó la sentencia de primera instancia, que hizo lugar a una medida cautelar requerida por la parte actora (un jubilado usuario financiero) y consecuentemente intimó al Banco demandado para que en el plazo de cinco días, suspenda los descuentos y/o retenciones que aplica al accionante en su cuenta, originados en los préstamos que se habrían obtenido por las sumas de pesos quinientos mil ($500.000.-) y pesos cuarenta y un mil seiscientos ($41.600.-), dado que el accionante *"... Denuncia haber sido víctima de 'phishing' y endilga responsabilidad objetiva al banco demandado en los términos de la ley 24.240 por el vicio que presentaría el sistema informático que opera para la prestación remota de servicios a través de una red de cajeros automáticos y en el uso del Home banking del cual el banco es el dueño o guardián así como del sistema (Software y Hardware) que es el que permite operar de modo remoto. La documentación adjuntada avala razonablemente la versión apuntada por el accionante..."*.

Para así decidir, los magistrados sostuvieron que: *"... la cuestión evidencia inicialmente rasgos de una contratación que involucra una relación de consumo y que permite ponderar 'prima facie' una evidente asimetría entre las posibilidades del cliente consumidor y las de la entidad bancaria prestadora del servicio en punto a la conducta que es dable esperar de cada uno de ellos en el desarrollo del v*[í]*nculo contractual al que ambas partes han hecho expresa referencia. Debe tenerse en cuenta que el nuevo Código Civil y Comercial regula de forma específica, dentro de las disposiciones generales de los contratos bancarios, a los celebrados por consumidores y usuarios (arts. 1384 a 1389) resultando entonces aplicables dichas especiales disposiciones a todos los contratos en los que intervengan..."*[13].

VI. Además, tanto la doctrina como la jurisprudencia, ya venían alertando acerca de la necesidad de acentuar los mecanismos de protección a aquellos/as usuarios/as y

consumidores/as que, por distintas circunstancias, se encuentran en situaciones de mayor vulnerabilidad o de vulnerabilidad agravada. En este sentido, la Secretaría de Comercio Interior de la Nación, mediante la Resolución nº 139/2020[14] -y modificatorias- estableció que: *"... a los fines de lo previsto en el Artículo 1° de la Ley N° 24.240 se consideran consumidores hipervulnerables, a aquellos consumidores que sean personas humanas y que se encuentren en otras situaciones de vulnerabilidad en razón de su edad, género, estado físico o mental, o por circunstancias sociales, económicas, étnicas y/o culturales, que provoquen especiales dificultades para ejercer con plenitud sus derechos como consumidores..."* (art. 1º).

Asimismo, dicha Resolución enumera en su art. 2º, de manera no taxativa, una serie de factores que pueden constituir causas de hipervulnerabilidad, entre las cuales se señala, por ejemplo: *"... c) ser personas mayores de 70 años; d) ser personas con discapacidad conforme certificado que así lo acredite; (...) f) la pertenencia a comunidades de pueblos originarios; g) ruralidad; h) residencia en barrios populares conforme Ley N° 27.453; i) situaciones de vulnerabilidad socio-económica acreditada por alguno de los siguientes requisitos: 1) Ser Jubilado/a o Pensionado/a o Trabajador/a en Relación de Dependencia que perciba una remuneración bruta menor o igual a DOS (2) Salarios Mínimos Vitales y Móviles; 2) Ser Monotributista inscripto en una categoría cuyo ingreso anual mensualizado no supere en DOS (2) veces el Salario Mínimo Vital y Móvil; (...) 6) Estar incorporado/a en el Régimen Especial de Seguridad Social para empleados del Servicio Doméstico (Ley 26.844)..."*.

Y, en su art. 3º le encomienda *"... la SUBSECRETARÍA DE ACCIONES PARA LA DEFENSA DE LAS Y LOS CONSUMIDORES de la SECRETARÍA DE COMERCIO INTERIOR del MINISTERIO DE DESARROLLO PRODUCTIVO, a fin que arbitre las medidas que crea necesarias para la implementación de la presente resolución.*

VII. Por otra parte, la preocupación por dotar de mayor protección a los/as consumidores/as en el comercio electrónico, así como a los/as usuarios/as de servicios financieros, tanto en lo que se refiere a medidas de seguridad como a la protección de sus datos personales, también se puso en manifiesto a escala internacional.

