Miqueias Micheletti
Túlio Tito Borges

LGPD

O Abismo entre a Teoria e a Prática

Prefácio
Cristina Cabral

Lei Comentada

1º Edição

Lei Geral de Proteção de Dados

O abismo entre a teoria e a prática

1ª Edição

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Micheletti, Miquéias
LGPD [livro eletrônico] : o abismo entre a teoria e a prática : comentada, artigo por artigo / Miquéias Micheletti, Túlio Tito Borges. -- 1. ed. -- Paulínia, SP : Ed. do Autor, 2021.
MOBI

Bibliografia
ISBN 978-65-00-17670-4

1. Direito 2. Direito à privacidade 3. Proteção de dados - Leis e legislação I. Borges, Túlio Tito. II. Título.

21-57253 CDU-342.721(094.56)

Índices para catálogo sistemático:

1. Lei geral de proteção de dados : Comentários : Direito à privacidade 342.721(094.56)

Aline Graziele Benitez - Bibliotecária - CRB-1/3129

Título: LGPD - O Abismo entre a Teoria e a Prática

Publicado no Brasil

Sumário

PREFÁCIO

Em uma sociedade que experimenta, cada vez mais, profundas e aceleradas transformações, sobretudo digitais, no Brasil surge a Lei 13.709/2018 – a LGPD, cujo objetivo principal é criar um âmbito legal de proteção para a privacidade e para os dados pessoais dos seus indivíduos.

De fato, nos últimos anos, viu-se um aumento exponencial do fluxo de transações com dados pessoais, o que acabou por criar ramos de negócios inteiramente novos e aumentar a eficiência de diversos setores da economia, como, por exemplo, os aplicativos de transporte ou de monitoramento da saúde.

Neste diapasão, a LGPD impacta todas as áreas da sociedade, e sua promulgação visa proporcionar uma maior estabilidade e segurança jurídica para os diversos ramos de negócios existentes e que deverão surgir nos próximos anos, derivados desta transformação digital, sem precedentes.

Como já se esperava, é uma legislação que tem um imenso impacto econômico, social e regulatório, e cuja implementação nas empresas e órgãos públicos não se trata de uma tarefa simples, considerando a novidade que este tema representa em solo brasileiro.

Logo, a LGPD deve tornar um imperativo a mudança no modelo de tratamento de dados pessoais, especialmente em um momento de profunda transformação digital, que acabou por ser acelerada pela atual situação pandêmica, fazendo com que a observação da proteção dos dados pessoais seja ainda mais necessária.

Tecidas estas considerações, os autores buscaram, no presente livro, fornecer uma visão geral de todos os dispositivos da Lei, com todas as suas minúcias e aspectos controversos, a fim de orientar melhor a sua aplicação prática além dos aspectos mais doutrinários e puramente teóricos.

Este aspecto prático pode ser verificado no decorrer da leitura do livro e, a título de curiosidade, nas partes finais deste material, são abordadas e comentadas algumas situações reais que, embora tenham ocorrido em momento anterior à aprovação da Lei, estão diretamente relacionadas com a segurança dos dados dos indivíduos, o que demonstra como este quadro normativo se fazia realmente necessário ao ordenamento jurídico brasileiro.

Portanto, desejo meus sinceros votos e que a leitura do presente livro agregue conhecimento em torno deste importante marco legislativo para além dos seus aspectos puramente teóricos, possibilitando que o leitor também entre em contato com os aspectos práticos da proteção de dados pessoais e da segurança da informação.

Cristina Cabral.

APRESENTAÇÃO

A cada ano, a humanidade vem gerando e acumulando uma quantidade crescente de dados e informações. Tecnologias como *smartphones*, redes móveis de *internet*, Wi-Fi, a *internet* das coisas (IoT), o uso de *Big Data* e algoritmos de inteligência artificial se espalharam ao redor do mundo, transformando radicalmente a economia, a cultura e a política em todo o planeta.

A utilização de dados pessoais vem avançando sobremaneira, ao passo que, através da utilização de algoritmos, é possível que uma empresa conheça o perfil exato de consumo de uma pessoa, o que pode proporcionar amplas vantagens competitivas sobre os seus concorrentes. A título exemplificativo, é possível que um determinado partido político identifique de forma detalhada todas as questões comportamentais de um eleitor, podendo criar perfis e, assim, possibilitar ganhos eleitorais expressivos.

Nessa toada, em uma era cujo motor da economia é a informação, a transformação digital na indústria vem em uma crescente, provocando um impacto considerável nos hábitos de consumo, que vão de microempréstimos na África Subsaariana, possibilitados por *fintechs*, a testes de carros autônomos na Califórnia, capitaneados por empresas como a Tesla e o Google.

Sob essa ótica, a consultoria IDC[1] já estimava que apenas no ano de 2020, 59 *zettabytes* (ZB) de dados seriam criados, capturados, consumidos ou copiados, com um crescimento estimado de 26% por ano até 2025. Isso corresponde a uma quantidade maior de dados do que aquela gerada por toda a humanidade, em toda a sua história, até o ano de 2010. E essa tendência está cada vez mais acelerada, tendo em vista que apenas a *internet* das coisas (IoT) deverá movimentar 80 *zettabytes* de dados em 2025[2].

Se comparadas as 10 empresas mais valiosas do mundo em 2010 e em 2020, é nítido que os dados tomaram o lugar do petróleo, como o produto mais valioso e cobiçado do planeta. Empresas como a Alphabet, Apple, Amazon e Facebook tomaram o lugar de gigantes do setor energético, como a ExxonMobil, BP e Shell.

Para se ter uma ideia da velocidade dessas mudanças, no ano de 2010 os *smartphones*, tão presentes no dia a dia das pessoas, eram considerados aparelhos eletrônicos de nicho para o ramo empresarial, e empresas hoje dominantes no mercado de consumo digital, como o Spotify, a Netflix, o Airbnb e a Uber ainda estavam dando seus primeiros passos na criação de novos modelos de negócio.

---

[1] IDC's Global DataSphere Forecast Shows Continued Steady Growth in the Creation and Consumption of Data. **IDC**, 2020. Disponível em: https://www.idc.com/getdoc.jsp?containerId=prUS46286020. Acesso em 13/11/2020.

[2] KANELLOS, Michael. 152,000 Smart Devices Every Minute In 2025: IDC Outlines The Future of Smart Things. **Forbes**, 2016. Disponível em https://www.forbes.com/sites/michaelkanellos/2016/03/03/152000-smart-devices-every-minute-in-2025-idc-outlines-the-future-of-smart-things/?sh=281bb41d4b63. Acesso em 13/11/2020.

A verdade é que o mundo assiste ao advento de uma extensão tecnológica do corpo humano, ou seja, se antes este era formado por cabeça, corpo e membros, hoje conta com mais um agregado, o *smartphone*[3].

Destarte, as pessoas estão cada vez mais reféns de seus celulares, vivendo conectadas 24 horas por dia e 7 dias por semana, de sorte que, uma vez desconectadas, experimentam uma triste condição de tortura. Assim, no afã de estarem antenadas, acabam por não se importar com qualquer espécie de monitoramento e sequer dão atenção aos reflexos de terem suas vidas espionadas.

Em vista disso, o efeito deste monitoramento ostensivo reflete os escândalos a que o mundo assistiu na última década. É o que se pode ver em casos relacionados com o uso abusivo de dados e com a invasão de privacidade, como nos escândalos da NSA, em 2013, e da Cambridge Analytica, em 2016, eventos paradigmáticos e que jogaram luz à necessidade de maior regulamentação nos ambientes digitais.

Posto isto, se de um lado a obtenção e manipulação de dados é algo estratégico para o mercado, possibilitando, inclusive, a criação de modelos de negócio disruptivos e que podem se tornar bastante lucrativos, por outro também é necessário sopesar as consequências negativas que podem advir do avanço dessa transformação digital.

[3] HARARI, Yuval Noah. **Homo Deus.** São Paulo: Companhia das Letras, 2016. p. 337.

Assim, esse ambiente digital cada vez mais integrado com a vida real, somado a esses escândalos envolvendo vazamento de dados, traduzem os riscos relacionados à segurança da informação que vêm crescendo de maneira exponencial.

Nessa toada, a Lei nº 13.709/18 - Lei Geral de Proteção de Dados Pessoais, mais conhecida como LGPD, foi concebida visando proteger os direitos à privacidade dos cidadãos e de seus dados pessoais, em um ambiente de rápida evolução tecnológica.

Sobre os autores, Miquéias Micheletti é empresário, graduado em Administração de Empresas pela Fundação Armando Alvares Penteado – FAAP, analista de segurança da informação há 19 anos, com vasta experiência em processamento de dados. É proprietário da EMBRASI (embrasi.com.br) e foi responsável por diversos projetos, dentre eles o processamento de dados de todo o plano econômico (Bresser, Verão, Collor I e Collor II) de um dos maiores banco no Brasil.

Já Túlio Borges é advogado formado pela Universidade Estadual Paulista "Júlio de Mesquita Filho" (Unesp) e pós-graduando em Direito Digital e *Compliance* pelo Instituto Brasileiro de Mercado de Capitais (Ibmec).

Nesse sentido, este livro visa analisar os pontos mais importantes desta legislação que tem gerado diversas dúvidas e indagações. Em linhas gerais, o objetivo é oferecer uma espécie de interpretação prática da legislação para todos os líderes, empresários, e

demais *stakeholders*, apresentando exemplos de medidas para adequação com a temática da proteção de dados pessoais e também alguns estudos de caso.

