© ***Cadernos de Dereito Actual*** Nº 14. Núm. Ordinario (2020), pp. 354-373
·ISSN 2340-860X - ·ISSNe 2386-5229

Responsabilidad Civil y Protección de Datos Personales: Tutela Individual y Derecho Procesal Colectivo

Civil Liability and Protection of Personal Data: Individual Guardianship and Collective Procedural Law

Mariana Battochio Stuart[1]
Victor Augusto Estevam Valente[2]
Pontifícia Universidade Católica de São Paulo

Resumen: Este artículo tiene por objetivo analizar los fundamentos de la responsabilidad civil como consecuencia del tratamiento inadecuado de datos personales, tanto desde la perspectiva de la tutela individual como del Derecho Procesal Colectivo. Nos preguntamos acerca de la interpretación dialógica entre la Ley nº 13.709/18 (Ley General de Protección de Datos Personales) con la Ley nº 8.078/90 (Código de Defensa del Consumidor), la Ley nº 12.414/11 (Ley de Registro Positivo), la Ley 7.347/85 (Ley de la Acción Civil Pública) y la Constitución de 1988.

Palabras-clave: Protección de Datos Personales; Responsabilidad Civil; Tutela Individual; Derecho Procesal Colectivo.

Abstract: This article aims to analyze the fundamentals of civil liability as a result of the inadequate treatment of personal data, both from the perspective of individual protection and of collective procedural law. We will verify about the dialogical interpretation between the federal Constitucion of 1988, Law number 13.709/18, Law number 8.078/90, Law number 7.347/1985 and Law number 12.414/11.

[1] Doctoranda y Máster en Derechos Difusos y Colectivos en la Pontifícia Universidade Católica de São Paulo (PUC/SP). Supervisora Jurídica en el Escritório Modelo Dom Paulo Evaristo Arns de la Facultad de Derecho de la PUC/SP.
[2] Doctorando y Máster en Derecho Penal en la Pontifícia Universidade Católica de São Paulo (PUC/SP). Coordinador del curso de Especialización de Criminología, Derecho Penal y Procesal Penal y de los Cursos de Extensión en *Compliance Digital* de la Pontifícia Universidade Católica de Campinas (PUC-CAMPINAS). Profesor de Derecho Penal y Procesal Penal de la Facultad de Derecho de la Pontifícia Universidade Católica de Campinas (PUC-CAMPINAS). Abogado y consultor jurídico.

Recibido: 17/10/2020
Aceptado: 28/11/2020

Keywords: Protection of Personal Data; Civil Reponsability; Individual Protection of Personal Data; Collective Procedural Law.

Introducción:

El instituto de la responsabilidad expresa las tendencias, transformaciones y evolución de la ciencia jurídica, estableciendo reglas y principios y con el objetivo de garantizar los intereses, individuales y transindividuales, para concretar la efectividad del postulado de la dignidad humana.

Debido a las relaciones sociales construidas en el seno de una sociedad digital y compleja, bajo la perspectiva del respeto a los llamados derechos humanos fundamentales[3], se muestra imperativo la mejora de un régimen de responsabilidad por la violación de datos personales apto a la inmediata prevención y, en el caso de que no sea viable tal prevención, posterior reparación, de manera amplia, de las diversas modalidades de daños provenientes de conductas antijurídicas que pueden alcanzar los más variados campos de intereses patrimoniales y extrapatrimoniales de los individuos titulares de datos personales o de una dada colectividad de datos constante de bancos de datos masificados.

La sociedad de masa, inevitablemente, generó bancos de datos de usuarios y consumidores que afectan derechos de la personalidad individuales o transindividuales, no limitados, por lo tanto, a la esfera de uno o algunos individuos.

La construcción de marcos legales complejos e innovadores evidencia la relevancia del derecho a la privacidad, en especial la protección de los datos personales. En palabras de Rafael Mafei Rabelo Queiroz, con la autonomización legislativa del derecho a la protección de datos, es más fácil reconocer el derecho a la protección de datos como un bien jurídico *per se*: tratándose de dato personal, poco importará si la información en cuestión es de hecho sensible al derecho a la privacidad de su titular. Ese desarrollo agregó al derecho de protección de datos personales un conjunto de subderechos, con remedios específicos, que el derecho a la privacidad no conocía, a ejemplo de los derechos de conocimiento, complementación, actualización y corrección de datos personales en pose de un controlador.

Se puede concluir que, violado o incumplido el deber jurídico de protección de datos personales, surge, para quien lo incumplió o violó, la responsabilidad o el deber jurídico impuesto, por la obligación de tutelar la privacidad y autodeterminación de los datos personales, según se expondrá a continuación.

1. Ley General de Protección de Datos en Brasil

1.1. Perspectiva Histórica

En la década del 70, la formación de diversos bloques económicos regionales intensificó el elevado compartimiento de datos personales a nivel internacional. Tanto las empresa como el gobierno alcanzaron mayor eficiencia y productividad, surgiendo al mismo tiempo la necesidad de resguardar la privacidad, especialmente frente al flujo abierto y transfronterizo de datos[4].

[3] Como vamos a inferir más adelante, la protección de los datos personales es integrante del rol de los Derechos Humanos, pues se trata de derecho del hombre positivado en tratados internacionales. Además, es integrante del rol de los derechos fundamentales, pues el artículo 5º, inciso X, de la Constitución Federal brasileña disciplinó que *son inviolables la intimidad, la vida privada, la honra y la imagen de las personas, asegurado el derecho a la indemnización por el daño material o moral proveniente de su violación*, siendo una inferencia lógica la fundamentalidad de la protección de datos personales.

[4] OPICE BLUM, R. NÓBREGA MALDONADO, V. *LGPD – Lei Geral de Proteção de Dados Comentada*, 2ª edição, Revista dos Tribunais, São Paulo, 2019, p. 20.

La protección de datos personales fue elevada a la categoría jurídica, haciéndose prevista en las más diversas legislaciones, teniendo como baluarte la autodeterminación informativa, que consiste en el derecho fundamental de la persona, de carácter subjetivo, de controlar y procesar el tratamiento de sus datos, posibilitando el libre desarrollo de su personalidad, como también su libre iniciativa en la comunidad democrática[5].

En esta toada, el Reglamento General de Protección de Datos de la Unión Europea (Reglamento EU 2016/679 o *General Data Protection Regulation*) tiene por fin prevaleciente crear mecanismos de adecuación para mejor salvaguardar la privacidad y la autodeterminación informativa, garantizando la transparencia y, concomitantemente, el derecho a la información por el titular de datos[6].

En América Latina, países como Argentina, Chile y Colombia, editaron sus legislaciones de protección de datos. En Argentina, vigora la Ley nº 25.326, reglamentada por el Decreto 1.558/01 y por otras disposiciones de la Dirección Nacional de Protección de Datos Personales, en cuanto en Chile se sigue la Ley General Sobre Protección de la Información Personal.

En Brasil, el sistema jurídico de protección a la privacidad era fragmentado en las áreas de la salud, del sector financiero, de crédito y de telecomunicaciones, generando dificultades en la actuación del Sistema Nacional de Defensa del Consumidor (SNDC) para la prevención y la reparación de los derechos correlatos.

Ese sistema no estaba orientado por una legislación específica, restringiendo a las siguientes disposiciones o leyes dispersas: (i) Constitución Federal; (ii) Código Civil, con énfasis para su artículo 21, que asegura la protección de la vida privada de la persona natural; (iii) Código de Defensa de Consumidor, especialmente en su artículo 43; (iv) Ley nº 12.414/11 (Ley de Registro Positivo), que dispone sobre la formación y consulta a bancos de datos con informaciones de cumplimiento, de personas naturales o de personas jurídicas, para formación de historial de crédito; (v) Marco Civil de la Internet (Ley nº 12.965/14), reglamentado por el Decreto-ley nº 8.771, del 11 de mayo de 2016; (vi) Ley General de Telecomunicaciones (Ley nº 9.472/97) con destaque a su artículo 3º; y (vii) Ley Complementar nº 105/2001, que dispone sobre la confidencialidad bancaria.

Sin embargo, la Ley nº 13.709, del 14 de agosto de 2018, intitulada "Ley General de Protección de Datos Personales" (LGPD), inauguró un sistema de gobernanza de recolección y uso legítimo de datos personales, ya sea por el poder público o por el sector privado[7], volviéndose el centro axiológico y legislativo de datos personales en Brasil[8]

---

[5] A título de ejemplo, Viktor Mayer-Sconberger clasificó la evolución de las leyes de protección de datos en cuatro generaciones. En líneas generales, la protección surgió con enfoque tecnológico, con el objetivo de asegurar el control, vía concesiones, para la creación de bancos de datos personales y regular el control de uso de estos datos por el Estado. La regulación se desarrolló hasta alcanzar, actualmente, una tutela más efectiva de los datos personales en la complejidad y relevancia que la temática merece. Cf. MAYER-SCONBERGER, V. *General development of data protection in Europe*, En: *Tecnology and privacy: The new landscape*. (AGRE, P; ROTENBERG, M. coord.), MIT Press, Cambridge, 1997.

[6] Este reglamento es autoaplicable, o sea, no depende de leyes nacionales que sean compatibles con sus disposiciones.

[7] "**Art. 1º** Esta Ley dispone sobre el tratamiento de datos personales, inclusive en los medios digitales, por persona natural o por persona jurídica de derecho público o privado, con el objetivo de proteger los derechos fundamentales de libertad y de privacidad y el libre desarrollo de la personalidad de la persona natural.".

[8] La LGPD pasó por diversas alteraciones, mereciendo destaque la Medida Provisoria nº 959 de 2020, que amplió la *vacatio legis* de un número significativo de dispositivos para el 03 de mayo de 2021. Según lo dispuesto en el artículo 65, inc. I, de la LGPD, entraron en vigor, el 28 de diciembre de 2018, los artículos 55-A a 55-L, 58-A y 58-B. Por otro lado, la Medida Provisoria nº 959 de 2020 amplió la *vacatio legis* de los demás dispositivos para el 03 de mayo de 2021, a pesar de que sea necesario que esa medida todavía sea tratada por la Cámara y

Es importante resaltar que la LGPD tiene alcance extraterritorial, puesto que incidirá independientemente del país donde está localizada la sede de la persona jurídica de derecho público o privado. Es decir, se aplica al país donde estén localizados los datos, independientemente del país sede (art. 3º, "*caput*").

1.2. **Consentimiento y Autodeterminación Informativa**

La valorización del consentimiento sirvió para la consolidación de la autodeterminación informativa, inaugurando, según Stefano Rodotà, un movimiento "rumbo a un renacimiento del consentimiento"[9].