En efecto, es dable recordar que como resultado del proceso de revisión y actualización de las *"Directrices para la Protección del Consumidor"* de Naciones Unidas, aprobadas por la Asamblea General en su Resolución nº 70/186, de fecha 22 de diciembre de 2015, se incorporaron distintas recomendaciones al respecto. Las Directrices son un documento internacional de suma importancia que sirve como guía y marco de referencia a los Estados Miembros para implementar políticas activas de defensa a los/as consumidores/as.

Así, por ejemplo, en cuanto a los *"Principios para las buenas prácticas comerciales"* -Capítulo IV- se incorporó la siguiente directriz: *"... e)Protección de la privacidad. Las empresas deben proteger la privacidad de los consumidores mediante una combinación de mecanismos adecuados de control, seguridad, transparencia y consentimiento en lo relativo a la recopilación y utilización de sus datos personales..."*.

Además, se agregó un segmento dedicado al *"Comercio electrónico"* en el Capítulo V *"Directrices"*, en donde se dispuso: *"63.Los Estados Miembros deben esforzarse por fomentar la confianza de los consumidores en el comercio electrónico, mediante la formulación constante de políticas de protección del consumidor transparentes y eficaces, que garanticen un grado de protección que no sea inferior al otorgado en otras formas de comercio. 64.Los Estados Miembros deben, cuando proceda, examinar las políticas de protección del consumidor en vigor para dar cabida a las características especiales del comercio electrónico y garantizar que los consumidores y las empresas estén informados y sean conscientes de sus derechos y obligaciones en el mercado digital. 65.Los Estados Miembros podrían tal vez examinar las directrices y normas internacionales pertinentes sobre el comercio electrónico y sus correspondientes revisiones y, en su caso, adaptar esas directrices y normas a sus circunstancias económicas, sociales y ambientales, para que puedan acatarlas, y colaborar con otros Estados Miembros en su aplicación a través de las fronteras. Al hacerlo, los Estados Miembros podrían tal vez estudiar las Directrices para la Protección de los Consumidores en el Contexto del Comercio Electrónico de la Organización de Cooperación y Desarrollo Económicos".*

En materia de *"Servicios financieros"*, también en el Capítulo V *"Directrices"*, se incluyeron las siguientes disposiciones: *"66.Los Estados Miembros deben, según proceda, establecer o fomentar: a)Políticas para la regulación y la aplicación efectiva de las normas en el ámbito de la protección del consumidor de servicios financieros. b)Órganos de supervisión con la autoridad y los recursos necesarios para llevar a cabo su misión. c)Controles y mecanismos de seguros adecuados para proteger los activos de los consumidores, incluidos los depósitos. d)Mejores estrategias de educación financiera que promuevan la adquisición de conocimientos financieros básicos. e)Un trato justo y una divulgación adecuada de la información, velando por que las instituciones financieras también se hagan responsables y rindan cuentas de los actos de sus agentes autorizados. Los proveedores de servicios financieros deben disponer de políticas por escrito sobre conflictos de intereses, para ayudar a detectarlos cuando aparecen. Cuando se plantee la posibilidad de un conflicto de intereses entre el proveedor y un tercero, se debe comunicar esta información al consumidor, a fin de evitar posibles perjuicios a los consumidores a raíz de esa situación. f)La actuación responsable de los proveedores de servicios financieros y sus agentes autorizados, en particular en lo que respecta a la concesión responsable de préstamos y la venta de productos que se ajusten a las necesidades y los medios del consumidor. g)Controles apropiados para proteger los datos financieros del consumidor contra el fraude y el abuso, entre otros. h)Un marco normativo que promueva la eficiencia en función de los costos (o costes, como se emplea mayoritariamente en España) y la transparencia de las remesas, a fin de que los consumidores dispongan de información clara sobre el precio y el envío de los fondos que se han de transferir, los tipos de cambio, los cargos y otros costos (o costes, como se emplea mayoritariamente en España) ligados a las transferencias de dinero, así como la reparación correspondiente si esas operaciones no se completan. 67.Los Estados Miembros deben adoptar medidas para reforzar e integrar las políticas de los consumidores relativas a la inclusión financiera, la educación financiera y la protección de los consumidores en cuanto al acceso y la utilización de servicios financieros".*