Para melhor compreensão, este livro, tal como a LGPD, é dividido em 10 capítulos, que abordam de forma simplificada e sem delongas os marcos principais da legislação, oferecendo *insights* de como as empresas poderão se adequar com as boas práticas de governança, não só relacionados à proteção de dados pessoais, como também à segurança da informação como um todo, principalmente no tocante aos padrões relativos à ISO 27001 e à legislação de proteção de dados pessoais europeia, também conhecida como RGPD (Regulamento Geral de Proteção de Dados).

CAPÍTULO I – DISPOSIÇÕES PRELIMINARES

Art. 1º - Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.

1. Histórico da Lei Geral de Proteção de Dados no Brasil

Antes de começar a tecer as devidas considerações sobre a LGPD, faz-se necessário narrar um breve histórico sobre a sua aprovação no Brasil.

No âmbito da OCDE, que é composta pelos países mais desenvolvidos, a proteção de dados pessoais ganhou um aspecto maior de discussão a partir da década de 70, com a promulgação da primeira lei sobre o tema no estado de Hesse, na Alemanha Ocidental. Entretanto, no Brasil, as tratativas para a promulgação de uma legislação abrangente de proteção de dados só começaram a partir de

2010, com a abertura, pelo Ministério da Justiça, da primeira consulta pública do Anteprojeto de Lei (APL) de Proteção de Dados Pessoais[4].

Este APL foi protocolado na Câmara dos Deputados como PL 5.276/2016, de autoria do Poder Executivo, e foi posteriormente apensado ao PL 4.060/12 na data de 18 de julho de 2016. Já em outubro de 2016[5], foi formada uma Comissão Especial para analisar estes projetos de lei sobre proteção de dados pessoais na Câmara, que realizou ao todo 11 (onze) audiências públicas e um seminário internacional. Estas tratativas na Câmara também foram acompanhadas por discussões no Senado, até que, no dia 14 de agosto de 2018, foi promulgada a LGPD pelo então Presidente Michel Temer.

2. Diretrizes básicas

O art. 1º da LGPD estabelece as diretrizes básicas da legislação de proteção de dados pessoais, definindo o âmbito de aplicação, a quem se destina e o que visa proteger.

Primeiramente, é importante ressaltar que a Lei se aplica a todas as operações com dados, sejam elas realizadas por meios físicos

[4] DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (orgs). **Tratado de Proteção de Dados Pessoais**. 1º ed. Rio de Janeiro: Forense, 2021. pp. 16-17.

[5] BIONI, Bruno Ricardo. De 2010 a 2018: a discussão brasileira sobre uma lei geral de proteção de dados. **Jota**, 2018. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378. Acesso em: 30/12/2020.

(arquivos e documentos em papel) ou por meios eletrônicos (bases de dados em ativos informáticos).

A LGPD também se aplica a todas as operações com dados realizadas por quaisquer pessoas físicas ou jurídicas, sejam empresas privadas ou órgãos públicos, e possui a finalidade de proteger a liberdade, a privacidade e os demais direitos fundamentais dos indivíduos em sociedade.

As disposições contidas na LGPD visam elevar o ordenamento jurídico brasileiro ao nível de proteção de dados pessoais visto nos países desenvolvidos, especialmente ao nível de proteção de dados visto nos países europeus com o RGPD[6]. Isso porque houve o efetivo reconhecimento legal da posição de vulnerabilidade dos indivíduos frente às empresas e governos que se utilizam de seus dados pessoais para os mais variados fins, equilibrando essa relação jurídica[7].

Inclusive, é possível comparar o impacto desta legislação no ordenamento jurídico do país à promulgação da Consolidação das Leis do Trabalho (CLT) na década de 40 ou do Código de Defesa do Consumidor (CDC) na década de 90, que também surgiram para equilibrar relações díspares entre as corporações e os indivíduos,

[6] DÖHMANN, Indra Spiecker Gen. A proteção de Dados Pessoais sob o Regulamento Geral de Proteção de Dados na União Europeia. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (orgs). **Tratado de Proteção de Dados Pessoais**. 1º ed. Rio de Janeiro: Forense, 2021. pp. 97-98.

[7] COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais** – Comentada. 3º ed. São Paulo, Revista dos Tribunais, 2019. pp. 48-49.

conferindo-lhes uma maior proteção legal nas relações de trabalho e nas relações de consumo, respectivamente.

3. Competência

Já o parágrafo único do art. 1º deixa claro que a legislação é de suma importância para o interesse nacional e que deve ser aplicada a todos os entes da federação, entretanto, não prevê a qual ente federativo compete legislar acerca da proteção de dados pessoais.

Portanto, ao menos teoricamente, um Estado ou Município poderia legislar de forma supletiva acerca do tratamento de dados pessoais, dando ensejo à criação de complicações ainda maiores para a adequação à legislação por empresas e agentes públicos.

Para tentar sanar esta questão, já tramita no Congresso Nacional a Proposta de Emenda à Constituição (PEC) nº 17/2019, que transfere à União a competência privativa de legislar acerca das questões tratadas na LGPD, conferindo assim uma maior segurança jurídica ao tema[8].

[8] A referida PEC já foi aprovada na Comissão de Constituição e Justiça da Câmara dos Deputados, e aguarda a pauta em Plenário. Informação disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757>. Acesso em: 29/01/2021.

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

I - o respeito à privacidade;

II - a autodeterminação informativa;

III - a liberdade de expressão, de informação, de comunicação e de opinião;

IV - a inviolabilidade da intimidade, da honra e da imagem;

V - o desenvolvimento econômico e tecnológico e a inovação;

VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

1. Fundamentos da LGPD

O art. 2º da LGPD lista os fundamentos da proteção de dados pessoais no ordenamento jurídico brasileiro. Diferentemente dos objetivos contidos no art. 1º, que se referem a algo exterior a ser

perseguido pela legislação[9], os fundamentos criam a base estrutural sobre a qual se forma um sistema legal. Nesse sentido, segundo Comparato[10], o fundamento de algo é a designação do "que serve de base ao ser, ao conhecer, ou ao decidir. Fundamento é, pois, a causa ou razão de algo (*ratio essenci, ratio cognoscendi, ratio decidendi*)".

2. Privacidade

Na visão jurídica brasileira tradicional, a privacidade se insere no espaço existente entre o que é considerado público e o que é considerado privado e, em razão disto, a sua definição depende da averiguação do momento histórico e do contexto social em que a discussão está inserida.

De forma geral, a privacidade constituiria uma liberdade negativa, ou seja, um "direito estático à espera de que seu titular delimite quais fatos da sua vida deveriam ser excluídos do domínio público"[11]. Logo, o cidadão teria o direito e a liberdade de estabelecer quais aspectos de sua vida poderiam ser conhecidos, sendo vedada a interferência de terceiros.

Tal liberdade encontra ampla ressonância no ordenamento jurídico, seja pelo art. 12 da Declaração Universal dos Direitos

[9] BASTOS, Celso Ribeiro. **Curso de direito constitucional**. São Paulo: Saraiva, 2021. pp. 159-160.
[10] COMPARATO, Fábio Konder. **Rumo à justiça**. São Paulo: Saraiva, 2010. p.41.
[11] BIONI. Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2020. p. 118.

Humanos[12], seja pelo inciso X do art. 5º da Constituição Federal[13] ou pelo art. 21 do Código Civil[14], estabelecendo-se o trinômio "pessoa-informação-sigilo", devendo qualquer cidadão se abster de adentrar a vida privada de outro cidadão[15].

Entretanto, na era da informação, o termo "privacidade" ganha uma concepção de liberdade positiva, como uma espécie de proteção dinâmica em relação ao fluxo de informações pessoais disponíveis nos meios tecnológicos, tendo em vista que o próprio acesso a produtos e serviços muitas vezes está condicionado ao fornecimento de dados pessoais. Há, pois, uma mudança de paradigmas no trinômio supramencionado, que se transforma em um quadrinômio "pessoa-informação-circulação-controle", ou seja, a conduta relativa à privacidade deixa de ser passiva - de um mero sigilo do cidadão frente

---

[12] ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Declaração Universal dos Direitos Humanos**, 1949. Artigo 12°: Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei.

[13] BRASIL. **Constituição da República Federativa do Brasil**, 1988. Art. 5º: Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação

[14] Idem. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Art. 21: A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

[15] SARLET, Ingo Wolfgang. Fundamentos Constitucionais: O Direito Fundamental à Proteção de Dados. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (orgs). **Tratado de Proteção de Dados Pessoais**. 1º ed. Rio de Janeiro: Forense, 2021. p. 23.

a coletividade - para se tornar uma conduta ativa - de controle da circulação dos dados plenamente disponíveis na esfera pública.

Assim, a liberdade relacionada com a privacidade deixa de ser negativa para se tornar positiva, ou seja, é o indivíduo quem determina e controla a circulação das suas informações pessoais, o que acaba por afastar o conceito de privacidade como direito inserido entre o público e o privado, tendo em vista que todas as informações anteriormente consideradas pessoais e privadas passam a ser potencialmente públicas.

3. O direito de autodeterminação informativa

Tendo em vista o quadrinômio supramencionado, a autodeterminação informativa se revela como um direito autônomo, oriundo de um desdobramento do direito à privacidade. Este direito surge através da necessidade de criação de mecanismos que permitam aos indivíduos controlar a limitação da circulação de seus dados, considerando o aumento exponencial da utilização de tecnologias que se baseiam na coleta e processamento de dados pessoais.

A experiência com governos autoritários de toda ordem fez com que a tradição jurídica europeia estivesse sempre atenta à preservação da dignidade da pessoa humana, inclusive no que diz respeito à utilização de dados pessoais[16].