Bajo ese prisma, entendemos que la autodeterminación informativa es una extensión de la personalidad humana, constituyendo el derecho del titular a controlar y proteger sus datos personales mediante tecnologías de procesamiento de información[10].

La misma es consectaria de la privacidad y establece que el titular de los datos personales debe tener el control sobre la omisión o transmisión de sus datos. Paralelamente, debe existir transparencia total, también denominada *full disclosure*, acerca de las informaciones por el agente de tratamiento.

E, incluso frente a una política de total transparencia, tal no es suficiente para eliminar la responsabilización por daños causados por el uso indebido de datos del titular.

Eso proviene, sobre todo, de contratos relacionales - es decir, aquellos cuya ejecución se transfiere en el tiempo -, que, por definición, no siempre ofrecerán *feedbacks* razonablemente previsibles a sus participantes, pues, dada la existencia de costos de transacción y de la racionalidad limitada de las partes involucradas, es inevitable que, eventualmente, tales contratos se vuelvan completos para eventos que, en principio, pueden no estar cubiertos en el abanico de derechos y obligaciones establecidos y de riesgos asignados *ex ante* por los contratantes.

Por otro lado, se destaca que, cualesquiera que sean las asignaciones de derechos y obligaciones provenientes de esas decisiones tomadas *ex post*, tales decisiones siempre se dotarán de externalidades, lo que impone cautela redoblada para que decisiones de esa naturaleza no tergiversen *ex post* las expectativas de las partes en el momento de la contratación *ex ante* – especialmente en cuanto a la asignación de riesgos a ser soportados por los contratantes – y para que las mismas no creen inseguridad jurídica e impongan un aumento sistémico de los costos de transacción[11].

Sostenemos que la autodeterminación informativa puede manifestarse de varias formas durante el proceso de conocimiento y control del flujo de los datos personales por su titular.

Hay casos en los que, una vez ya compartidos sus datos personales, el titular desea tan solamente obtener la transparencia y el conocimiento acerca del tratamiento de sus datos por las organizaciones.

En este caso, se encuadran los deberes de información de los agentes de tratamiento con relación al titular, en observancia a los principios de la transparencia y del libre acceso.

---

por el Senado a fin de que la conviertan en ley y, con eso, produzca sus regulares efectos. Finalmente, los artículos correspondientes a las sanciones administrativas solamente entrarán en vigor a partir del 1º de agosto de 2021.

[9] RODOTÀ, S. *A vida na sociedade de vigilância: a privacidade hoje*, Ed. Renovar, Rio de Janeiro, 2008, p. 74.

[10] Según lo ya destacado, ese término surgió en el Tribunal Constitucional Federal alemán, en 1983, en decisión que involucra la Ley del Censo, en la que fueron declarados nulos dispositivos que permitían la comparación y transmisión de datos sensibles por reparticiones públicas.

[11] Nota técnica número 32/2019/CGCTSA/DPDC/SENACON/MJ. Proceso 08012.000723/2018-19. Disponible en: https://www.justica.gov.br/Acesso/sistema-eletronico-de-informacoes-sei. Acceso el 19.04.2020.

Por otro lado, hay situaciones en las que el titular de datos desea preservar su privacidad, intimidad o vida privada, poseyendo el derecho de anonimización, eliminación o rectificación de sus datos personales.

Esa es la lógica del artículo 17 de la LGPD, bajo el fundamento de que "*Toda persona natural tiene asegurada la titularidad de sus datos personales y garantizados los derechos fundamentales de libertad, de intimidad y de privacidad, en los términos de esta Ley.*".

En este punto, siguen los principios de la precisión y de la seguridad física y lógica. En el primero, el titular tiene asegurado el derecho de rectificación de sus datos. En el segundo, el controlador y el operador de banco de datos se ocupan de garantizar las precauciones necesarias en relación a la inapropiada utilización de los datos.

Creemos, por lo tanto, que la autodeterminación informativa es derecho personalísimo autónomo, dirigida a finalidades específicas de su titular, aunque tenga cierta relación con la privacidad. Se verifica, por ejemplo, la previsión del artículo 2º de la LGPD, que cita la privacidad, en un sentido amplio, en inciso apartado con relación a la autodeterminación informativa[12].

Cabe destacar el concepto de autodeterminación informativa emitido por el Departamento de Protección y Defensa del Consumidor, bajo el fundamento de que esta consiste en el poder de tomar personalmente las decisiones fundamentales sobre la utilización de sus datos personales, estando informado y consciente de las consecuencias de esta decisión[13].

Por ejemplo, la autodeterminación informativa y la transparencia exigen que el contrato de prestación de servicios tenga claridad en la política de uso de aplicaciones de internet.

Así, el tratamiento inadecuado de datos personales proviene del incumplimiento de la legislación pertinente al tema, o del no suministro de la seguridad que el usuario puede esperar del propio tratamiento, teniéndose en cuenta ciertas circunstancias relevantes.

Siguiendo lo dispuesto en el artículo 44 de la LGPD, son circunstancias relevantes, entre otras, "*el modo a través del cual se realiza el tratamiento*" (inc. I); "*el resultado y los riesgos que razonablemente se esperan del mismo*" (inc. II); y "l*as técnicas de tratamiento de datos personales disponibles en la época en la que fue utilizado*" (inc. III).

Los agentes de tratamiento deben adoptar medidas de seguridad como también medidas técnicas y administrativas aptas para la protección de datos personales frente a accesos no autorizados, además "[...] *de situaciones accidentales o ilícitas de destrucción, pérdida, alteración, comunicación o cualquier forma de tratamiento inadecuado o ilícito*" (art. 46, "caput", LGPD).

En el caso de que no se adopten esas medidas de seguridad, tanto el controlador como el operador responderán por los daños provenientes de aquella violación (art. 44, párrafo único, LGPD)[14].

---

[12] "Art. 2º La disciplina de la protección de datos personales tiene como fundamentos: I - el respeto a la privacidad; II - la autodeterminación informativa; III - la libertad de expresión, de información, de comunicación y de opinión; IV - la inviolabilidad de la intimidad, de la honra y de la imagen; V - el desarrollo económico y tecnológico y la innovación; VI - la libre iniciativa, la libre competencia y la defensa del consumidor; y VII - los derechos humanos, o-el libre desarrollo de la personalidad, la dignidad y el ejercicio de la ciudadanía por las personas naturales." .

[13] DPDC, de la Secretaría de Derecho Económico, del Ministerio de Justicia, fechado el 11.09.2013, nota número 40/CGEMM/DPDC/SENACON/2013. Disponible en: https://www.justica.gov.br/seus-direitos/consumidor/notas-tecnicas/anexos/40-2013.pdf. Acceso el 19.04.2020.

[14] En la esfera civil, las responsabilidades del controlador y del operador se definen con base en el artículo 42, §1, de la LGPD, que así dispone: "A fin de asegurar la efectiva indemnización al titular de los datos: I - el operador responde solidariamente por los daños causados por el tratamiento cuando incumpla las obligaciones de la legislación de protección de datos o cuando no haya seguido las instrucciones lícitas del controlador, hipótesis en que el operador se

Otra cuestión de suma importancia dice respecto al consentimiento y a la incidencia de daños a los titulares de los datos personales.

En la práctica forense, se firmó el entendimiento de que el carácter genérico del consentimiento obtenido por usuarios de plataformas *on-line* no puede ser visto como un "cheque en blanco" para que sus datos estén a disposición de quien quiera que sea[15].

En verdad, el conocimiento y el control de flujo de datos por sus titulares son de suma importancia para impedir prácticas consumeristas abusivas o fraudulentas.

En caso contrario, la divulgación de datos que no esté en consonancia con la declaración de voluntad del consumidor viola, entre otros dispositivos, el artículo 112 del Código Civil.

A título de ilustración, la incumbencia de demostrar la no filtración de datos y su regularidad es de los propios desarrolladores de los sitios y aplicaciones, pues estos tienen la capacidad de monitorear las operaciones en su plataforma, lo que no pueden realizar los propios consumidores.

2. **Tratamiento Inadecuado de Datos Personales y Modelos de Responsabilidad Jurídica**

2.1. **De la Integridad Como Flujo Informacional**

El tratamiento de datos proviene de una relación obligacional, ya sea gratuita u onerosa. Consiste en toda operación realizada con datos personales, tales como las que se destinan a la recolección, producción, recepción, clasificación, utilización, acceso, reproducción, transmisión, distribución, procesamiento, archivo, almacenamiento, eliminación, evaluación o control de la información, modificación, comunicación, transferencia, difusión o extracción (art. 5º, inc. X, de la Ley nº 13.709/18).

En ese prisma, el tratamiento adecuado de datos personales requiere una evaluación más amplia: es indispensable que se analice la integridad del flujo o tráfico de sus datos personales, denominada "privacidad como integridad contextual" ("privacy as contextual integrity"), bajo el riesgo de que desaparezca la importancia social del dato.

Los actores involucrados, el tipo o característica del dato personal y la forma a través de la cual se disemina son elementos para el análisis contextual. Compartiendo ese entender, Bruno Bioni agrega que es necesario un análisis progresivo de esos elementos bajo los prismas tanto del flujo informacional interno, referente a los actores y atributos del dato, como del flujo informacional externo, correspondiente a la diseminación[16].

En ese marco, la LGPD restringe las posibilidades en que el tratamiento de datos personales será admitido y, por lo tanto, legítimo, por medio de hipótesis legales, llamadas de bases legales o jurídicas. Vale decir, el tratamiento de los datos personales comunes solamente será posible si posee base teórica en una de las 10 (diez) bases legales previstas en el artículo 7º de la ley de regencia[17].

---

equipara al controlador, salvo en los casos de exclusión previstos en el art. 43 de esta Ley; II - los controladores que estén directamente involucrados en el tratamiento del cual provinieron daños al titular de los datos responden solidariamente, salvo en los casos de exclusión previstos en el art. 43 de esta Ley.".

[15] Nota técnica número 32/2019/CGCTSA/DPDC/SENACON/MJ. Proceso 08012.000723/2018-19. Disponible en: https://www.justica.gov.br/Acesso/sistema-eletronico-de-informacoes-sei. Acceso el 19.04.2020.

[16] BIONI, B. R. *Proteção de Dados Pessoais: a função e os limites do consentimento*, 2 ed, Ed. Forense, Rio de Janeiro, 2020, p. 199.