De igual forma, es importante tener en miras la Directiva de la Unión Europea[15], relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Esta Directiva impone a las entidades gestoras de servicios esenciales, así como a los/as prestadores/as de ciertos servicios digitales considerados clave en el funcionamiento de Internet, la obligación de establecer sistemas de gestión de la seguridad de la información en sus organizaciones y de notificar a las

autoridades los incidentes que tengan especial gravedad. Además, obliga a los Estados miembros a supervisar el cumplimiento de estas obligaciones, y a velar por que existan equipos de respuesta a incidentes de seguridad con capacidad para proteger a las empresas de la propagación de estos incidentes. Asimismo, impulsa la cooperación entre autoridades nacionales y el intercambio de información como medio para elevar el nivel de seguridad en la Unión Europea frente a las amenazas de carácter transfronterizo. Se advierte entonces, una clara orientación jurídica orientada a priorizar el enfoque en la seguridad en las redes y en los sistemas de información.

VIII. Finalmente, es de señalar que mediante la Comunicación "A" 6878, el Banco Central de la República Argentina, ha establecido y reiterado en su normativa, la imposición a *"... Las entidades deberán tener implementados mecanismos de seguridad informática que garanticen la genuinidad de las operaciones..."*[16]; como también que en el marco de la emergencia sanitaria la Comunicación "A" 6942, prorrogada por la Comunicación "A" 6949, derivó la operatoria del sistema financiero a los canales electrónicos y de cajeros automáticos.

IX. En resumen, conforme todo lo señalado, lo que se quiere poner de manifiesto es que las entidades bancarias, en su carácter de proveedores especializados en ofrecer y brindar servicios financieros, tienen una responsabilidad aún mayor de acuerdo a la importancia social de la actividad profesional que desarrollan. Ello implica, entre otras cosas, que deben extremar los recaudos para que los servicios que ofrecen y organizan se presten en condiciones de máxima seguridad, en aras de proteger los derechos de los/as usuarios/as financieros/as, como sujetos especialmente tutelados por las normas constitucionales y legales de defensa del consumidor y todas las referidas a la protección de sus datos personales.

Por lo expuesto, teniendo en cuenta que la misión de esta Defensoría del Pueblo es la defensa, protección y promoción de los derechos humanos y demás derechos y garantías e intereses individuales, colectivos y difusos tutelados en la Constitución Nacional, la Constitución de esta Ciudad y las leyes, frente a los actos, hechos u omisiones de la administración, de prestadores de servicios públicos (art. 137 Constitución local, y art. 2º de

la Ley nº 3[17] -según texto consolidado Ley nº 6.017[18]-) y de conformidad a las facultades y atribuciones que la ley le confiere, se considera oportuno emitir una serie de recomendaciones al Banco Central de la República Argentina, para que disponga las comunicaciones o instrucciones pertinentes a las entidades del sistema financiero bajo su control, dirigidas a reforzar los mecanismos de seguridad informática y de protección adicional a los/as usuarios/as del sistema.

Como es de público conocimiento se viven días de total excepcionalidad a raíz de la declaración de la pandemia por el nuevo coronavirus (Covid-19).

Ninguna duda cabe del esfuerzo realizado por el Estado -en todos sus niveles- para proteger a sus ciudadanos/as. Al respecto, no resulta ocioso resaltar el importante rol que está cumpliendo este Órgano Constitucional dentro de dicho contexto.

Cabe decir también que, los problemas individuales y/o colectivos de los/as vecinos/as de esta Ciudad continúan de la misma forma que su derecho a requerir de las autoridades una solución a sus necesidades, más aún cuando la Administración local continúa trabajando adaptada a las nuevas condiciones que exigen las circunstancias actuales y que las obligaciones impuestas por la Ley nº 3 (según texto consolidado por Ley nº 6.017) a esta Defensoría del Pueblo continúan en plena vigencia.