[16] SARLET, Ingo Wolfgang. Fundamentos Constitucionais: O Direito Fundamental à Proteção de Dados. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (orgs). **Tratado de Proteção de Dados Pessoais**. 1º ed. Rio de Janeiro: Forense, 2021. p. 30.

Nessa toada, é interessante notar um julgado paradigmático do Tribunal Constitucional Alemão da década de 70, considerando inconstitucional parte do censo demográfico do país, por ser considerado muito invasivo e representar um grande risco aos cidadãos caso caísse em mãos erradas[17].

A importância da autodeterminação informativa pode ser verificada em um extrato do julgado do tribunal germânico: "aquele que, com segurança suficiente, não pode vislumbrar quais informações pessoais a si relacionadas existem em áreas determinadas de seu meio social, e aquele que não pode estimar em certa medida qual o conhecimento que um possível interlocutor tenha da sua pessoa, pode ter sua liberdade consideravelmente tolhida"[18].

Os direitos dos titulares de dados contidos no Capítulo III da LGPD dizem respeito especialmente a essa liberdade positiva do indivíduo, de efetivamente possuir acesso e controle sobre todas as suas informações, com o intuito de propiciar mais segurança a este indivíduo.

Não obstante, a efetivação destes direitos pode não parecer tão efetiva, especialmente frente à crescente demanda, pelos diversos

---

[17] MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia. **Direito, inovação e tecnologia**. São Paulo: Saraiva, 2015. v. 1. p.205.

[18] MENDES, Laura Schertel. Autodeterminação informacional: origem e desenvolvimento conceitual na jurisprudência da corte constitucional alemã. In: VILLAS BÔAS CUEVA, Ricardo, DONEDA, Danilo, MENDES, Laura Schertel (Org.). **Lei Geral de Proteção de Dados (Lei nº 13.709/2018)** - A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters, 2020, p. 177-178.

aplicativos e *websites* acessados no dia a dia, da leitura de extensas políticas de privacidade e termos de uso.

A título de exemplificação, um estudo acadêmico da Universidade Carnegie Mellon já demonstrou que um usuário precisaria, em média, de 201 horas por ano para ler todos os termos de uso dos *websites* que acessa, o que equivaleria, à data do estudo, à quantia de U$3.354[19].

4. Liberdade de expressão

A liberdade de expressão é considerada um marco importante do pensamento liberal que se estabeleceu desde o século XVIII nas sociedades ocidentais. Entretanto, apesar de estar positivada no art. 5º, incisos IV e IX da Constituição Federal[20], não perfaz um direito absoluto.

A inserção da liberdade de expressão como um fundamento da proteção de dados pessoais busca oferecer ao julgador a possibilidade de sopesar o direito de privacidade e o direito de se expressar

[19] MCDONALD, Alecia M.; CRANOR, Lorrie Faith. The Cost of Reading Privacy Policies. **Journal of Law and Policy for information Society**, 2008 v.4, p. 565: "We estimate that Reading privacy policies carries costs in time of approximately 201 hours a year, worth about $3,354 annually per American Internet user".

[20] BRASIL. **Constituição da República Federativa do Brasil**, 1988. Art. 5º: Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
IV - é livre a manifestação do pensamento, sendo vedado o anonimato;
IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;

livremente, vide o julgado a seguir da Corte Interamericana de Direitos Humanos[21], declarando que:

> A justiça deve encontrar um balanço entre a vida privada e a liberdade de expressão que, não sendo absolutos, são dois direitos fundamentais garantidos pela Convenção Americana e são de grande importância em uma sociedade democrática. A Corte recorda que todo direito fundamental deve ser exercido em relação a outros direitos fundamentais. Esse é um processo de harmonização no qual o Estado tem papel chave na tentativa de determinar as responsabilidades e a imposição de sanções que possam ser necessárias para atingir tal propósito.

De fato, com a fusão dos espaços públicos e privados, na era da informação, através do crescente uso de redes sociais, a proteção da liberdade de expressão acaba por se tornar mais complexa, tendo em vista que não só as manifestações puras de pensamento devem ser protegidas, mas também qualquer externalização de gostos, interesses e características do ser humano realizados através das redes sociais[22].

As redes sociais tomaram o lugar de realização do debate público, anteriormente protagonizado pela mídia tradicional, o que tornou os processos informacionais muito mais fluídos e potencialmente nocivos, tendo em vista que as informações pessoais

---

[21] ORGANIZAÇÃO DOS ESTADOS AMERICANOS (OEA). Corte Interamericana de Direitos Humanos. **Caso de Fontevecchia and D'amico v. Argentina**, julgado em 29.11.2011. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_238_por.pdf. Acesso em: 27/01/2020.

[22] BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 1.010.606 RJ**. Direito Civil. Responsabilidade Civil. Indenização por Dano Material. Direito de Imagem. Relator: Ministro Dias Toffoli. Disponível em: <http://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=5091603>. Acesso em: 28/01/2021.

podem facilmente fugir do controle do titular e ficar eternamente disponíveis em ferramentas de buscas e redes sociais, atentando contra a dignidade básica do ser humano.

De forma anterior à LGPD, o STF, no âmbito do julgamento do caso Aída Curi, vem discutindo o direito dos indivíduos de serem efetivamente esquecidos, ou seja, que seus dados sejam retirados da esfera de discussão pública. Neste caso, que está pendente de julgamento, estão envolvidos dados veiculados através de um programa televisivo veiculado pela Rede Globo, sobre um caso de assassinato ocorrido na década de 50. Devido ao longo período passado desde o crime, pretende a parte autora o direito de "esquecimento" frente a emissora, em conjunto com uma indenização por danos morais[23].

Na experiência internacional, entretanto, as ações deste tipo levam em conta a separação entre a produção e a difusão do conteúdo, como o caso europeu de Mario Costeja González vs. Google Spain, em que houve uma distinção entre o meio que produziu o conteúdo (um jornal) e quem o difundiu (um sistema de busca)[24]. O certo é que a

[23] MOREIRA, Rodrigo Pereira; MEDEIROS, Jaqueline Souza. Direito ao Esquecimento: Entre a Sociedade da Informação e a Civilização do Espetáculo. In: **Revista de Direito Privado**, vol. 70, ano 17. São Paulo: RT, 2016. p. 72.

[24] "[...] Não se discute que entre os dados encontrados, indexados e armazenados pelos motores de busca e postos à disposição dos seus utilizadores figuram também informações sobre pessoas singulares identificadas ou identificáveis e, portanto, 'dados pessoais' na acepção do artigo 2.°, alínea a), da referida diretiva. [...] ao explorar a Internet de forma automatizada, constante e sistemática, na busca das informações nela publicadas, o operador de um motor de busca 'recolhe' esses dados, que 'recupera', 'registra' e 'organiza' posteriormente no âmbito dos seus programas de indexação, 'conserva' nos seus servidores e, se for caso disso, 'comunica' e 'coloca à disposição' dos seus utilizadores, sob a forma de listas de resultados das suas

temática do "direito ao esquecimento" deve ganhar maior relevância com a vigência da LGPD e a necessidade de sopesamento dos direitos dos titulares de dados[25].

5. Proteção da intimidade, da honra e da imagem

Segundo o art. 11 do Código Civil, a intimidade, a honra e a imagem são consideradas aspectos irrenunciáveis e intransmissíveis da personalidade. Portanto, neste inciso, a LGPD procurou se adequar à doutrina civilista da dignidade da pessoa humana, buscando proteger todos os aspectos da personalidade contra quaisquer invasões.

---

pesquisas". Logo, concluiu a Corte que: "[...] "é o operador do motor de busca que determina as finalidades e os meios dessa atividade e, deste modo, do tratamento de dados pessoais que ele próprio efetua no contexto dessa atividade e que deve, consequentemente, ser considerado 'responsável' por esse tratamento por força do referido artigo 2.°, alínea d)". UNIÃO EUROPEIA. **Corte de Justiça da União Europeia**. ACÓRDÃO DO TRIBUNAL DE JUSTIÇA (Grande Secção), 13 de maio de 2014 (*). Dados pessoais — Proteção das pessoas singulares no que diz respeito ao tratamento desses dados — Diretiva 95/46/CE — Artigos 2º, 4º, 12º e 14º — Âmbito de aplicação material e territorial — Motores de busca na Internet — Tratamento de dados contidos em sítios web — Pesquisa, indexação e armazenamento desses dados — Responsabilidade do operador do motor de busca — Estabelecimento no território de um Estado-Membro — Alcance das obrigações desse operador e dos direitos da pessoa em causa — Carta dos Direitos Fundamentais da União Europeia — Artigos 7º. e 8º. Disponível em: < https://www.conjur.com.br/2014-mai-21/direito-apagar-dados-decisao-tribunal-europeu-google-espanha#:~:text=Inconformadas%20com%20a%20decis%C3%A3o%20da,Spain%20e%20a%20Google%20Inc.&text=Mario%20Costeja%20Gonz%C3%A1lez%20teve%2C%20ent%C3%A3o,13%20de%20maio%20de%202014.>. Acesso em: 29/01/2021.

[25] SILVA, Jennifer Gomes da. Direito ao esquecimento: a bola agora está com o Supremo Tribunal Federal. **Conjur**, 2020. Disponível em: <https://www.conjur.com.br/2020-set-30/jeniffer-gomes-direito-esquecimento-pauta>. Acesso em 29/01/2021.

Da mesma forma dispõe o Código Civil em seu art. 20, ao aduzir que a divulgação da escrita, da fala ou da imagem de um determinado indivíduo poderão ser condutas por ele proibidas, a seu requerimento e inclusive com a possibilidade de indenização, se forem atingidas a honra, a boa fama ou a respeitabilidade desse indivíduo, ou se forem utilizados seus dados para fins comerciais.