[17] CRUZ, A; RIBEIRO, C.A; TEIXEIRA, J.P. F; BAÑOS, J; MIRANDA, L.A; COTS, M; AZEVEDO, R; OLIVEIRA, R. "O Legítimo Interesse e a LGPD", (Oliveira, R; Cots, M. coords.), Thomson Reuters, São Paulo, 2020, p. 49-50.

El suministro del consentimiento (inc. I) es una base legal que autoriza el tratamiento de datos por el controlador y por el operador. Ya en las demás hipótesis (incs. II a X), los agentes de tratamiento están autorizados a tratar los datos independientemente del consentimiento.

En cuanto a los datos sensibles, se seguirán las 8 (ocho) bases legales del artículo 33 de la LGPD, además de una más híbrida, consistente en el tratamiento para la prevención de fraudes.

Si bien, será el caso de tratamiento inadecuado de datos si, en alguna de esas etapas, la operación con los propios datos ofende: (i) a la finalidad de los límites contractuales estipulados por las partes, o sea, si hay obtención y utilización de datos desvinculada o ajena a las finalidades de la propia recolección; (ii) al consentimiento del usuario.

Así, ese tratamiento inadecuado es susceptible de responsabilización en las esferas civil y administrativa, sin daño de responsabilidad criminal[18].

2.2. Tutela Individual y Modelos de Responsabilidad Civil en la LGPD

Fuera de la reglamentación legal acerca del tratamiento de datos personales, la responsabilidad civil es de suma importancia para el equilibrio de las relaciones correspondientes, máxime si la actividad acarrea daños a los titulares de datos[19].

Bajo el ángulo de la tutela individual, la protección de datos personales es instrumento esencial para la salvaguardia de la personalidad humana, razón por la cual es indispensable la institución de mecanismos que le garanticen al titular el conocimiento y control sobre sus propios datos[20].

El artículo 42 de la LGPD prevé la responsabilidad civil proveniente de las operaciones de datos personales, bajo el fundamento de que, en caso de violación a la legislación de protección de datos, tanto el controlador como el operador deberán responder por el daño causado a los otros, a título patrimonial, moral, individual o colectivo.

El operador también debe conocer las normas relativas a la protección de datos personales. En caso contrario, podrá incurrir en descumplimiento de la ley o actuar en desacuerdo con las instrucciones lícitas del controlador, respondiendo solidariamente (art. 42, §1º, inc. I)[21].

Además, es común que el tratamiento de datos personales envuelva más de un agente, principalmente más de un controlador. Así, serán responsabilizados

---

[18] La LGPD no prevé crímenes específicos para el tratamiento inadecuado de datos personales, al contrario de lo que se verifica en otros países, a ejemplo de la Ley de Protección de Datos Personales en Portugal (Ley nº 58/2019), que asegura la ejecución, en el orden jurídico nacional, del Reglamento General de Protección de Datos de la Unión Europea (Reglamento nº 2016/679).

[19] OPICE BLUM, R. NÓBREGA MALDONADO, V. *LGPD – Lei Geral de Proteção de Dados Comentada*, 2ª edição, Revista dos Tribunais, São Paulo, 2019, p. 323. Opice Blum y Nóbrega Maldonado agregan: "La responsabilidad civil en materia de datos personales es primordial para el equilibrio de las relaciones de esa naturaleza, sobre todo cuando se involucra la tecnología. A título ejemplificativo, una rápida búsqueda por un tema específico en Internet podrá rápidamente devolver una enorme base de datos. Más que eso, ese estudio, o acceso a un sitio, podrá iniciar o alimentar un interminable perfil sobre preferencias e intereses de ese usuario de la red, alimentando algoritmos y otras tecnologías predictivas a respecto del comportamiento del usuario, con masivo tratamiento de datos personales involucrado".

[20] Según dispone el artículo 22 de la LGPD, la defensa de los intereses de los titulares de datos podrá ser ejercida en juicio, individual o colectivamente, de acuerdo con las disposiciones e instrumentos previstos acerca de las tutelas individual y colectiva.

[21] "§1º A fin de asegurar la efectiva indemnización al titular de los datos: I - el operador responde solidariamente por los daños causados por el tratamiento cuando incumpla las obligaciones de la legislación de protección de datos o cuando no haya seguido las instrucciones lícitas del controlador, hipótesis en que el operador se equipara al controlador, salvo en los casos de exclusión previstos en el art. 43 de esta Ley".

solidariamente los controladores que estén involucrados directamente en el tratamiento del cual ocurrieron daños al titular de los datos (art. 42, §1º, inc. II)[22].

Ese modelo de responsabilidad ocupa suma importancia, pues no le compete al titular de datos el onus de identificar, dentro de una cadena económica, cuál de los agentes fue quien causó el daño[23].

Sin embargo, los agentes de tratamiento no serán responsabilizados si prueban (art. 43): (i) que no realizaron el tratamiento de datos personales que se les atribuye (inc. I); (ii) que, aunque hayan realizado el tratamiento de datos personales que se les atribuye, no hubo violación a la LGPD (inc. II); o (iii) que el daño proviene de culpa exclusiva del titular de los datos o de tercero (inc. III).

No obstante, la LGPD no prevé, claramente, si la responsabilidad es de naturaleza objetiva o subjetiva, haciéndose indispensable el análisis de esa temática[24].

En el ámbito de las relaciones de consumo, prevalece la responsabilidad objetiva, independientemente de culpa, por daños causados a consumidores por incidente de datos, aplicándose lo dispuesto en el CDC.

En efecto, la legislación consumerista, en sus artículos 12 a 14, disciplina, de forma clara, la responsabilidad objetiva de involucrados en la cadena de consumo, ya sea de productos o de servicios, cuyas características se analizarán oportunamente.

Los casos que no abarquen las relaciones de consumo, prevalece, en regla, la responsabilidad subjetiva mientras la responsabilidad objetiva será aplicada solamente en hipótesis excepcionales, es decir, mediante expresa previsión legal, puesto que tal no es presumible[25].

2.3. Responsabilidad Objetiva y Teorías del Riesgo

Bajo el ángulo del Derecho Civil, la responsabilidad objetiva tiene respaldo en la teoría del riesgo, en particular en el riesgo de la actividad, según consagrado en el artículo 927, párrafo único, del Código Civil[26].

En virtud de la teoría del riesgo, se configura la responsabilidad objetiva como resultado del riesgo de la actividad. Sin embargo, esa teoría posee diversas vestiduras, a saber: (i) teoría del riesgo integral; (ii) teoría del riesgo administrativo; (iii) teoría del riesgo provecho; y (iv) teoría del riesgo creado.

Por la teoría del riesgo integral, la responsabilidad es más abarcativa y contundente, prescindiendo de la configuración de nexo causal y aunque la causa del daño haya sido exclusivamente de la víctima.

Esa teoría no se aplica a la LGPD, pues el artículo 43 de la aludida legislación prevé, expresamente, causas de exclusión de la responsabilidad de los agentes de tratamiento, quitando toda posibilidad de riesgo integral por incidente de datos[27].

---

[22] "§1º II - los controladores que estén directamente involucrados en el tratamiento del cual ocurrieron daños al titular de los datos responden solidariamente, salvo en los casos de exclusión previstos en el art. 43 de esta Ley.".

[23] OPICE BLUM, R. NÓBREGA MALDONADO, V. *LGPD – Lei Geral de Proteção de Dados Comentada*, 2ª edição, Revista dos Tribunais, São Paulo, 2019, p. 323.

[24] La responsabilidad objetiva está respaldada en la prueba del daño y del nexo causal, independientemente de culpa. La responsabilidad subjetiva, a su vez, calza en la culpa en sentido amplio, envolviendo el dolo (conducta voluntaria) o la culpa en sentido estricto, o sea, negligencia, imprudencia o imperícia.

[25] OPICE BLUM, R. NÓBREGA MALDONADO, V. *LGPD – Lei Geral de Proteção de Dados Comentada*, 2ª edição, Revista dos Tribunais, São Paulo, 2019, p. 325.

[26] "Art. 927. Aquel que, por acto ilícito (arts. 186 y 187), cause daño a otros, queda obligado a repararlo. Párrafo único: Habrá obligación de reparar el daño, independientemente de culpa, en los casos especificados en ley, o cuando la actividad normalmente desarrollada por el autor del daño implique, por su naturaleza, riesgo para los derechos de otros."

[27] OPICE BLUM, R. NÓBREGA MALDONADO, V. *LGPD – Lei Geral de Proteção de Dados Comentada*, 2ª edição, Revista dos Tribunais, São Paulo, 2019, p. 327.

Por la teoría del riesgo administrativo, la responsabilidad objetiva vincula la Administración Pública por los daños causados en sus actividades de consecución del interés público. Vale decir, el particular no debe asumir los daños que son resultado de actividades de esa naturaleza, ya que depende del poder público proporcionarlas, asumiendo sus riesgos ante terceros (art. 37, §6º, CF)[28].

Ese modelo de responsabilidad se encuadra en la LGPD para los agentes públicos como resultado del tratamiento de datos personales. Cabe, sin embargo, una advertencia en cuanto a la responsabilidad objetiva, pues, de acuerdo con el entendimiento predominante del Supremo Tribunal Federal, tal solamente se aplica para eventuales actos comisivos de los agentes públicos, en cuanto que, para actos omisivos, la responsabilidad estatal es subjetiva[29].

Por la teoría del riesgo provecho, la caracterización de la responsabilidad objetiva, en especial del deber de indemnizar, se condiciona al provecho económico ganado en razón de la operación de tratamiento de datos personales, aunque indirectamente, con baluarte en la máxima "donde está el bono deberá estar la carga" ("*ubi emolumentum ibi ônus*").

Por último, la teoría del riesgo creado significa que el agente será obligado a indemnizar, independientemente de culpa o de cualquier provecho económico, por ejercer una actividad que, en su naturaleza, lo somete a una situación de riesgo.

2.4 **Toma de Postura**

Entendemos que la LGPD se fundamenta, en regla, en la responsabilidad civil subjetiva, siendo necesaria la demostración de la culpa y del daño, de conformidad con el artículo 186, c./c. el artículo 927, ambos del Código Civil.

Ese modelo de responsabilidad es compatible con la dignidad humana (art. 1º, inc. III, CF) y las finalidades de la LGPD, en particular la libre iniciativa y la seguridad jurídica de los agentes de tratamiento, evitando la banalización del deber de indemnizar simplemente por la realización de una actividad de riesgo[30].

Excepcionalmente, el tratamiento de datos personales puede constituir una actividad específica que, por su naturaleza y circunstancias, los riesgos le sean inherentes, siendo el caso de responsabilidad objetiva por los daños causados.