Por lo expuesto y sin desconocer el contexto de emergencia descripto, se solicita que el cumplimiento de lo requerido en la presente Resolución, se realice en el marco del desempeño estricto de todas las medidas y/o precauciones tendientes a garantizar la salud de los/as trabajadores/as del organismo requerido.

POR TODO ELLO:

EL DEFENSOR DEL PUEBLO

DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES

R E S U E L V E :

1) Recomendar al Presidente del Banco Central de la República Argentina (BCRA), licenciado Miguel Ángel Pesce, tenga a bien evaluar y, en su caso, emitir las comunicaciones y/o instrucciones que estime pertinentes para todas las entidades bancarias y financieras que se encuentran bajo su esfera de control, dirigidas a:

a) reforzar las medidas de seguridad informática interna de todas las distintas entidades bancarias, y en sus comunicaciones e intercambio de información interbancaria;

b) disponer canales y vías de atención prioritaria a los/as usuarios/as que denuncien haber sido víctimas de ciberdelitos o contravenciones, para tomar debido registro, brindarles asesoramiento adecuado y adoptar medidas eficaces que permitan proteger el patrimonio de los/as afectados/as, con especial énfasis en aquellos/as usuarios/as que queden comprendidos/as dentro de la categoría de “consumidores/as hipervulnerables”, de conformidad a lo dispuesto en la Resolución de la Secretaría de Comercio de la Nación;

c) implementar medidas adicionales de validación en aquellas modalidades de créditos automáticos, pre otorgados, o similares que se ofrecen y se ejecutan por medios informáticos;

d) propiciar, en todo el país, la formalización de convenios de cooperación recíproca entre las entidades bancarias y las unidades fiscales especializadas en delitos informáticos, a fin de articular medidas que permitan prevenir, neutralizar e investigar la comisión de delitos informáticos y perseguir penalmente a sus autores;

e) impulsar la creación de Códigos de Conducta o de Buenas Prácticas Profesionales, tal como lo promueve el art. 30 de la Ley Nacional nº 25.326 -y modificatorias-, a los fines de unificar el tratamiento de datos personales y brindar una correcta capacitación de los/as empleados/as bancarios/as.

2) Sugerir al Presidente del Banco Central de la República Argentina (BCRA), licenciado Miguel Ángel Pesce, que las comunicaciones y/o instrucciones que eventualmente se

impartan a las entidades del sistema financiero -tales como las enumeradas en el apartado 1 de la presente- vinculadas a la seguridad informática, sean coordinadas con la Secretaría de Innovación Pública de la Jefatura de Gabinete de Ministros del Gobierno Nacional, en relación a la Ciberseguridad y a la Prevención en Seguridad de Sistemas y Redes Informáticas.

3) Poner en conocimiento de la presente Resolución, al Gerente Principal de Protección al Usuario de Servicios Financieros del Banco Central de la República Argentina, contador Oscar A. Diakovsky, a través de correo electrónico analisistecnicolegal@bcra.gob.ar, a los efectos que estime corresponder.

4) Poner en conocimiento de la presente Resolución, al titular de la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) del Ministerio Público Fiscal de la Nación, señor Horacio Azzolin, a los efectos que estime corresponder.

5) Fijar en treinta (30) días el plazo previsto en el art. 36 de la Ley nº 3 (según texto consolidado Ley nº 6.017) de la Ciudad Autónoma de Buenos Aires[19].

6) Registrar, notificar, reservar en la Coordinación Operativa para su seguimiento y oportunamente archivar.