Este fundamento torna-se especialmente importante com o crescimento da chamada *internet* das coisas (IoT), em que serão coletados cada vez mais dados acerca de todos os aspectos da vida dos indivíduos em sociedade. Fala, imagem, dados biométricos, tudo isso será processado e utilizado para entregar produtos inovadores que, ao mesmo tempo em que trarão muitos benefícios, como a detecção precoce de um câncer através de dados biométricos, possivelmente trarão malefícios ao indivíduo, como o aumento do preço de um seguro de vida ou de saúde[26], dentre outras consequências imprevistas.

6. Desenvolvimento econômico

O fato de a LGPD se fundamentar no desenvolvimento econômico está intimamente ligado à própria existência da "*data driven economy*", ou "economia guiada por dados".

É crucial para o avanço da economia do país a adequação da legislação às necessidades de desenvolvimento, devendo a regulação

[26] HARARI. Yuval Noah. **21 lições para o século 21**. São Paulo: Companhia das Letras. 2018. p. 23.

ser utilizada estrategicamente para fomentar o crescimento econômico e a inovação[27].

Neste contexto, foi instituída pelo Governo Federal, através do Decreto nº 9.319/18, a "Estratégia Nacional para a Transformação Digital", que tem como objetivo a harmonização das políticas públicas da União acerca do uso de tecnologia para promover o desenvolvimento econômico e social sustentável e inclusivo, com inovação, aumento de competitividade, de produtividade e dos níveis de emprego e renda no País.

Destarte, a LGPD oferece segurança jurídica a este ambiente de inovação que atrai cada vez mais investimentos ao país, possibilitando que sejam criados e desenvolvidos novos serviços e produtos, utilizando tecnologia de ponta com um arcabouço normativo e regulatório estável.

7. Livre concorrência e direitos do consumidor

As questões acerca da defesa da concorrência têm tomado centralidade nas discussões sobre a privacidade e a proteção de dados pessoais, tendo em vista que a economia baseada em dados desafia a lógica tradicional da criação de monopólios. Isto porque a centralização de dados pessoais em um só agente permite que sejam criados

[27] VAINZOF, Rony. Capítulo I – Disposições Preliminares. MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). LGPD – Lei Geral de Proteção de Dados – Comentada. 2ª ed. São Paulo: Revista dos Tribunais, 2019. p. 38

algoritmos melhores e que atendam de maneira mais eficaz as necessidades do usuário, ao contrário do que ocorre com outros tipos de monopólios.

É o que acontece com as grandes empresas de tecnologia atualmente, como o Google e o Facebook, que detêm uma fatia gigantesca do mercado de buscas e de redes sociais, respectivamente, e deste modo conseguem oferecer produtos melhores e mais atrativos. Há inclusive uma série de investigações antitruste contra estas e outras empresas de tecnologia, diante de indícios de que teriam embarcado em uma série de práticas anticoncorrenciais e abusivas[28].

No âmbito do direito do consumidor, as questões relativas à privacidade e à proteção de dados pessoais já vêm tendo alguma atenção do legislador, como por exemplo a disposição do art. 43 do Código de Defesa do Consumidor[29], que regula a criação e a utilização de bancos de dados de consumidores, ou a Lei do Cadastro Positivo (Lei nº 12.414/11), que regulamenta a criação de perfis de crédito de consumidores.

Desta forma, este fundamento da LGPD é importante para guiar os futuros reguladores na perseguição do equilíbrio entre as

[28] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 2ª ed. Rio de Janeiro: Forense, 2018. pp.41-42.
[29] BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Art. 43: O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

práticas de mercado e a proteção da concorrência. Deve-se aguardar as articulações futuras que a ANPD deverá realizar com os órgãos setoriais de direito da concorrência e de direito do consumidor, como o Conselho Administrativo de Defesa Econômica (CADE) e a Secretaria Nacional do Consumidor (SENACON), e as demais agências reguladoras, como a Agência Nacional de Telecomunicações (ANATEL) e a Agência Nacional de Saúde Suplementar (ANS), o que deve moldar as futuras regulações sobre proteção de dados no país.

8. Princípio da dignidade da pessoa humana

O princípio da dignidade da pessoa humana é o ponto fundamental da teoria constitucional contemporânea. Deste modo, a influência crescente que o espaço digital vem tendo sobre a vida dos indivíduos em sociedade tem gerado diversas preocupações na temática da proteção dos direitos humanos.

Neste sentido, o Conselho de Direitos Humanos das Nações Unidas publicou disposições para a promoção, proteção e fruição dos direitos humanos no âmbito da *internet*, destacando que a privacidade do indivíduo é essencial para a efetivação dos direitos à liberdade de expressão, liberdade de opinião e liberdade de associação[30].

[30] ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Human Right Council**. Thirty-second session. Disponível em: <http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/32/L.20>. Acesso em 16.11.2020.

Como parte dos direitos de personalidade do indivíduo, a autodeterminação e controle sobre os próprios dados também foi inserida na Convenção 108 do Conselho da Europa em 2018, considerando a necessidade de garantir a dignidade da pessoa humana frente a diversificação, intensificação e globalização do processamento e fluxo de dados pessoais[31].

Pode-se dizer que este fundamento possui uma base normativa constitucional, tendo em vista que a proteção e o cuidado com as informações pessoais do indivíduo deixam de se relacionar apenas com as esferas do sigilo ou da privacidade, e passam a figurar como um componente essencial para determinar o grau de liberdade e capacidade de autodeterminação de cada pessoa[32].

De fato, nas lições de Harari, há uma clara preocupação com a ubiquidade cada vez maior dos dados no cotidiano dos seres humanos. Em um futuro próximo, ele cogita que podem surgir sistemas de crenças parecidos com religiões, uma das quais seria o "dataísmo" [33], na qual o Universo consistiria

> num fluxo de dados e o valor de qualquer fenômeno ou entidade seria determinado por sua contribuição ao

[31] CONSELHO DA EUROPA. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**. Disponível em [https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37]. Acesso em 16/11/2020.
[32] DONEDA, Danilo. Princípios e proteção de dados pessoais. In: LUCCA, Newon de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III**: Marco Civil da Internet. São Paulo: Quartier Latin, 2015. p. 370.
[33] HARARI, Yuval Noah. **Homo Deus.** São Paulo: Companhia das Letras, 2016. p. 370.

> processamento de dados. Desta forma, o avanço tecnológico de algoritmos de *Big Data* permitiria a criação de produtos e serviços cada vez melhores e mais customizados, capazes de adivinhar os gostos, hábitos e comportamentos das pessoas, e que poderiam influenciar sobremaneira os indivíduos, inclusive nas suas funções psicológicas e bioquímicas.

Na China, os dados pessoais já vêm sendo utilizados, desde 2014, em programas-piloto que instituem um sistema de "crédito social", no qual as ações dos cidadãos são medidas e controladas a todo o momento, com sanções que podem variar de multas à perda de direitos, o que na visão Ocidental se revela um flagrante desrespeito ao princípio da dignidade da pessoa humana[34].

[34] KOBIE, Nicole. The complicated truth about China's social credit system**. Wired**, 2019. Disponível em: <https://www.wired.co.uk/article/china-social-credit-system-explained>. Acesso em: 27/01/2021.

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

I - a operação de tratamento seja realizada no território nacional;

II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou

III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

Este artigo busca definir o âmbito de aplicação da legislação, seguindo os moldes da legislação europeia, e por isso deve ser considerado um dos mais importantes para fins de adequação à LGPD,

tendo em vista que estabelece uma ampla abrangência da Lei, com algumas exceções previstas no art. 4º.

Portanto, com base neste artigo, toda operação de tratamento de dados pessoais, seja em meio físico quanto em meio digital, realizada por pessoa física ou jurídica, de direito público ou privado, deve estar adequada à legislação, observadas as condições contidas nos incisos I, II e III deste artigo.

Assim, a primeira hipótese de tratamento diz respeito à territorialidade da aplicação da Lei, ou seja, importa o território de tratamento dos dados pessoais, e não a nacionalidade dos titulares. Desta forma, qualquer operação de dados realizada dentro do território nacional deverá estar adequada à legislação, mesmo que sejam tratados dados de pessoas de outros países[35].

A título de exemplificação, um aplicativo canadense de empréstimo de bicicletas para cidadãos da África do Sul, se realizar o tratamento destes dados em servidores localizados no Brasil, deverá estar adequado e em conformidade com a LGPD.

A segunda hipótese de tratamento diz respeito à extraterritorialidade da aplicação da Lei. Deste modo, qualquer oferta de serviço ou bem para indivíduos localizados no Brasil, mesmo que o

[35] VAINZOF, Rony. Capítulo I – Disposições Preliminares. In. MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). **LGPD** – Lei Geral de Proteção de Dados – Comentada. 2ª ed. São Paulo: Revista dos Tribunais, 2019. pp. 57-59.

tratamento seja realizado fora do país, deve observar a adequação do tratamento de dados pessoais à LGPD.

Na legislação europeia, muito se discute o escopo de definição do que constitui um serviço ou bem a uma pessoa localizada em determinado país, tendo em vista que as páginas de *internet* podem ser acessadas de qualquer país do mundo. Deste modo, para evitar que todas as empresas do mundo que ofereçam um serviço tenham que se adequar ao RGPD, os europeus elencaram algumas considerações para a avaliação do direcionamento de bens e serviços que deverão ser observadas a partir das seguintes condições:

(i) se o país é considerado como referência ao bem ou serviço oferecido;

(ii) se o controlador ou operador realiza o pagamento de ferramentas de busca para facilitar o acesso aos consumidores do país;

(iii) se existem campanhas de *marketing* e publicidade dirigidas aos consumidores do país;

(iv) se há menção de endereços ou números de telefone localizados no país;

(v) se há menção de clientes localizados no país;

(vi) se há a utilização da língua e moeda do país no *site*; e

(vii) se há a entrega de bens ou serviços no país[36].