En ese punto, la responsabilidad objetiva consubstanciada en la teoría del riesgo, prevista en el Código Civil para casos excepcionales, también se aplica a incidentes de seguridad en datos personales a la luz de la LGPD.

La culpa asume aún mayor relevancia en las hipótesis del artículo 42, §1º, de la LGPD, que equipara el operador al controlador.

Es posible que ocurra una mitigación de la responsabilidad del controlador ante la inobservancia de alguna instrucción lícita por el operador.

---

[28] "Art. 37. §6º Las personas jurídicas de derecho público y las de derecho privado prestadoras de servicios públicos responderán por los daños que sus agentes, en esa cualidad, causen a terceros, asegurado el derecho de regreso contra el responsable en los casos de malicia o culpa"

[29] La LGPD disciplina la posibilidad de tratamiento e intercambio de datos por la administración pública. El artículo 7º, inc. III, de la LGPD prevé la base legal para tratamiento de datos, asegurando a la administración pública el tratamiento y uso compartido de datos necesarios para la ejecución de políticas públicas preceptuadas en leyes y reglamentos o respaldadas en contratos, convenios o instrumentos similares. En lo que respecta a los datos sensibles, el tratamiento compartido de tales datos solamente podrá ocurrir, sin consentimiento del titular, cuando sean necesarios para la ejecución de políticas públicas previstas en leyes o reglamentos (art. 11, inc. II, "b", de la LGPD).

[30] Opice Blum y Nóbrega Maldonado complementan: "En versiones anteriores del Proyecto de Ley que dio origen a la Ley General de Protección de Datos, se llegaron a incluir disposiciones que conceptuaban la actividad de tratamiento de datos personales como actividad de riesgo, expresamente, las que después fueron retiradas de la proposición en el transcurso del proceso legislativo" (Cf. OPICE BLUM, R. NÓBREGA MALDONADO, V. *LGPD – Lei Geral de Proteção de Dados Comentada*, 2ª edição, Revista dos Tribunais, São Paulo, 2019, p. 327).

En un primer caso, si el controlador contrata al operador, mediante instrucciones lícitas, para el tratamiento de datos, pero el último los opera en desacuerdo con aquellas instrucciones, iniciando una nueva actividad de control para la cual no fue delegado, el operador se equipara al controlador y deberá ser responsabilizado solidariamente, con fulcro en el art. 42, §1º, inc. I, de la LGPD.

Incluso así, el controlador podrá eximirse de la responsabilidad civil si comprueba que el daño fue resultado de culpa exclusiva del operador, ajustándose en la hipótesis prevista en el artículo 43, inciso III, de la LGPD[31].

También es digno de mención, la inversión de la carga probatoria, que podrá ser determinada por el magistrado en caso de imposibilidad o excesiva dificultad en cumplir el encargo probatorio, siendo cierto que tal medida depende de la fundamentación necesaria[32].

E, independientemente de la responsabilidad objetiva o subjetiva, es cierto que el deber de indemnizar depende, estrictamente hablando, de la efectiva demostración del daño, salvo en los casos de daño presumido ante el incidente que haya violado la intimidad del titular de datos.

En el último caso, sostenemos que no todo daño deberá ser presumido - incluso los casos excepcionales -, debiendo ser analizadas las circunstancias de cada situación fáctica, bajo pena de volverse trivial el deber de indemnizar.

En el caso de que se reconociera el daño presumido en todas las situaciones excepcionales, operaría de forma automatizada, la responsabilidad objetiva por un incidente de seguridad incluso frente a un daño inexistente, alejándose de los reales objetivos de la LGPD, que son los de garantizar la libre iniciativa y la seguridad jurídica a los agentes de tratamiento[33].

2.5. **De la Tutela Procesal Colectiva**

Bajo la perspectiva colectiva, la autodeterminación informativa no involucra solamente el permiso del consumidor para la utilización de sus datos personales. Va más allá: constituye un proceso de tratamiento de las informaciones en etapas, cada una de ellas contiene mecanismos para garantizar los derechos fundamentales colectivos.

Por lo que se ha firmado el entendimiento de que las normas de protección colectiva también son necesarias para la salvaguarda de datos personales, no bastando la tutela individual.

Eso porque, con el desarrollo tecnológico y el crecimiento y consolidación del comercio electrónico, se verificó la masificación de bancos de datos personales de consumidores. Por esta razón, la construcción de un ordenamiento jurídico internacional de protección de datos personales se desvinculó, al menos en parte, del enfoque individualista y adoptó la protección colectiva.

El tratamiento de datos personales puede consistir en actividad de masa, afectando un número indeterminado de personas, razón por la cual es pacífica la idoneidad de las acciones para la reparación de daños colectivos, o sea, para la protección de los derechos difusos, colectivos e individuales homogéneos.

El artículo 22 de la LGPD prevé la aplicación de la tutela colectiva de los datos personales, con incidencia de las legislaciones pertinentes, sean ellas, la Ley

---

[31] Por más que el ejemplo se refiera a la exclusión de responsabilidad del controlador, tal distancia podrá incidir en el operador, he aquí que el artículo 43 de la LGPD se refiere a "agentes de tratamiento".

[32] La LGPD también reconoce la posibilidad de inversión de la carga de la prueba en sede de proceso civil, en los términos del artículo 42, §2º: "El juez, en el proceso civil, podrá invertir la carga de la prueba a favor del titular de los datos cuando, a su juicio, la alegación sea verosímil, haya hiposuficiencia para fines de producción de prueba o cuando la producción de prueba por el titular le resulte excesivamente onerosa.".

[33] En el mismo sentido: OPICE BLUM, R. NÓBREGA MALDONADO, V. *LGPD – Lei Geral de Proteção de Dados Comentada*, 2ª edição, Revista dos Tribunais, São Paulo, 2019, p. 328.

7.347/85 (Ley de la Acción Civil Pública), especialmente su artículo 21, y los artículos 81, 90 y 104 del CDC, en virtud del principio de la integración.

La protección colectiva también está consagrada en el artículo 42 de la LGPD, bajo el fundamento de que el controlador o el operador tienen la obligación de reparar el daño causado a otros en virtud del ejercicio de actividad de tratamiento de datos personales.

Y, en consonancia con lo que dispone el §3º del artículo 42 de la ley de regencia, las acciones de reparación por daños colectivos que tengan por objeto la responsabilización civil, pueden ser ejercidas colectivamente en juicio[34].

En nuestra opinión, la protección de datos personales deberá ser ejercida en todas las categorías de derechos colectivos (en sentido amplio o "lato sensu"), involucrando tanto los derechos difusos y colectivos como los individuales homogéneos, además de comprender la máxima amplitud del proceso colectivo, admitiendo todas las especies de acciones, procedimientos, disposiciones y medidas, máxime de liminares ante la dinámica de flujo de los datos personales[35].

Los derechos difusos comprenden grupos menos determinados de personas - mejor que personas indeterminadas, son antes personas indeterminables-, entre las cuales no existe vínculo jurídico o fáctico preciso. Son como un haz o conjunto de intereses individuales, de objeto indivisible, compartidos por personas indeterminables, que están unidas por circunstancias de hecho conexas[36].

Incidirá esa forma de protección para asegurar el respeto, por los agentes de tratamiento, a la privacidad y a la autodeterminación informativa de ciudadanos indeterminables expuestos a prácticas abusivas, cuya tutela se caracteriza por su naturaleza indivisible y sin existencia de relación jurídica-base.

Los intereses colectivos en sentido estricto ("*stricto sensu*"), a su vez, tienen como principal diferencia la indeterminación relativa de los sujetos. El enlace entre los varios titulares colectivos surge de una relación jurídica-base, tales como el hecho de integrar el mismo banco de datos personales de un determinado proveedor de producto o servicio[37].

Es decir, hay una relación jurídica-base entre los consumidores y el controlador de banco de datos – léase, el proveedor -, bien como una tutela indivisible.

Los derechos individuales homogéneos, como lo sugiere la propia terminología, son esencialmente individuales. No obstante, se tratan de forma colectiva para la mejor defensa de sus titulares en juicio, desde que provengan de origen común[38].

Por ejemplo, esa tutela se dirige al resarcimiento de daños materiales (patrimoniales) y morales por fuga de datos personales de un grupo de personas, desde que los daños provienen de un origen común.

Se expresa en ese sesgo, el principio de la amplia jurisdicción de la demanda, que tiene por finalidad primordial discutir asunto en común en la acción colectiva, posibilitando la extensión "in utilibus" de la cosa juzgada colectiva, con base en el artículo 94 del CDC, combinado con los artículos 6º y 7º de la LACP.

Y, siguiendo los principios de la universalidad de la jurisdicción y del máximo beneficio de la tutela jurisdiccional colectiva común, una única sentencia, por medio de la inmutabilidad de sus efectos, aprovecha a un número indeterminado de interesados, notadamente de las víctimas y sus sucesores, que la podrán invocar, en provecho individual, para la liquidación y la ejecución de ese título, sin la necesidad de presentación de acciones individuales para la obtención de sentencias individuales (art. 103, §3º, CDC).

---

[34] "Art. 42. §3º Las acciones de reparación por daños colectivos que tengan por objeto la responsabilización en los términos del caput de este artículo pueden ser ejercidas colectivamente en juicio, observado lo dispuesto en una legislación pertinente."

[35] Se desprende del análisis conjunto de la LACP (arts. 12 y 21), del CDC (arts. 83 y 90) y del principio constitucional de la inestabilidad jurisdiccional (art. 5º, XXXV, CF).

[36] MAZZILI, H. N. *A defesa dos interesses difusos em juízo*, 31ª ed, Saraiva, São Paulo, 2018, p. 55.

[37] CARVALHO NETO, I. *Manual de Processo Coletivo*, Juruá, Curitiba, 2008, p. 36.

[38] VIGLIAR, J. M. M. *Ação Civil Pública*, Atlas, São Paulo, 2001, p. 54.

Se señala que los legitimados para ejercer la protección colectiva de los datos personales son los mismos de la acción civil pública, o sea, todos los enumerados en el artículo 5º de la Ley 7.347/85[39].

Habiendo una brecha de alguna de las leyes de ese microsistema de tutela colectiva de datos personales, le cabrá al intérprete suplirla por medio de la aplicación subsidiaria del Código de Proceso Civil.

3. Daño Moral Colectivo y Sello de Doble Castigo por el Mismo Hecho ("*Ne bis in idem*")

Antes de la edición de la LGPD, la jurisprudencia ya se inclinaba hacia el reconocimiento del daño moral colectivo, en particular por el riesgo de fuga de los datos personales de clientes o no clientes.