Código 441

ND/GG/MLB

COCA/CEDCCyU

co/COCF/CEAL

ea/SOADA

Mlm/MAER/COMESA

NOTAS

1. ^ *https://www.onu.org.ar/stuff/Informe-COVID-19-Argentina.pdf Páginas 3 y 4.*
2. ^ *ALTMARK, Daniel R. - MOLINA QUIROGA, Eduardo. Tratado de derecho informático.- 1a ed. – Buenos Aires: La Ley, 2012. vol. 1, 1040 pág.*
3. ^ *Ley Nacional nº 25.326, sancionada el día 4 de octubre de 2000, promulgada parcialmente con fecha 30 de octubre de 2000 y publicada en el Boletín Oficial nº 29.517 del 2 de noviembre de 2000.*
4. ^ *http://abe.org.ar/noticia-detalle.php?articulo=83*
5. ^ *http://www.defensoria.org.ar/noticias/phishing-encuentro-con-asociaciones-bancarias/*
6. ^ *http://www.defensoria.org.ar/noticias/reunion-con-la-ufeci/*
7. ^ *UFECI | Ministerio Público Fiscal | Procuración General de la Nación (mpf.gob.ar)*
8. ^ *Ley Nacional nº 26.388, sancionada el día 4 de junio de 2008, promulgada de hecho con fecha 24 de junio de 2008, y publicada en el Boletín Oficial nº 31.433 del 25 de junio de 2008.*
9. ^ *http://www.defensoria.org.ar/noticias/recomendaciones-de-la-defensoria-para-evitar-el-robo-de-las-cuentas-bancarias-y-los-datos-personales/*
10. ^ *DARCY, Norberto C "Responsabilidad bancaria en las relaciones de consumo. Legitimación del consumidor que pide daño directo y justicia gratuita" La Ley 29/07/2020, 8 - RCyS 2020-IX, 79 - Cita on line AR/DOC/1239/2020.*
11. ^ *CHAMATROPULOS, Demetrio A., "El deber de seguridad de los bancos y los daños derivados de la utilización de cajeros automáticos", en RCyS2010-IX, 95, Cita Online: AR /DOC/5129/2010*
12. ^ *DE NÚÑEZ, Rodrigo, "La responsabilidad objetiva en la actividad bancaria" SJA 27/06 /2018, 27/06/2018, 5 - Cita Online: AR/DOC/3012/2018*
13. ^ *PEDERNERA JUAN ALBERTO C/ BANCO DE LA PROVINCIA DE BUENOS AIRES S/ NULIDAD DE ACTO JURÍDICO (INCIDENTE ART 250 DEL CPCC) (DIGITAL) REG. INTER. N° 333/20, LIBRO INTERLOCUTORIOS LXXVI. JDO. JUZGADO CIVIL Y COMERCIAL NRO. 10 Causa: 128367.*
14. ^ *Resolución nº 139/2020, publicada en el Boletín Oficial nº 34.391 de fecha 28 de mayo de 2020.*
15. ^ *2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 6 de julio de 2016*
16. ^ *http://www.bcra.gov.ar/Pdfs/comytexord/A6878.pdf*
17. ^ *Ley nº 3 de la Ciudad Autónoma de Buenos Aires, sancionada el día 3 de febrero de 1998 y publicada en el Boletín Oficial nº 394 de fecha 27 de febrero de 1998.*
18. ^ *Ley nº 6.017, sancionada el día 4 de octubre de 2018, promulgada con fecha 23 de octubre de 2018, y publicada en el Boletín Oficial nº 5.485 del 25 de octubre de 2018.*
19. ^ *Ley nº 3, art. 36: "Con motivo de sus investigaciones, el Defensor o Defensora del Pueblo puede formular advertencias, recomendaciones, recordatorios de los deberes de los*

funcionarios, y propuestas para la adopción de nuevas medidas. Las recomendaciones no son vinculantes, pero si dentro del plazo fijado la autoridad administrativa afectada no produce una medida adecuada, o no informa de las razones que estime para no adoptarla, el Defensor o Defensora del Pueblo puede poner en conocimiento del ministro o secretario del área, o de la máxima autoridad de la entidad involucrada, los antecedentes del asunto y las recomendaciones propuestas. Si tampoco así obtiene una justificación adecuada, debe incluir tal asunto en su informe anual o especial a la Legislatura, con mención de los nombres de las autoridades o funcionarios que hayan adoptado tal actitud".