Assim, caso a ANPD defina uma normativa similar a ser aplicada no Brasil, poderia se considerar que uma empresa paraguaia que aceita o pagamento em reais, possui *site* em versão e língua portuguesa e vende bens ou serviços a brasileiros teria que se adequar à LGPD, segundo o inciso II do art. 3º, mesmo que realize toda a operação de tratamento em solo paraguaio.

Já a terceira hipótese de tratamento, diz respeito aos dados coletados em território nacional, porém possui pouca relevância prática. Isso porque há uma interpolação com a hipótese de tratamento contida nos incisos anteriores. Se uma empresa coleta os dados e trata em

[36] UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Considerando n º 37: A fim de evitar que as pessoas singulares sejam privadas da proteção que lhes assiste por força do presente regulamento, o tratamento dos dados pessoais de titulares que se encontrem na União por um responsável pelo tratamento ou subcontratante não estabelecido na União deverá ser abrangido pelo presente regulamento se as atividades de tratamento estiverem relacionadas com a oferta de bens ou serviços a esses titulares, independentemente de estarem associadas a um pagamento. A fim de determinar se o responsável pelo tratamento ou subcontratante oferece ou não bens ou serviços aos titulares dos dados que se encontrem na União, há que determinar em que medida é evidente a sua intenção de oferecer serviços a titulares de dados num ou mais Estados-Membros da União. O mero facto de estar disponível na União um sítio web do responsável pelo tratamento ou subcontratante ou de um intermediário, um endereço eletrónico ou outro tipo de contactos, ou de ser utilizada uma língua de uso corrente no país terceiro em que o referido responsável está estabelecido, não é suficiente para determinar a intenção acima referida, mas há fatores, como a utilização de uma língua ou de uma moeda de uso corrente num ou mais Estados-Membros, com a possibilidade de encomendar bens ou serviços nessa outra língua, ou a referência a clientes ou utilizadores que se encontrem na União, que podem ser reveladores de que o responsável pelo tratamento tem a intenção de oferecer bens ou serviços a titulares de dados na União.

território nacional, existe interpolação com o inciso I. Se uma empresa coleta os dados no território nacional e os envia ao exterior para tratamento, é o caso da hipótese contida no inciso II. Assim, não é possível vislumbrar os casos em que a abrangência da Lei se daria a partir exclusivamente deste inciso III[37].

Importante ressaltar que o artigo 3º deixa claro que o critério utilizado é o da territorialidade, e não o da nacionalidade do indivíduo. Ou seja, busca-se proteger os dados pessoais de qualquer indivíduo localizado no Brasil, e não apenas dos cidadãos brasileiros.

[37] Neste sentido: VAINZOF, Rony. Capítulo I – Disposições Preliminares. In. MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). **LGPD** – Lei Geral de Proteção de Dados – Comentada. 2ª ed. São Paulo: Revista dos Tribunais, 2019. pp. 64-65; COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais** – Comentada. 3º ed. São Paulo, Revista dos Tribunais, 2019. p. 63.

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:

I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

II - realizado para fins exclusivamente:

a) jornalístico e artísticos; ou

b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;

III - realizado para fins exclusivos de:

a) segurança pública;

b) defesa nacional;

c) segurança do Estado; ou

d) atividades de investigação e repressão de infrações penais; ou

IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência

proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

§ 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.

§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.

§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público.

1. Hipóteses de exceção à LGPD

O art. 4º busca oferecer algumas exceções à aplicação da LGPD, com fundamento na razoabilidade e na necessidade de ponderação da aplicação da Lei com outros princípios fundamentais previstos no ordenamento jurídico.

A inexistência destas isenções certamente traria inúmeros transtornos para os particulares e para o Poder Público, tendo em vista todas as novidades trazidas pela Lei no campo da proteção de dados pessoais[38].

2. Tratamento para fins particulares

O inciso I do art. 4º determina a não incidência da LGPD para fins particulares e não econômicos de uma pessoa física, tais como listas, diários, fotos e anotações.

Apesar de parecer simples, este inciso pode gerar algumas controvérsias no que diz respeito à utilização de sistemas de vigilância no contexto de proteção e segurança de ambientes privados, por exemplo. Isso quer dizer que o indivíduo poderá se utilizar destes sistemas desde que respeite a finalidade não-econômica do seu tratamento, sob pena de ter que se adequar à LGPD.

[38] COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais** – Comentada. 3º ed. São Paulo, Revista dos Tribunais, 2019. p. 65.

3. Tratamento para fins jornalísticos

Assim como o inciso I, o inciso II do art. 4º busca sopesar a efetivação de outros direitos fundamentais frente à necessidade de proteção de dados pessoais.

Desta forma, em atendimento ao disposto no art. 220 da CF[39], buscou-se a efetivação da liberdade de imprensa e de manifestações artísticas.

Contudo, qualquer agente que pretender se utilizar desta isenção deverá estar atento à documentação das suas motivações para o enquadramento nesta isenção, vez que o jornalismo é atividade intimamente atrelada ao interesse público, que deverá ser demonstrado nestes casos.

Portanto, ainda que possuam esta isenção do art. 4º, os veículos de imprensa ainda terão que se adequar minimamente à LGPD para demonstrar que estão agindo de boa fé e com a devida transparência na utilização de todos os dados pessoais que eventualmente tratarem[40].

[39] BRASIL. **Constituição da República Federativa do Brasil**, 1988. Art. 220: A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição.

[40] VAINZOF, Rony. Capítulo I – Disposições Preliminares. In. MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). **LGPD** – Lei Geral de Proteção de Dados – Comentada. 2ª ed. São Paulo: Revista dos Tribunais, 2019. p. 70.

4. Tratamento para fins acadêmicos

Há também uma isenção à aplicação da Lei que busca conferir um incentivo à produção acadêmica, o que ocorre de maneira apenas mitigada, tendo em vista a complexidade da matéria e a possibilidade de desvirtuação desta isenção por empresas privadas, que poderiam financiar pesquisas acadêmicas com a intenção de se beneficiar das isenções conferidas às instituições acadêmicas.

Assim, a legislação obriga a observação dos artigos 7º e 11 da LGPD, dizendo respeito à obrigação de buscar o enquadramento dos dados pessoais coletados em alguma hipótese legal de tratamento, bem como todos os meios técnicos razoáveis e disponíveis no momento do tratamento para a proteção dos dados pessoais dos titulares.

Apesar da menção expressa de apenas essas duas disposições da legislação, quais sejam, os artigos 7º e 11, uma instituição acadêmica que optasse, por exemplo, por tratar os dados com base no consentimento, teria de invariavelmente observar as outras disposições contidas no art. 8º da Lei. Da mesma forma, caso optasse por tratar os dados sob o manto do legítimo interesse, teria que observar os ditames contidos no art. 10 da Lei, bem como as demais disposições sobre a realização de um Relatório de Impacto à Proteção de Dados Pessoais, por exemplo.

Desta forma, mesmo que exista a isenção, os pesquisadores ainda terão que estar atentos às documentações que comprovem o interesse puramente acadêmico no tratamento dos dados, e que

comprovem que estejam sendo observados os demais princípios da LGPD, como a finalidade, a adequação, a necessidade e a segurança[41].

5. Tratamento pelo Estado

A LGPD, a fim de resguardar os interesses nacionais no que tange ao tratamento de dados pessoais, criou a exceção contida no inciso III. Entretanto, tendo em vista a sua relevância e potencial utilização para fins econômicos, os parágrafos do artigo 4º buscam colocar algumas limitações a esta utilização pelo Estado, enquanto as iniciativas para o estabelecimento de um marco legal de tratamento de dados pelo Poder Público nestas condições não forem promulgadas.

Sem prejuízo destas disposições, a Lei estabelece que a ANPD também realizará toda a fiscalização deste tipo de tratamento pelo Poder Público, inclusive com a necessidade de apresentação de Relatório de Impacto à Proteção de Dados Pessoais (RIPD) pelos agentes públicos.

Frise-se que o Capítulo IV da lei se dedica a informar os requisitos e condições de tratamento para o Poder Público nos casos que não envolvem a segurança pública, a defesa nacional, a segurança do Estado ou investigações criminais, como ocorre na utilização de

[41] BARRETO, Maurício L.; ALMEIDA, Bethânia; DONEDA, Danilo. Uso e Proteção de Dados Pessoais na Pesquisa Científica. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (orgs). **Tratado de Proteção de Dados Pessoais**. 1º ed. Rio de Janeiro: Forense, 2021. pp. 528-530.

dados pessoais para a formulação de políticas públicas de saúde, por exemplo.

Outrossim, a LGPD proíbe o tratamento daqueles dados relacionados à segurança pública, defesa nacional, segurança do Estado e investigações criminais, por pessoas jurídicas que se submetam ao regime jurídico de direito privado, salvo se realizado sob a tutela do Poder Público, ou seja, de pessoa jurídica que se submeta ao regime jurídico de direito público, observando-se ainda as regulamentações específicas da ANPD.

Com o intuito de garantir a segurança dos dados e de que eles estejam sendo tratados para as finalidades pretendidas, o tratamento desses dados por uma pessoa jurídica de direito privado deverá se dar nas dependências da entidade pública, o que ressalta a necessidade de adequação dos contratos firmados pelo poder público com agentes terceirizados[42].