Por ejemplo, el Ministerio Público del Distrito Federal y de los Territorios, por medio de su Comisión de Protección de Datos Personales, pleiteó, en acción civil pública, la condenación de un banco digital a la indemnización de daños causados a intereses colectivos, como resultado de un incidente de seguridad, o sea, omisión en la seguridad de la información ante la extorsión de un supuesto "hacker", culminando en la fuga de datos personales de clientes y no clientes (v.g., empleados y ejecutivos) de aquella institución financiera[40].

En el proceso administrativo, la reparación del daño colectivo también es posible en el ámbito de las sanciones administrativas para las prácticas infractoras consideradas graves, sin perjuicios de las sanciones de naturaleza civil, penal y de las definidas en normas específicas, según lo dispuesto en el CDC y en el Decreto nº 2.181/97[41].

Tratándose de datos personales, es posible la caracterización de las prácticas infractoras previstas en los incisos X a XV del artículo 12 en el Decreto nº 2.181/97, que generalmente involucran la circunstancia agravante relativa al daño colectivo o de carácter repetitivo, cuya sanción administrativa deberá ser fijada con ayuda del artículo 18, c./c. el artículo 26, inciso VI, ambos del decreto aludido[42].

---

[39] Ellos son: (i) Ministerio Público, (ii) Defensoría Pública, (iii) Unión, estados, Distrito Federal y Municipios, (iv) autarquías, empresas públicas, fundaciones o sociedades de economía mixta; y (v) asociaciones.

[40] Acerca de los hechos, se instauró la investigación civil nº 08190.097749/18-95. El Ministerio Público del Distrito Federal y de los Territorios ofreció acción civil pública (proceso nº 0721831.64.2018.8.07.0001), bajo la narración de que el banco digital se vale de tecnologías móviles, tales como aplicaciones, bajo la alegación de que sus usuarios cuentan con un control rápido y "seguro" de sus cuentas. A principios de mayo de 2018, un "hacker" invadió el sistema informático del banco y reubicó los datos personales de, aproximadamente, 100 mil personas, que involucraban documentos, fotos de cheques, e-mails, transacciones, contraseñas e informaciones personales de clientes y no clientes, en archivo criptografado de 40 GB, exigiendo ventaja financiera para impedir la fuga de datos. Negándose a responder a los cuestionamientos formulados por el órgano ministerial, el banco se limitó a informar, el 10 de mayo de 2018, que no había fraude referente al incidente, ni a la presencia de daños a sus clientes. El 18 de diciembre de 2018, la 15ª Vara Cívil de la Circunscripción Especial Judiciaria de Brasília homologó el acuerdo, en audiencia de conciliación, entre el banco y el órgano ministerial, consistente en la reparación de los daños morales colectivos de carácter nacional, por el valor de R$ 1.500.000,00. Para acceso a la acción civil pública y al acuerdo, cf.: Disponible: https://www.mpdft.mp.br/portal/pdf/noticias/dezembro_2018/ACP_-_Banco_Inter.pdf. Acceso el 02/06/2020; https://www.mpdft.mp.br/portal/pdf/noticias/dezembro_2018/Ata_de_Audi%C3%AAncia_Banco_Inter.pdf. Acesso el 02/06/2020.

[41] El Decreto nº 2.181/97 dispone sobre la organización del Sistema Nacional de Defensa del Consumidor, además de instituir normas generales de aplicación de las sanciones administrativas, sin perjuicio de las sanciones de naturaleza civil, penal y de las definidas en normas específicas (art. 18).

[42] "Art. 12. [...] X - impedir o dificultar el acceso gratuito del consumidor a las informações existentes en subscripciones, fichas, registros de datos personales y de consumo, archivados sobre sí mismo como también sobre las respectivas fuentes; XI - elaborar registros de

En el caso *Cambridge Analytica*, el Departamento de Protección y Defensa del Consumidor (DPDC), de la Secretaría Nacional del Consumidor (SENACON), instauró proceso administrativo (nº 08012.000723/2018-19) ante *Facebook Inc.* y *Facebook* Serviços Online do Brasil Ltda., con el fin de determinar irregularidades cometidas por los representados, consistente en el intercambio indebido de datos de usuarios.

Facebook fue condenado por violación a los principios de la buena fe, al derecho a la privacidad y a las informaciones claras y adecuadas sobre bienes y servicios, reconociendo que, pese a que los actos lesivos fueron de responsabilidad de la matriz norteamericana de la empresa, la teoría de la apariencia y de la solidariedad determinan que la persona jurídica del mismo grupo económico localizada en Brasil tiene legitimidad para figurar en el polo pasivo de la acción, con apoyo en §2º del artículo 11 del Marco Civil de Internet[43].

En ese marco, el Ministerio de Justicia y Seguridad Pública editó la Portería nº 71, del 28 de febrero de 2020, que dispone sobre las reglas para la formalización de término de ajuste de conducta (TAC) en los procesos administrativos sancionatorios, en el ámbito de la Secretaría Nacional del Consumidor y del Ministerio de Justicia y Seguridad Pública.

Entre las cláusulas obligatorias de acuerdo, una de ellas se refiere al daño colectivo. Es decir, el acuerdo deberá contener el compromiso de ajuste de la conducta irregular dirigido a la reparación del daño colectivo y, al mismo tiempo, la prevención de conductas similares (art. 10, inc. I, de la Portería nº 71)[44].

La conclusión del acuerdo no tendrá importancia en la confesión acerca del asunto de hecho, tampoco en el reconocimiento de la ilicitud de la conducta irregular, ocasionando el archivo del proceso administrativo correspondiente. No obstante, la prestación de informaciones incorrectas sobre los compromisos asumidos autorizará el reenvío del hecho a los órganos de persecución criminal, además de la aplicación de la multa por valor superior a las sanciones a ser cumplidas en el proceso administrativo originario (art. 10, §3º, inc. I).

Sin perjuicio, la LGPD cuenta con previsión demasiado amplia, admitiendo expresamente el daño moral colectivo en sede de tutela civil, bajo la premisa de que el controlador u operador que "[...] cause a otros daño patrimonial, moral, individual

---

consumo con datos irreales o imprecisos; XII - mantener registros y datos de consumidores con informaciones negativas, divergentes de la protección legal; XIIII - dejar de comunicar al consumidor, por escrito, la abertura de subscripción, ficha, registro de datos personales y de consumo, cuando él no lo solicitó; XIV - dejar de corregir, inmediata y gratuitamente, la inexactitud de datos y registros, cuando el consumidor lo solicite; XV - dejar de comunicar al consumidor, en un plazo de cinco días útiles, las correcciones de registro que él solicitó [...]".

[43] Según la nota técnica, *Facebook* Serviços Online do Brasil Ltda. fue notificado para responder a los siguientes cuestionamientos, con base en el art. 44 de la Ley nº 9.784/99 y en el art. 42 del Decreto nº 2.181/97: "¿Cuál es el alcance del supuesto intercambio irregular? O sea, ¿cuál es el número de usuarios brasileños afectados por eso? ¿Cuál era la finalidad de la captura de los datos de los consumidores? Detalle y aclare; Según las noticias, los usuarios habían estado de acuerdo en hacer un "test" en línea y habían consentido en compartir sus datos "para fines académicos". ¿Esa información procede? Si no, ¿cómo los datos de los usuarios brasileños fueron compartidos con Cambridge Analytica? Informe; Informe si, además de Cambridge Analytica, los datos compartidos también se proporcionaron a otras empresas sin que el usuario brasileño haya dado consentimiento específico para eso; ¿Facebook tiene asociación, contrato o cualquier vínculo con empresa que promueva el marketing político partidario en Brasil? En caso afirmativo, explique; Después de la asunción de intercambio irregular, por parte de la empresa, ¿qué hizo o está haciendo Facebook para solucionar el problema? Especifique las acciones tomadas de forma minuciosa; ¿Cómo actúa Facebook para proteger los datos de sus usuarios y de qué instrumentos dispone para que esa protección sea efectiva?" Nota Técnica nº 32/2019/ CGCTSA/DPDC/SENACON/MJ. Proceso 08012.000723/2018-19. Representante: Departamento de Protección y Defensa del Consumidor – *ex officio*. Representados: Facebook Inc. y Facebook Serviços Online do Brasil Ltda. Decisión de 27/12/2019, pág. 2.

[44] Disponible: http://www.in.gov.br/en/web/dou/-/portaria-n-71-de-28-de-fevereiro-de-2020-245476418. Acceso el: 02/06/2020.

o colectivo, en violación a la legislación de protección de datos personales, está obligado a repararlo" (art. 42, "caput", parte final).

A partir de la lectura precisa de la ley, son posibles las siguientes modalidades de daño: (i) daño patrimonial, de naturaleza individual; (ii) daño moral individual; y (iii) daño moral colectivo.

Se sugiere, además, cautela en la fijación de la reparación del daño civil y de la multa en la esfera administrativa, bajo el riesgo de violación a la prohibición del doble castigo por el mismo hecho ("ne bis in idem").

Dependiendo de las circunstancias fácticas, la multa simple podrá ser impuesta en hasta el 2% (dos por ciento) de la facturación de la persona jurídica de derecho privado – excluidos los tributos -, limitado el total a R$ 50.000.000,00 (cincuenta millones de reales) por infracción (art. 52, inc. II). Paralelamente, el daño moral colectivo también asume funciones punitiva, preventiva, pedagógica y reparadora, debiendo ser arbitrado en cumplimiento a los principios de la razonabilidad y de la proporcionalidad, sin la exacerbación de valores y enriquecimiento sin causa.

Además, ha de ser calculado con base en la extensión o consecuencias del daño, además de tener en cuenta las condiciones económicas y sociales tanto de la víctima como de la persona jurídica obligada, siguiendo lo dispuesto en el artículo 944 del Código Civil[45].

Tratándose de relaciones de consumo, las funciones preventivas y pedagógicas tienen el objetivo de desestimular la práctica de actos similares no solamente por el infractor como también por los demás integrantes de la sociedad. Se destina al perfeccionamiento continuo de los proveedores y prestadores de servicio en general, bajo pena de condena judicial.

La función reparadora, a su vez, tiene la finalidad de compensar los daños sufridos por la víctima, ante la imposibilidad de restablecerse, mediante pago en dinero, la condición anterior ("status quo ante").

La función punitiva implica subsidio de dinero por parte del infractor por no respetar las normas protectoras y cogentes del Código de Defensa del Consumidor, correspondiéndole, de esa manera, satisfacer al consumidor por el ilícito practicado.