O termo "totalidade dos dados pessoais de banco de dados", presente no §4º, deve ser entendido como todos os dados em um determinado banco de dados do agente público. Assim, caso o Poder Público opte por terceirizar o tratamento à pessoa submetida ao regime jurídico de direito privado, deverá realizar operações de separação e

[42] ABREU, Jacqueline de Souza. Tratamento de Dados Pessoais para a Segurança Pública: Contornos do Regime Jurídico pós-LGPD. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (orgs). **Tratado de Proteção de Dados Pessoais**. 1º ed. Rio de Janeiro: Forense, 2021. p. 597.

randomização das suas bases de dados antes da transferência, a fim de impedir que estes dados possam ser posteriormente associados a um determinado indivíduo[43].

6. Dados provenientes do exterior

O inciso IV possui eficácia contida, pois depende de uma regulamentação posterior da ANPD para ser efetivo na proteção de dados pessoais. Busca, assim, oferecer um incentivo legal para o tratamento de dados do exterior em solo nacional, sem tornar o país uma espécie de "paraíso fiscal" de dados pessoais.

Deste modo, apenas os dados provenientes do país que foram coletados poderão ser tratados sob essa exceção, e desde que este país também proporcione grau de proteção de dados adequado, o que será possivelmente indicado através de regulamentações da ANPD.

[43] VAINZOF, Rony. Capítulo I – Disposições Preliminares. In. MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). **LGPD** – Lei Geral de Proteção de Dados – Comentada. 2ª ed. São Paulo: Revista dos Tribunais, 2019. p. 88.

Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 13.853, de 2019)

IX - agentes de tratamento: o controlador e o operador;

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado

XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e

XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

1. Importância das definições legais

As definições legais contidas no art. 5º buscam evidenciar o verdadeiro sentido da Lei, a fim de respaldar futuras decisões judiciais ou políticas públicas e, desta forma, garantir uma melhor segurança jurídica aos titulares e agentes de tratamento.

2. Dados pessoais

Primeiramente, importante ressaltar que a LGPD visa proteger apenas os dados referentes aos indivíduos (pessoas físicas). Portanto, informações relacionadas a empresas, mesmo que sejam sigilosas ou confidenciais, tais como planejamentos estratégicos, balanços financeiros, sistemas em desenvolvimento, protótipos, fórmulas ou outras inovações, não são protegidas pela LGPD. Ressalte-se que tais

informações e documentos são amparados por outras leis, tais como a Lei de Propriedade Industrial (Lei nº 9.279/96), a Lei de Direitos Autorais (Lei nº 9.609/98) e a Lei de Software (Lei nº 9.610/98)[44].

Deste modo, qualquer informação que possa identificar a pessoa, ou pelo menos torná-la identificável, é protegida por esta Lei. Assim, uma determinada informação que não faça referência a determinada pessoa (um metadado de uma foto, ou até mesmo informações da própria empresa, como um CNPJ, por exemplo), mas que se cruzada com outras informações presentes em outros bancos de dados, torne possível a identificação da pessoa, é considerada um dado pessoal.

Nesse sentido, a Lei aplica uma lógica expansionista, ou seja, expande o conceito de dados pessoais para fora da esfera imediata do indivíduo, visando proteger mesmo aqueles dados que não podem ser a ele diretamente conectados[45].

3. Dados pessoais sensíveis

Dados pessoais sensíveis dizem respeito àqueles dados que podem dar causa a uma discriminação contra determinado indivíduo.

---

[44] VAINZOF, Rony. Capítulo I – Disposições Preliminares. In. MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). **LGPD** – Lei Geral de Proteção de Dados – Comentada. 2ª ed. São Paulo: Revista dos Tribunais, 2019. p. 90.

[45] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 2ª ed. Rio de Janeiro: Forense, 2018. p. 60.

Portanto, o rol presente no inciso II é meramente exemplificativo, sendo considerado sensível todo e qualquer dado que revele uma possível vulnerabilidade à dignidade do titular.

É ainda mais relevante esta consideração quando se coloca a possibilidade de revelação de dados sensíveis através do cruzamento de bases de dados, resultando em condições de tratamento de dados que possam ser indesejadas, discriminatórias ou prejudiciais ao titular.

Nesse sentido, discorre Doneda[46] que "um dado, em si, não é perigoso ou discriminatório – mas o uso que dele se faz, pode sê-lo".

Semelhantemente, na mesma linha, Bioni[47] alerta para a utilização de algoritmos de *Big Data* para a revelação de informações sensíveis através de dados triviais ou até mesmo metadados. O autor ressalta um estudo realizado pela Universidade de Cambridge, que com base na análise de "curtidas" em *posts* do Facebook, concluiu ser possível identificar, de forma convincente, a orientação sexual, a raça e a ideologia política dos usuários.

Da mesma forma, dados sobre a geolocalização de um usuário poderiam indicar se ele frequenta determinada igreja ou se vai com frequência a determinado sindicato, por exemplo.

---

[46] DONEDA, Danilo. **Da privacidade à proteção de dados**. Rio de Janeiro: Renovar, 2005. p.162.

[47] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 2ª ed. Rio de Janeiro: Forense, 2018. p. 85.

Trata-se, portanto, da efetivação do princípio previsto no art. 6º, inciso IX, da não discriminação, que será abordado com mais profundidade no momento oportuno.

Ademais, importante frisar que as hipóteses de tratamento, mais restritivas do que aquelas concernentes aos dados pessoais comuns, se encontram dispostas nos incisos do art. 11 da LGPD.

4. Anonimização e dados anonimizados

O dado anonimizado é a antítese do dado pessoal, ou seja, é aquele dado que impede a identificação de uma determinada pessoa.

Em linhas gerais, a anonimização é o processo pelo qual o dado deixa de ser pessoal e passa a ser anônimo. Nesse sentido, Bioni[48] comenta que as diferentes técnicas de anonimização se prestam a realizar um gerenciamento da "identificabilidade" das informações em determinado banco de dados. Assim, quanto mais sensíveis, maior será a necessidade de tornar os dados anônimos para os fins de tratamento.

A LGPD, ao invés de escolher dar enfoque a um método específico de anonimização, preferiu por deixar essa questão em aberto, tendo em vista o rápido avanço tecnológico na área de processamento de dados e segurança da informação. Assim, estabelece o critério da razoabilidade, que pode ser desdobrado em dois eixos principais de

[48] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 2ª ed. Rio de Janeiro: Forense, 2018. p. 63.

análise da eficácia do processo de anonimização: um critério objetivo e um critério subjetivo.

O eixo objetivo leva em conta, principalmente, o custo e o tempo da reversão do processo de anonimização, de acordo com as tecnologias disponíveis à época da anonimização. Trata-se, portanto, do grau de resiliência de um determinado processo de anonimização perante os padrões tecnológicos presentes[49].

O eixo subjetivo, por sua vez, leva em conta se o próprio agente de tratamento possui os meios para a reversão do processo de anonimização. Analisa-se, assim, a capacidade individual de engenharia reversa de quem está processando os dados[50].

Esse eixo de análise é importante pois existem práticas de anonimização em que a própria empresa mantém em separado outras bases de dados relacionadas, permitindo a reversão do processo de anonimização, o que a lei convencionou chamar de pseudonimização, ou seja, uma falsa e apenas aparente anonimização. Sobretudo, é certo que tal processo, apesar de não transformar os dados em anonimizados, minimiza os riscos de uma atividade de tratamento de dados, vez que terceiros terão maior dificuldade em reverter a anonimização.

Ainda no eixo subjetivo, importante ressaltar a possibilidade de terceiros externos realizarem o processo de reversão por meios

[49] BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. **Revista do Advogado**. São Paulo, n. 144, nov. 2019. p.24.
[50] Ibidem. p. 25

próprios, especialmente nas ocasiões em que há o efetivo compartilhamento de dados pessoais. É o caso de um determinado terceiro deter bases de dados adicionais ou tecnologias disruptivas de processamento de dados, diminuindo em muito a eficácia e resiliência de qualquer procedimento de anonimização[51].

Assim, nenhuma técnica de anonimização poderia ser considerada 100% eficaz. Para ilustrar esse fato, é interessante levantar o caso de alguns pesquisadores da Universidade do Texas, que conseguiram, a partir do cruzamento de uma base de dados anonimizada fornecida pelo Netflix, com informações públicas contidas na plataforma do IMDB, identificar de maneira precisa a esmagadora maioria dos usuários da plataforma de *streaming*[52].

Entretanto, a LGPD é clara ao dispor a anonimização como uma boa medida de proteção aos dados pessoais, devendo os agentes de tratamento realizar adequações de ordem técnica, organizacional e contratual, com o objetivo de controlar os riscos associados à reidentificação de dados pessoais, de acordo com as particularidades de suas atividades.

Ressalta-se, uma vez mais que nenhum método de anonimização se mostra 100% infalível, tendo em vista que os vínculos

---

[51] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 2ª ed. Rio de Janeiro: Forense, 2018. p. 64.

[52] NARAYANAN, Arvind; SHMATIKOV, Vitaly. Myths and Fallacies of "Personally Identifiable Information". **Communications of the ACM**. Association for Computing Machinery, jun/2010, v. 53, n. 06, p. 24. Disponível em: www.cs.utexas.edu/~shmat/shmat_cacm10.pdf>. Acesso em 07.12.2020.

de identificação com determinada base de dados sempre existirão. Assim, começa a existir uma aparente contradição no estabelecimento do conceito de dados anonimizados, vez que todo dado anonimizado é, potencialmente, um dado pessoal[53].

Para contornar essa contradição, a LGPD estabeleceu o critério da razoabilidade para a delimitação do conceito de dados pessoais, o que, possivelmente, será regulamentado pela ANPD. Desta forma, se para a identificação de dados anonimizados requer-se um esforço maior do que o razoavelmente exigível, não há que se falar em dados pessoais.

5. Bancos de dados

A conceituação de banco de dados é útil para dois objetivos. Primeiramente, com tal conceito é possível dar efetividade ao direito dos titulares de requisitar a eliminação ou retificação de seus dados, além de possibilitar a imposição de algumas das sanções previstas pela Lei. Em segundo lugar, torna possível a separação entre os dados pessoais e os algoritmos que organizam essas bases de dados[54].

Assim, caso haja a necessidade de bloqueio ou eliminação de determinado dado de uma base de dados, tais medidas não terão qualquer efeito sobre o software utilizado para o tratamento, tendo em

[53] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 2ª ed. Rio de Janeiro: Forense, 2018. p. 64.
[54] BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. **Revista do Advogado**, n. 144, nov. 2019. P. 23.

vista que poderia ser uma propriedade intelectual do agente de tratamento, mas somente serão aplicadas em relação aos dados contidos naquela base de dados.

Entretanto, ao mesmo tempo em que se afigura como uma proteção ao titular, a utilização do termo "estruturado" pode levar a algumas dúvidas sobre a aplicação da LGPD a conjuntos de dados não-estruturados.

Em um entendimento mais técnico, os dados estruturados são aqueles que são altamente organizados para permitir uma análise mais eficiente, como bem define a Lei.

Por outro lado, estima-se que a maior parte dos dados coletados e tratados na atualidade sejam dados não-estruturados, que não seguem padrões pré-definidos ou podem ser facilmente relacionados com outras bases de dados, como é o caso das informações armazenadas por grandes conglomerados de tecnologia[55].

Logo, se as sanções ou os direitos dos titulares só podem ser efetivados com relação às bases que contém dados estruturados, pode-se identificar uma lacuna normativa, que deverá ser integrada com base em cada caso concreto.

[55] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 2ª ed. Rio de Janeiro: Forense, 2018. p. 18.

6. Titulares de dados

O titular de dados pessoais é o núcleo de proteção da LGPD, que busca proteger os seus direitos fundamentais de liberdade, privacidade e livre desenvolvimento de sua personalidade.

No Brasil, tendo em vista as recentes discussões acerca dos direitos do nascituro, pode-se afirmar que a tutela prevista pela LGPD se inicia na concepção da pessoa, em razão do início da sua personalidade jurídica formal, como uma expectativa de direito sobre seus dados pessoais, que é totalmente adquirida com o nascimento com vida, e se encerra com o seu falecimento, conforme dispõe o art. 6º do Código Civil[56].

Importante frisar também que as pessoas falecidas não são consideradas pessoas naturais e, portanto, no âmbito da LGPD, não seriam consideradas titulares de dados pessoais. Entretanto, vale ressaltar que estas possuem seus dados pessoais resguardados pelo art. 12, parágrafo único e pelo art. 20, parágrafo único do Código Civil, que visam proteger os direitos de personalidade das pessoas falecidas.

[56] BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Art. 6º: A existência da pessoa natural termina com a morte; presume-se esta, quanto aos ausentes, nos casos em que a lei autoriza a abertura de sucessão definitiva.

7. Agentes de tratamento

A Lei conceitua agentes de tratamento para se referir de forma conjunta ao controlador e ao operador de dados. Entretanto, é sobre o controlador que a LGPD busca impor maior fiscalização, tendo em vista que é ele quem efetivamente toma todas as decisões pertinentes acerca do tratamento dos dados dos titulares, enquanto o operador apenas segue as suas diretivas.

Com a crescente diversificação dos serviços e produtos ofertados na *internet*, a tarefa de se diferenciar um controlador de um operador, que age apenas sob as ordens estritas do controlador, se torna um procedimento cada vez mais complexo. O enquadramento como controlador, desta forma, pode advir de uma disposição expressa ou implicitamente prevista em Lei ou por circunstâncias do caso concreto[57].

Tome-se de exemplo o caso de um escritório de contabilidade que necessite tratar os dados de seus clientes para a própria prestação dos serviços contábeis, bem como tratar dados de seus funcionários para o cumprimento do contrato de trabalho. No caso dos dados de seus clientes, não há dúvidas de que o escritório de contabilidade será mero operador; entretanto, no caso do tratamento de dados pessoais de seus funcionários, será considerado controlador.

---

[57] VAINZOF, Rony. Capítulo I – Disposições Preliminares. In. MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). **LGPD** – Lei Geral de Proteção de Dados – Comentada. 2ª ed. São Paulo: Revista dos Tribunais, 2019. p. 106.

A definição de quem será o controlador e de quem será o operador também pode advir de uma análise das cláusulas contratuais pactuadas entre as partes envolvidas, por exemplo, ou da análise das atividades exercidas por cada uma das partes.

Isto porque uma empresa que se enquadre como operadora, se realizar um tratamento fora das finalidades dispostas pela controladora, ou seja, de forma ilícita, se torna também uma controladora em seus próprios termos, em relação ao novo tratamento que der aos dados.

Assim, se a operadora de dados começar a utilizar os dados fornecidos pelo controlador em seu benefício próprio, haverá a modificação da sua qualificação de operadora para controladora.

8. Encarregado de dados

O encarregado de dados é a pessoa, física ou jurídica, responsável não só pela comunicação entre o controlador, os titulares e a ANPD, mas também por cumprir com todas as responsabilidades dispostas no art. 42, §3º da LGPD, que incluem a orientação dos funcionários e contratados da empresa a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.

O encarregado de dados também pode ser denominado DPO ("*Data Protection Officer*"), nomenclatura que é utilizada na Europa e no RGPD, e que também é comum no Brasil.

Até posterior regulamentação pela ANPD, todas as empresas do Brasil que realizam o tratamento de dados pessoais estão obrigadas a nomear um DPO, independentemente do seu tamanho. Espera-se que esta regulamentação futura delimite tal obrigação de acordo com a natureza e o porte da empresa, bem como o volume de dados por ela tratados.

Frise-se também que o encarregado pode ser um funcionário, uma equipe de funcionários (com um contato principal indicado), ou até mesmo uma empresa terceirizada, devendo o agente de tratamento se atentar à carga do serviço e ao volume de dados quando realizar a escolha do DPO.

É importante também que o encarregado de dados não sofra qualquer tipo de interferência em suas atribuições, o que será mais bem exemplificado nas disposições que tratam de forma exclusiva das suas responsabilidades e obrigações, mais precisamente no capítulo VI.

Também é recomendado que este encarregado possua um sólido conhecimento da LGPD e da regulamentação setorial de proteção de dados pessoais, além de todas as outras questões relativas às atividades desempenhadas pela companhia, envolvendo a natureza, o âmbito, o contexto e as finalidades das operações de tratamento de dados da empresa[58].

[58] VAINZOF, Rony. Capítulo I – Disposições Preliminares. In. MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). **LGPD** – Lei Geral de Proteção de Dados – Comentada. 2ª ed. São Paulo: Revista dos Tribunais, 2019. p. 113.

Após nomeado o encarregado, deve tal fato ser devidamente comunicado a todos os colaboradores da empresa, com informações sobre o seu papel e suas atribuições, sendo também recomendado que ele tenha acesso a todos os recursos para que possa cumprir com as suas atribuições de maneira efetiva.

9. Tratamento de dados pessoais

A LGPD é extremamente abrangente nas hipóteses que qualificam o tratamento de dados pessoais. Assim, a partir da data de 18 de setembro de 2020, quando a legislação entrou em vigor, qualquer das ações contidas no inciso X, realizadas por pessoa física ou jurídica, se qualificam como tratamento de dados pessoais.

Desta maneira, é de suma importância a realização de um mapeamento de dados pelas empresas, a fim de verificar todas as operações de tratamento realizadas, e se estas operações se encontram enquadradas nas bases legais contidas nesta Lei, conforme será mais bem analisado no Capítulo VII.

10. Consentimento

O consentimento, na doutrina civilista, nada mais é do que a manifestação de vontade do titular, e, até a positivação da LGPD, era considerado pelo Marco Civil da *Internet* como sendo a única base de

tratamento possível para a coleta e processamento de dados pelos agentes de tratamento[59].

De acordo com o inciso X do art. 5º da Lei, o consentimento deixou de ser definido como uma manifestação simples de vontade, para se tornar uma manifestação livre, informada e inequívoca de vontade.

Dada a sua importância, a legislação confere o devido destaque ao consentimento, fazendo o total de 37 referências a esta base legal, mais do que qualquer outra hipótese de tratamento referenciada na LGPD.

Diz-se que o consentimento deve ser "livre" porque o titular tem o direito de agir ou não agir no que diz respeito a dar o seu consentimento. Desta forma, caso não esteja fundamentado nos princípios elencados no art. 6º da LGPD, como a necessidade e a finalidade, o agente de tratamento não poderá condicionar o acesso do titular a um produto ou serviço ao fornecimento do seu consentimento, sob o risco de esta ser considerada uma prática abusiva[60].

---

[59] BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Art. 7º: O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: [...] VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei.