4. Complejidad Digital y Vulnerabilidad Ampliada

4.1. De la Vulnerabilidad en el Ambiente Digital

Desde la perspectiva del Código de Defensa del Consumidor, la vulnerabilidad es uno de los principios de mayor importancia para la protección del consumidor, consagrado en el artículo 4º, inciso I, de la Ley nº 8.078/90. Vale decir, la vulnerabilidad es un presupuesto fáctico, inherente a todo consumidor, que asegura una ecuación justa en el ámbito de las relaciones de consumo.

La vulnerabilidad asume las siguientes clasificaciones: (i) vulnerabilidad técnica; (ii) vulnerabilidad jurídica; (iii) vulnerabilidad fáctica; y (iv) vulnerabilidad informacional[46].

En vista de las más diversas vulnerabilidades, se garantiza a los consumidores el conocimiento y el control acerca del flujo de sus datos personales en las relaciones de consumo, máxima en el comercio electrónico, en vista de que tales informaciones se ofrecen inexorablemente para la constitución del contrato consumerista.

En este contexto, el ambiente digital se caracteriza por su complejidad, causando la despersonalización, desmaterialización, desterritorialización y atemporalidad de la contratación electrónica, haciendo que el consumidor sea más

[45] "La indemnización se mide por la extensión del daño".

[46] Por ejemplo, se aplica la LGPD a borrador o lista que contenga datos personales y que servirá a cierta actividad empresarial, de connotación económica.

frágil, con la consecuente ampliación de su vulnerabilidad, sobre todo del titular de datos[47].

Y esa vulnerabilidad ampliada o agravada[48] es designada por una parte considerable de la doctrina como "hiper vulnerabilidad"[49].[50]

Entre los desiguales, la voluntad de las partes no puede ser más dejada enteramente libre (escenario exclusivamente privado), debiendo ser sometida a las dimensiones pública y social de las relaciones jurídicas. O sea, la libertad de las partes es, en lo sucesivo, pautada y limitada por normas que aunque no anulen el interés privado, lo condicionan a la búsqueda del equilibrio; normas que limitan el poder del proveedor - más fuerte en la relación - y, al mismo tiempo, crean mecanismos de compensación al consumidor – parte vulnerable[51].

La informática se caracteriza por su complejidad, pues, aunque haya educación en el usuario para utilizarla, no se volverá un técnico del asunto y, por lo tanto, constantemente encontrará dudas acerca de su modo de uso e informaciones.

Vale decir, el usuario está distante de las informaciones técnicas en el área de la informática, desconociendo las funciones, límites y riesgos de los sistemas.

La complejidad induce, a veces, al propio usuario a adherirse o a adoptar comportamientos de forma insegura.

Valiéndose de esa complejidad, no es poco común que los proveedores, voluntariamente, dejen de registrar, en los *websites*, las informaciones necesarias sobre su producto o servicio, incumpliendo su deber de informar al consumidor.

La violación del deber de informar proviene de varias causas, entre las cuales: (i) la intención de ocultar condiciones contractuales que sean abusivas o "leoninas"; (ii) intención de ocultar productos defectuosos o servicios deficientes.

---

[47] La vulnerabilidad técnica significa que, en ciertas situaciones, el consumidor no tiene informaciones técnicas sobre el producto o el servicio. La vulnerabilidad jurídica significa que el consumidor no conoce sus derechos y deberes en el ámbito de las relaciones de consumo. La vulnerabilidad fáctica, a su vez, se caracteriza como una situación concreta específica en la cual el consumidor posee cierta debilidad, como en los siguientes ejemplos: (i) consumidor niño; (ii) anciano; (iii) consumidor analfabeto, entre otros. Finalmente, la vulnerabilidad informacional es desdoblamiento de la vulnerabilidad fáctica, o sea, el consumidor está situado en una posición pasiva en el ámbito de las relaciones de consumo, sin tener condiciones plenas de conferir la veracidad de las informaciones del producto, además de ser vulnerable a las estrategias de comunicación y de publicidad de los proveedores ("marketing"). La vulnerabilidad informacional también guarda relación con la vulnerabilidad técnica, puesto que el consumidor, frente a la complejidad del ambiente digital, no posee conocimiento suficiente acerca de elementos técnicos del producto o servicio ofrecidos en aplicaciones o sitios de internet, haciendo inviable su comprensión sobre el funcionamiento de las tecnologías y de los riesgos a los cuales está sometido.

[48] Según Bruno Bioni: "Por eso, se señala que el consumidor es (hiper) vulnerable en medio de ese mercado informacional. Ese agravamiento proviene de la situación objetiva pertinente a su inserción en el mercado informacional, cuyos trazos de vulnerabilidad son peculiares y se sobreponen al común de las tradicionales relaciones de consumo" (BIONI, B. R. "Proteção de Dados Pessoais: a função e os limites do consentimento", 2 ed, Ed. Forense, Rio de Janeiro, 2020, p. 158).

[49] Etimológicamente, la "hiper vulnerabilidad" está compuesta por el prefijo griego "hyper", que consiste en "aumento" o "agravamiento", además de "vulnerabilidad", que proviene del latín "vulnus", o sea, "lastimado" o "herida". Así, "hiper vulnerabilidad" consiste en la potencialización o agravamiento de la vulnerabilidad.

[50] La doctrina difiere si la hiper vulnerabilidad se define a partir de criterio objetivo o subjetivo. Para Bruno Bioni, se adopta el criterio objetivo del consumidor, independientemente del análisis acerca de la situación, permanente o temporaria, que se encuentra el consumidor; basta que esté inserto en el mercado informacional para que sea hiper vulnerable (BIONI, B. R. *Proteção de Dados Pessoais: a função e os limites do consentimento*, 2 ed, Ed. Forense, Rio de Janeiro, 2020, p. 158, nota de pie de página, ítem 134).

[51] RIOS, J. O. "A defesa do consumidor e a imprensa". En: MORATO, A. C. NERI, P. T. *Vinte anos do Código de Defesa do Consumidor. Estudos em Homenagem ao Professor José Geraldo Brito Filomeno*, Atlas, São Paulo, 2010, p. 42.

En ese escenario, los productos singulares o específicos, que poseen características propias, impiden o dificultan el conocimiento pleno de sus especificidades por parte del consumidor, ampliando la vulnerabilidad técnica de este.

La vulnerabilidad técnica no deriva tan sólo de la falta o insuficiencia de informaciones sino también de sus excesos o del suministro de informaciones innecesarias, dificultando la comprensión del consumidor acerca de los detalles o especificaciones técnicas del producto o servicio, con la consecuente "polución informacional".

Teniendo en vista que la vulnerabilidad del usuario es agresiva y amplia, es indispensable que se amplíe, proporcionalmente, el espectro del deber de informar del proveedor.

Por otro lado, se amplía la complejidad del ambiente digital a medida que las tecnologías y los medios de suministro de productos y servicios evolucionan rápida y abruptamente, razón por la cual el consumidor, incluyendo al titular de datos personales, no tiene condiciones – técnicas e informacionales - de acompañar *in pari passu* tales cambios, restando ampliadas sus vulnerabilidades técnicas e informacionales.

Esa vulnerabilidad es incluso agravada debido a las siguientes prácticas: (i) asimetría informacional[52]; (ii) datos comportamentales y *adaptive pricing*[53]; (iii) *geoblocking* y *geopricing*[54]; y (iv) problema de agregación (*problem of aggregation* ou *aggregation effect*)[55] y crimen de hurto de identidad ("*identify theft*"), que equivale al *phishing*, todavía no criminalizado en Brasil[56].

---

[52] El amplio acceso del proveedor a las informaciones obtenidas sobre el consumidor puede caracterizar una nueva vulnerabilidad. Esa información en abundancia del proveedor, involucrando la obtención de datos personales del consumidor, provoca un desequilibrio en las relaciones de consumo en sus diversas etapas y, como consecuencia, una asimetría informacional, requiriendo una reevaluación de los fundamentos contractuales, a ejemplo de la buena fe.

[53] La publicidad comportamental tiene la finalidad de analizar los modos de uso de internet y de consumo por parte de los usuarios, con el objetivo de utilizarlos para la elaboración y divulgación de anuncios alineados a las preferencias y hábitos de los propios usuarios-consumidores.

[54] Los proveedores, por medio del análisis de esos dados comportamentales, adaptan el precio de sus productos o servicios ofrecidos por internet, de acuerdo con la localización o región en que el consumidor realiza el acceso, acarreando en el *geoblocking* y *geoprincing* y, consecuentemente, en la discriminación ilícita del consumidor.

[55] Para Solove, la concepción tradicional de privacidad no debe prosperar frente a lo que él denomina "problema de agregación" ("*problem of aggregation*"). La tecnología tiene el potencial de agregar detalles e informaciones del consumidor y, con eso, hace posible la creación de su personalidad. Vale decir, cada parte de las informaciones individuales, una vez analizadas aisladamente, no son reveladoras. Sin embargo, las informaciones personales se hacen significativas a partir del momento en el que se analizan en conjunto, siendo posible crear un retrato sobre la personalidad de cada individuo, o mejor dicho, de su biografía digital (*digital biography*). Así, "la información genera información" (SOLOVE, D. J. "Access and Aggregation: Public Records, Privacy and the Constitution". En: *Minnesota Law Review*, v. 86, 2002, p. 1138-1217. Disponible: https://scholarship.law.umn.edu/mlr/1094. Acceso el: 19/04/2020, p. 1185).

[56] El hurto de identidad consiste en la conducta del agente que se apodera de informaciones personales de un individuo para abrir nuevas cuentas bancarias, adquirir tarjetas de crédito, obtener préstamos de la forma más rápida posible, entre otros. Se encuadra, técnicamente, en el *phishing*, también llamado "pesca *on-line* de identidad" o "pesca de informaciones personales y confidenciales por medio de dispositivos informáticos", o sea, en la conducta de confundir a los usuarios de internet para que brinden informaciones personales o confidenciales, en lo que el infractor, con pose de las informaciones, logra acceso a determinados servicios, tales como e-mail o home banking, con la finalidad de obtener ventaja económica indebida. En Brasil, la jurisprudencia lo clasifica como crimen de hurto mediante fraude, aunque, a nuestro ver, no deba ser considerado crimen patrimonial sino un acto preparatorio para otros crímenes. A propósito del tema, cf. GOMES, R. B. O; SILVA, M. S. L. "O Enquadramento Jurídico Penal do 'Phishing" e Suas Repercussões no Furto Informático". En: *Letras Jurídicas*, Centro Universitário Newton Paiva, n. 3, 2/2014, p. 177.

A título de ejemplo, la empresa "Decolar" ofreció una representación frente a "Booking.com", por la práctica de *geopricing* y *geoblocking*, ocasionando la instauración del proceso administrativo nº 08012.002116/2016-21[57].

Otra muestra es la discriminación de precio y la calidad del producto o servicio definidos de acuerdo con la publicidad comportamental ("profiling") y que, en regla, configuran prácticas abusivas. No raras veces, se ofrecen los precios discriminadamente a los usuarios, teniendo en cuenta sus circunstancias o características personales conocidas por la empresa.

Esas prácticas anticompetitivas generan consecuencias en los más diversos senos jurídicos.

En el Código de Defensa del Consumidor, está la configuración de prácticas abusivas, notoriamente la elevación, sin justa causa, del precio de productos y servicios (art. 39, inc. X, de la Ley nº 8.078/90).

En la Ley Antimonopolio, se caracteriza en acto competitivo, particularmente de discriminación de adquirientes o proveedores de bienes o servicios por medio de la fijación diferenciada de precios, o de condiciones operacionales de venta o prestación de servicios (art. 36, inc. X, "d", de la Ley nº 12.529/11).

En el Marco Civil de Internet, se configura una violación a la neutralidad de red, o sea, al tratamiento isonómico de datos, pues hay (indebidamente) una distinción de contenido, origen, servicio, terminal o aplicación.

Así, le compite al responsable por la discriminación o degradación del tráfico actuar de otra manera, tales como (art. 9º, §2º, incs. II y IV, de la Ley nº 12.965/14): (i) actuar con proporcionalidad, transparencia e isonomía (inc. II); y (ii) ofrecer servicios en condiciones comerciales no discriminatorias y abstenerse de practicar conductas anticompetitivas (inc. IV).

En la Ley General de Protección de Datos Personales, está la obtención y el uso indebido de datos personales. Cabe decir, la recolección y el tratamiento de datos, ya sean personales o sensibles, dependen del consentimiento de su titular (art. 2º, incs. II y VI, de la Ley nº 13.709/18), con respecto a la autodeterminación informativa (inc. II) y a la libre iniciativa, a la libre competencia y a la defensa del consumidor (inc. VI).

Importante sobresaltar que, tratándose de las bases legales, las actividades de tratamiento de datos personales deberán observar la buena fe y, máxime para la defensa del consumidor y evitar el *geopricing* y *geoblocking*, a los principios de la finalidad, de la adecuación, de la necesidad y de la no discriminación, siguiéndose lo dispuesto en el artículo 6º de la LGPD[58].

---

[57] "`EMENTA: PROCESO ADMINISTRATIVO. CONSUMIDOR. OFENSA A LA LIBERTAD DE DECISIÓN EN LAS CONTRATACIONES, POR LOS CONSUMIDORES. DIFERENCIACIÓN DE PRECIO DE ALOJAMIENTOS Y NEGATIVA DE OFERTA DE PLAZAS, CUANDO EXISTENTES, DE ACUERDO CON LA LOCALIZACIÓN GEOGRÁFICA DEL CONSUMIDOR. TÉCNICAS DE GEOPRINCING Y GEOBLOCKING. APLICACIÓN DE SANCIÓN DE MULTA POR EL VALOR DE R$ 7.500.000,00 (SIETE MILLONES QUINIENTOS MIL REALES). Se trata de Proceso Administrativo instaurado en el ámbito del Departamento de Protección y Defensa del Consumidor (DPDC), de la Secretaría Nacional del Consumidor, del Ministerio de Justicia (MJ), en razón del recibimiento de representación propuesta por Booking.com Brasil Serviços de Reserva de Hotéis Ltda. (Booking) – empresa que actúa en el mercado de hospedaje como intermediaria entre establecimientos hoteleros y consumidores – frente a la empresa Decolar.com Ltda" (Nota técnica del proceso 08012.002116/2016-21)".

[58] "Art. 6º Las actividades de tratamiento de datos personales deberán observar la buena fe y los siguientes principios: I - finalidad: realización del tratamiento para propósitos legítimos, específicos, explícitos e informados al titular, sin posibilidad de tratamiento posterior de forma incompatible con esas finalidades; II - adecuación: compatibilidad del tratamiento con las finalidades informadas al titular, de acuerdo con el contexto del tratamiento; III - necesidad: limitación del tratamiento al mínimo necesario para la realización de sus finalidades, con amplitud de los datos pertinentes, proporcionales y no excesivos en relación a las finalidades del tratamiento de datos; IV - libre acceso: garantía, a los titulares, de consulta facilitada y gratuita sobre la forma y la duración del tratamiento como también sobre la integralidad de sus datos personales; V - calidad de los datos: garantía, a los titulares, de exactitud, claridad,

En síntesis, todos los fundamentos abrazados comprueban que es extrínseca la fragilidad del consumidor, incluyendo la del titular de datos, pues tal deriva del poder económico y de prácticas abusivas en las relaciones de consumo.

La hiper vulnerabilidad no se define, por lo tanto, a partir de la condición subjetiva o especial de cada consumidor o titular de datos – tal como ocurre con los niños, adolescentes, ancianos, personas con deficiencia -, sino a partir de un criterio objetivo. Es decir, basta el consumidor estar insertado en el mercado informacional para que su vulnerabilidad se amplíe[59].

Frente a ese panorama, es imprescindible que se ofrezcan instrumentales jurídicos suficientes y dialógicos para la mitigación de esa vulnerabilidad y reequilibrio de las relaciones en el mercado informacional.

Proponemos, en un primer lugar, que los datos personales se salvaguarden a partir de una interpretación dialógica de las más diversas legislaciones, involucrando el Código de Defensa del Consumidor, el Marco Civil de Internet y la LGPD.

Además, es importante que, en la práctica forense, el intérprete y aplicador de la ley aprendan, lo máximo posible, el sentido y la finalidad de la LGPD, guiándose por la isonomía material.

En el intento de "desigualar las desigualdades", las normas de equilibrio, que componen la LGPD, aseguran tratamiento diferenciado al titular de datos que, a primera vista, parece infringir el principio de la isonomía cuando, en verdad, este garantiza el escopo de la legislación, concretando la igualdad jurídica o substancial.

Para identificar una violación al principio de la igualdad, es necesario averiguar cuándo es válida la desigualdad de una norma, o sea, es preciso que se conozca, con profundidad, cuál es el trazo de legitimidad que fundamenta determinado factor discriminatrio de una norma. El factor discriminatorio o diferenciador será válido si consustanciado en el camino posible y lógico para alcanzar el fin jurídico pretendido, cual sea, la justicia igualitaria[60].

En la mayoría de los casos, es necesaria y legítima la tutela penal de la privacidad y de datos personales, ya sea en el medio *off-line* o en el ambiente digital, sin perjuicio de los principios de la lesividad, de la fragmentariedad y de la intervención mínima (*ultima ratio legis*).

4.2. Derecho Administrativo Sancionador y Controversias Acerca de la Tutela Penal de los Datos Personales: la Hiper Vulnerabilidad Penal en el Ámbito de la LGPD

En Brasil, la opción legislativa se restringió a las responsabilidades administrativa y civil para la protección de datos personales, dejando de prever un modelo específico de responsabilidad criminal.

---

relevancia y actualización de los datos, de acuerdo con la necesidad y para el cumplimiento de la finalidad de su tratamiento; VI - transparencia: garantía, a los titulares, de informaciones claras, precisas y fácilmente accesibles sobre la realización del tratamiento y los respectivos agentes de tratamiento, observados los secretos comercial e industrial; VII - seguridad: utilización de medidas técnicas y administrativas aptas para proteger los datos personales de accesos no autorizados y de situaciones accidentales o ilícitas de destrucción, pérdida, alteración, comunicación o difusión; VIII - prevención: adopción de medidas para prevenir que ocurran daños en virtud del tratamiento de datos personales; IX - no discriminación: imposibilidad de realización del tratamiento para fines discriminatorios ilícitos o abusivos; X - responsabilización y prestación de cuentas: demostración, por el agente, de la adopción de medidas eficaces y capaces de comprobar la observancia y el cumplimiento de las normas de protección de datos personales e, inclusive, de la eficacia de esas medidas.".

[59] En el mismo sentido, el entendimiento de Ricardo Bioni: "Se nota que esa nueva capa de vulnerabilidad no está basada sobre el estado subjetivo o incluso la condición personal del consumidor, tal como ocurre con los consumidores niños (BIONI, B. R. *Proteção de Dados Pessoais: a função e os limites do consentimento*, 2 ed, Ed. Forense, Rio de Janeiro, 2020, p. 158).

[60] FUX, L. WAMBIER, T. A. A. NERY JR, N. *Processo e Constituição. Estudos em homenagem ao Professor José Carlos Barbosa Moreira*, Revista dos Tribunais, São Paulo, 2006, p. 617.

Así, se optó por un Derecho Administrativo Sancionador, en el que los agentes de tratamiento de datos, en razón de las infracciones cometidas a las normas de la LGPD, quedan sujetos a las sanciones administrativas previstas en el artículo 52 de la aludida legislación y aplicables por la autoridad nacional de protección de datos personales, pudiendo, inclusive, ser impuesta una multa simple, de hasta el 2% (dos por ciento) de la facturación de la persona jurídica de derecho privado, grupo o conglomerado en Brasil en su último ejercicio, excluidos los tributos, limitada, en total, a R$ 50.000.000,00 (cincuenta millones de reales) por infracción[61].

A pesar del alto nivel de las multas, tal puede revelarse insuficiente en caso de grupos económicos. Por ejemplo, las sanciones presentadas pueden ser internalizadas por empresas de gran poder económico y, por lo tanto, se vuelven inocuas.

Entendemos, a partir de reglas de experiencia, que las penalidades administrativas más drásticas a los agentes de tratamiento, notoriamente a las sociedades empresarias, se refieren a la inoperancia de los datos, alcanzando, abruptamente, la actividad empresarial. El bloqueo (inc. V) o eliminación de datos personales (inc. VI), así como la suspensión (inc. XI) o prohibición total de actividades de tratamiento (inc. XII), hace inviable el desarrollo y el acompañamiento minucioso de la actividad empresarial, sobre todo del perfil y de cuestiones financieras de clientes, por ejemplo[62].

Y, aunque se contenplen esas penalidades en el seno administrativo, tales no tienen el don de alejar la dignidad penal, pues la violación a los datos personales constituye ofensa a la personalidad humana y, por lo tanto, de valor incomensurable.

Se señala que, en el caso de violación intencional al consentimiento o incluso a las finalidades del uso de datos personales, la LGPD no prevé ninguna responsabilidad criminal, que vaya en contra de las legislaciones europeas y latinoamericanas que tratan del asunto.

Por ejemplo, la Ley de Protección de Datos Personales de Portugal (Ley nº 58/2019) prevé, además de las responsabilidades administrativa y jurisdiccional, contra-ordenaciones y crímenes específicos para el tratamiento inadecuado de datos personales, entre los cuales el de "utilización de datos de forma incompatible con finalidad de la recolección" (art. 46º), según se evaluará oportunamente.

En Argentina, la Ley nº 25.326 consagra la responsabilidad administrativa, sin perjuicio de la responsabilidad criminal, a punto de conferir nueva redacción a los artículos 117 *bis* y 157 *bis* del Código Penal[63].

---

[61] El artículo 52 de la LGPD cataloga las infracciones administrativas aplicables a los agentes de tratamiento de datos, a seguir: (i) advertencia; (ii) multa de hasta el 2% de la facturación; (iii) multa diaria; (iv) publicización de la infracción cometida; (v) bloqueo de datos personales; (vi) eliminación de los datos personales.

[62] Igualmente en cuanto a la suspensión parcial del funcionamiento del banco de datos por el período máximo de 6 (seis) meses, prorrogable por igual período, hasta la regularización de la actividad de tratamiento por el controlador (inc. X); suspensión del ejercicio de la actividad de tratamiento de los datos personales por el período máximo de 6 (seis) meses, prorrogable por igual período (inc. XI); y prohibición parcial o total del ejercicio de actividades relacionadas con tratamiento de datos (inc. XII).

[63] Dispone el artículo 32 de la Ley nº 25.326: "1. El artículo 117*bis* del Código Penal debe ser incorporado como sigue: ´1 °. Será punida con una pena de prisión de un mes a dos años, a quien coloque o haga colocar informaciones, sabiendo que son falsas, en un archivo de datos personales. 2º. La pena será de seis meses a tres años, para quien, conscientemente, suministre informaciones falsas a terceros contenidas en archivo de datos personales. 3º. La pena será aumentada por la mitad del mínimo y del máximo, cuando el hecho termine en perjuicio a cualquier persona. 4º. Si el autor es funcionario público en ejercicio de sus funciones, le será aplicada la pena accesoria de inhabilitación para el ejercicio del cargo público por el doble del tiempo que lo fijado en la condenación. 2. El artículo 157*bis* del Código Penal debe ser incorporado como sigue: ´Será punido con pena de prisión de un mes a dos años a quien: 1º. De forma consciente e ilegítima, o en violación de los sistemas de confidencialidad y seguridad de datos, accese, por cualquier medio, un banco de datos personales; 2º Divulgue, a otros, informaciones registradas en banco de datos personales, cuyo secreto está obligado

Es cierto que los usuarios de internet se caracterizan por su vulnerabilidad ampliada, es por eso que la inseguridad digital los somete a los más diversos ilícitos penales, por lo que sugerimos el siguiente ideario: la "*hiper vulnerabilidad penal*".

Esa inseguridad también la provocan, entre otros factores, los fraudes o invasión de *crackers*, o sea, profesionales intelectualizados, con conocimiento informático, exploran las fallas técnicas de sistemas y dispositivos.

Y, según ya se resaltó, la LGPD no prevé crímenes específicos para el tratamiento inadecuado de datos personales, pese a que, actualmente, los fraudes a los datos personales y sensibles se someten a los tipos penales del Código de Defensa del Consumidor, Código Penal, Ley de los Crímenes Contra la Economía Popular, Ley 8.137/1990, Ley 7.716/89, entre otros.

Lo más apropiado es que, dependiendo del caso, la responsabilidad criminal incida de forma paralela a las responsabilidades civil y administrativa, apreciando el diálogo de las fuentes y por el "ne bis in idem".

CONCLUSIONES

A modo de conclusión, en las últimas décadas; comenzando en el ámbito internacional y enseguida en Brasil como también en otras naciones de América Latina; emergieron legislaciones dirigidas a la transparencia en la protección de datos personales. Todas estas normas se basan en la autodeterminación informativa y preponderan el consentimiento y el legítimo interés del titular de los datos personales.

Notamos que al ocurrir tratamiento inadecuado de datos se instaura el sistema de la responsabilidad tríplice, que puede darse a través de la tutela individual o de la tutela colectiva. En regla, la responsabilidad es subjetiva y, excepcionalmente, podrá ocurrir la incidencia de la responsabilidad objetiva, que dispensa el análisis de la culpa para que ocurra el daño.

Independientemente de la responsabilidad objetiva o subjetiva, es necesario resaltar que el deber de indemnizar depende de la efectiva demostración del daño, salvo hipótesis de daño presumido. En este último caso, entendemos que no todo daño deberá ser presumido, siendo fundamental el análisis casuístico de la situación fáctica.

En lo que atañe a la tutela colectiva, los instrumentos principales del proceso colectivo como el transporte *in utilibus* de la cosa juzgada colectiva, el inquérito civil, el término de ajuste de conducta, entre otros, disciplinan y crean un microsistema de tutela de colectiva de protección de datos personales formado por la LGPD, la Ley de Acción Civil Pública y el Código de Defensa del Consumidor. En esta senda, la protección de datos personales se desvincula del enfoque exclusivamente individualista de los daños a la privacidad y a la autodeterminación informativa para adoptar, también, la protección colectiva.

Con relación a los derechos de la personalidad de índole difusa que son resguardados por la LGPD en lo que atañe a la privacidad, libertad, honra y autodeterminación, su violación puede generar resarcimiento no sólo de orden material (patrimonial) como también moral e inmaterial.

Por último, la complejidad, principal característica del ambiente virtual, crea la hiper vulnerabilidad técnica, fáctica e informacional de los consumidores. Frente a estas fragilidades es fundamental crear mecanismos de compensación al consumidor que le permitan conocimiento claro y objetivo para adherir o adoptar comportamientos de forma segura.

En el caso de que ocurra incumplimiento de estas reglas, surgirá responsabilización civil y administrativa por prácticas anticompetitivas. Con respecto a los principios de la lesividad, de la fragmentariedad y de la intervención mínima

---

a preservar por disposición expresa en ley. Si el autor es funcionario público, le será aplicada, cumulativamente, la penalidad especial de inhabilitación de uno a cuatro años" (Traducción nuestra).

que rigen el Derecho Penal, no siendo suficiente la protección de datos en las esferas civil y administrativa, es necesaria y legítima la tutela penal de la privacidad y de datos personales, en el medio *off-line* y en el ambiente digital.

BIBLIOGRAFÍA

BIONI, B. R. *Proteção de Dados Pessoais: a função e os limites do consentimento*, 2 ed, Ed. Forense, Rio de Janeiro, 2020.

CANOTILHO, JJ. *Direito Constitucional e Teoria da Constituição*, 7ª ed, Almedina, Coimbra, 2003.

CARVALHO NETO, I. *Manual de Processo Coletivo*, Juruá, Curitiba, 2008.

CRUZ, A; RIBEIRO, C.A; TEIXEIRA, J.P. F; BAÑOS, J; MIRANDA, L.A; COTS, M; AZEVEDO, R; OLIVEIRA, R. "O Legítimo Interesse e a LGPD", (Oliveira, R; Cots, M. coords.), Thomson Reuters, São Paulo, 2020.

DPDC, de la Secretaría de Derecho Económico, del Ministerio de Justicia, nota número 40/CGEMM/DPDC/SENACON/2013. Disponible en: https://www.justica.gov.br/seus-direitos/consumidor/notas-tecnicas/anexos/40-2013.pdf. Acceso el 19.04.2020.

FUX, L. WAMBIER, T. A. A. NERY JR, N. *Processo e Constituição. Estudos em homenagem ao Professor José Carlos Barbosa Moreira*, Revista dos Tribunais, São Paulo, 2006.

GOMES, R. B. O; SILVA, M. S. L. "O Enquadramento Jurídico Penal do 'Phishing" e Suas Repercussões no Furto Informático". En: *Letras Jurídicas*, Centro Universitário Newton Paiva, n. 3, 2/2014.

MAYER-SCONBERGER, V. *General development of data protection in Europe*, En: *Tecnology and privacy: The new landscape*. (AGRE, P; ROTENBERG, M. coord.), MIT Press, Cambridge, 1997.

MAZZILI, H. N. *A defesa dos interesses difusos em juízo*, 31ª ed, Saraiva, São Paulo, 2018.

Ministerio de Justicia. Nota técnica número 32/2019/CGCTSA/DPDC/SENACON/MJ. Proceso 08012.000723/2018-19. Disponible en: https://www.justica.gov.br/Acesso/sistema-eletronico-de-informacoes-sei. Acceso el 19.04.2020.

Ministerio de Justicia. Nota Técnica número 92/2018/CSA-SENACON/CGCTSA/GAB-DPDC/DPDC/SENACON/MJ. Disponible en: https://www.cmlagoasanta.mg.gov.br/abrir_arquivo.aspx/PRATICAS_ABUSIVAS_DECOLARCOM?cdLocal=2&arquivo=%7BBCA8E2AD-DBCA-866A-C8AA-BDC2BDEC3DAD%7D.pdf. Acceso: 19.04.2020.

Ministerio Público Distrito Federal y Territorios. Disponible: https://www.mpdft.mp.br/portal/pdf/noticias/dezembro_2018/ACP_-_Banco_Inter.pdf. Acceso el 02/06/2020.

Ministerio Público Distrito Federal y Territorios. Disponible: https://www.mpdft.mp.br/portal/pdf/noticias/dezembro_2018/Ata_de_Audi%C3%AAncia_Banco_Inter.pdf. Acesso el 02/06/2020.

OPICE BLUM, R. NÓBREGA MALDONADO, V. *LGPD – Lei Geral de Proteção de Dados Comentada*, 2ª edição, Revista dos Tribunais, São Paulo, 2019.

RIOS, J. O. "A defesa do consumidor e a imprensa". En: MORATO, A. C. NERI, P. T. *Vinte anos do Código de Defesa do Consumidor. Estudos em Homenagem ao Professor José Geraldo Brito Filomeno*, Atlas, São Paulo, 2010.

RODOTÀ, S. *A vida na sociedade de vigilância: a privacidade hoje*, Ed. Renovar, Rio de Janeiro, 2008.

SOLOVE, D. J. "Access and Aggregation: Public Records, Privacy and the Constitution". En: *Minnesota Law Review*, v. 86, 2002, p. 1138-1217. Disponible: https://scholarship.law.umn.edu/mlr/1094. Acceso el: 19/04/2020.

VIGLIAR, J. M. M. *Ação Civil Pública*, Atlas, São Paulo, 2001.