[60] BRASIL. Superior Tribunal de Justiça. **Recuso Especial nº 13485332 SP 2012/020805-4**. CONSUMIDOR. CERCEAMENTO DE DEFESA. NÃO OCORRÊNCIA. CONTRATO DE CARTÃO DE CRÉDITO. CLÁUSULAS ABUSIVAS. COMPARTILHAMENTO DE DADOS PESSOAIS. NECESSIDADE DE OPÇÃO POR SUA NEGATIVA. DESRESPEITO AOS PRINCÍPIOS DA

Já a manifestação do consentimento também deve ser "informada" porque deve ser devidamente explicado ao titular todos os termos do tratamento dos seus dados pessoais, incluindo a forma, os prazos e se há transferência a terceiros, estando diretamente conectada com o princípio da transparência, previsto no art. 6º, inciso VI da LGPD.

Por fim, a manifestação deve ser "inequívoca", pois a anuência do titular dos dados pessoais deve ser feita a partir de condutas afirmativas, de forma explícita ou implícita, capazes de ser devidamente armazenadas pelo controlador para fins de prova. Isso significa que o silêncio, a omissão ou opções pré-marcadas não serão consideradas formas válidas de consentimento[61].

TRANSPARÊNCIA E CONFIANÇA. ABRANGÊNCIA DA SENTENÇA. ASTREINTES. RAZOABILIDADE. [...] 3. É abusiva e ilegal cláusula prevista em contrato de prestação de serviços de cartão de crédito, que autoriza o banco contratante a compartilhar dados dos consumidores com outras entidades financeiras, assim como com entidades mantenedoras de cadastros positivos e negativos de consumidores, sem que seja dada a opção de discordar daquele compartilhamento. 4. A cláusula posta em contrato de serviço de cartão de crédito que impõe a anuência com o compartilhamento de dados pessoais do consumidor é abusiva por deixar de atender a dois princípios importantes da relação de consumo: transparência e confiança. 5. A impossibilidade de contratação do serviço de cartão de crédito, sem a opção de negar o compartilhamento dos dados do consumidor, revela a exposição que o torna indiscutivelmente vulnerável, de maneira impossível de ser mensurada e projetada. 6. De fato, a partir da exposição de seus dados financeiros abre-se possibilidade para intromissões diversas na vida do consumidor. Conhecem-se seus hábitos, monitoram-se a maneira de viver e a forma de efetuar despesas. Por isso, a imprescindibilidade da autorização real e espontânea quanto à exposição. [...] 11. Recurso especial parcialmente provido.
(STJ – Resp: 13485332 SP 2012/020805-4, Relator: Ministro Luis Felipe Salmoão, Data de julgamento: 10/10/2017, T4 – Quarta Turma, Data de publicação: DJe 30/11/2017).

[61] VAINZOF, Rony. Capítulo I – Disposições Preliminares. In. MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). **LGPD** – Lei Geral de

A título de exemplificação, se um usuário acessa um *website*, é alertado com um *banner* do uso de *cookies* de navegação, aceita a utilização desses *cookies* através da marcação em uma caixa de seleção, com a possibilidade de recusa, e mesmo assim continua navegando no *site*, pode-se dizer que a sua conduta foi inequívoca no consentimento para o tratamento de seus dados de navegação.

Importante ressaltar a diferenciação entre o consentimento disposto no Marco Civil da *Internet* (MCI) e na LGPD, vez que no MCI, apenas é mencionado que este deve ser expresso e se dar de forma destacada das demais cláusulas contratuais.

Entretanto, a qualificação oferecida pela LGPD, até por ser Lei posterior e específica, oferece uma maior proteção aos titulares, pois não deixa qualquer espaço para ambiguidades relacionadas com condutas incompatíveis com a recusa no tratamento de dados.

11. Bloqueio e eliminação de dados

O bloqueio é uma forma de interrupção de toda e qualquer forma de tratamento de dados, seja de um dado específico ou de um conjunto inteiro e estruturado de dados. Entretanto, o bloqueio não atinge o armazenamento destes dados, tendo em vista que é uma medida de natureza temporária e que pode ser revertida.

Proteção de Dados – Comentada. 2ª ed. São Paulo: Revista dos Tribunais, 2019. p. 120.

O bloqueio pode ser realizado pelo próprio controlador, quando houver dúvidas acerca da legalidade do tratamento, ou mediante requisição do titular, nos termos do art. 18, inciso IV da LGPD. Também pode ser resultado de uma sanção administrativa aplicada pela ANPD, respeitado o direito de ampla defesa e devido processo legal, nos termos do art. 52, inciso V da LGPD.

Já a eliminação é a exclusão definitiva de um dado específico ou de um conjunto estruturado de dados contidos em um banco de dados. Pode ser realizado pelo próprio controlador, como medida de mitigação de riscos de segurança da informação, ou mediante requisição do titular de dados, nos termos do art. 18, inciso IV da LGPD[62]. Também pode ser resultado de uma sanção administrativa aplicada pela ANPD, sendo essa sanção uma das mais extrema dentre todas as previstas, conforme preleciona o seu art. 52, inciso VI[63].

Ao proceder com o bloqueio ou eliminação, o controlador deve comunicar de forma imediata a todos os terceiros que tiverem compartilhado os dados para que também procedam com o respectivo

[62] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Art. 18: O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: [...] IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei.

[63] Ibidem. Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: [...] VI - eliminação dos dados pessoais a que se refere a infração.

bloqueio ou eliminação desses dados, nos termos do art. 18, §6º da Lei[64].

12. Transferências internacionais e compartilhamento de dados

A globalização é um imperativo da sociedade contemporânea, e o tratamento de dados pessoais geralmente envolve uma longa cadeia de agentes que atuam em território nacional e em outros países, sobretudo quanto aos serviços de armazenamento em nuvem, que armazenam arquivos, e-mails, backups, dentre outras informações.

Desta forma, para assegurar o cumprimento da Lei e a segurança dos dados pessoais transferidos a outros países, a LGPD regula estas transferências internacionais de dados através das hipóteses contidas no rol taxativo do seu artigo 33, que são devidamente comentadas no próprio artigo.

Destaca-se, ainda, que a Lei busca também regular todo e qualquer compartilhamento de dados pessoais, ressaltando o cumprimento das competências legais, no caso de compartilhamento por órgãos do Poder Público, ou de autorização específica, nos casos de

[64] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: [...] § 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional.

compartilhamento entre entidades privadas. Assim, o conceito do "uso compartilhado de dados" entra em consonância com os demais fundamentos, objetivos e princípios da Lei, provendo uma adequada proteção aos dados pessoais no ordenamento jurídico nacional.

13. Relatório de impacto à proteção de dados pessoais (RIPD)

O relatório de impacto à proteção de dados pessoais (RIPD) é um instrumento que deve ser confeccionado pelo controlador para determinar todo o ciclo de vida dos dados pessoais e também os riscos relacionados ao tratamento de dados, bem como para descrever os processos de mitigação destes riscos.

Cabe destacar, também, a necessidade da elaboração de um RIPD adicional, nas hipóteses baseadas no legítimo interesse[65] ou naqueles tratamentos que possam atingir os direitos fundamentais dos titulares.

Dentro dos procedimentos de governança em proteção de dados, o RIPD serve como base para a efetivação dos seguintes princípios, abarcados no art. 6º da LGPD:

(i) finalidade: avaliação dos propósitos legítimos de tratamento;

[65] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...] IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; [...]

(ii) adequação: avaliação da compatibilidade entre as finalidades de tratamento pretendidas e o contexto de tratamento;

(iii) necessidade: adoção de medidas que limitem o tratamento ao mínimo necessário para as finalidades pretendidas;

(iv) segurança: adoção de medidas técnicas e organizacionais relacionadas à segurança da informação;

(v) prevenção: adoção de medidas dispostas a mitigar os riscos relacionados ao tratamento de dados pessoais[66].

O relatório de impacto é de obrigação do controlador, mas pode ser confeccionado por agentes externos ou internos, sendo recomendável o devido acompanhamento pelo encarregado de dados da entidade.

Em linhas gerais, visa analisar a viabilidade de novos produtos ou serviços, ou a continuidade de antigos, sob a ótica da proteção de dados pessoais, mediante uma avaliação da necessidade e razoabilidade das operações em relação aos objetivos pretendidos, indicando as medidas de mitigação de riscos a serem adotadas, permitindo aos

[66] VAINZOF, Rony. Capítulo I – Disposições Preliminares. In. MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). **LGPD** – Lei Geral de Proteção de Dados – Comentada. 2ª ed. São Paulo: Revista dos Tribunais, 2019. p. 129.

gestores tomar decisões baseadas em custos, riscos, benefícios e eventuais oportunidades[67].

14. Órgãos de pesquisa

Os órgãos de pesquisa mais comumente conhecidos incluem instituições públicas como o IBGE (Instituto Brasileiro de Geografia e Estatística) e o IPEA (Instituto de Pesquisa Econômica Aplicada) e também instituições privadas, como o IBOPE (Instituto Brasileiro de Opinião Pública e Estatística) e o Datafolha.

Estes órgãos estão diretamente relacionados com o tratamento de dados pessoais para o fornecimento de informações estatísticas relevantes. Desta forma, a LGPD prevê algumas permissões notórias para os órgãos de pesquisa, dentre as quais: (i) o tratamento de dados pessoais, independentemente de consentimento (art. 7º, inciso IV e art.11, inciso II, alínea "c" da LGPD); (ii) o acesso a bases de dados na realização de estudos em saúde pública (art. 13 da LGPD); (iii) a conservação de dados pessoais mesmo após o término do tratamento (art. 16, inciso II da LGPD).

Entretanto, a Lei também destaca que, sempre que possível, as operações de tratamento por órgãos de pesquisa devem ser realizadas com os dados anonimizados.

[67] Ibidem.p. 130.

Para se enquadrar como sendo um órgão de pesquisa, a pessoa jurídica de direito privado deve ser legalmente constituída como sendo sem fins lucrativos, podendo se encaixar nessa definição as associações do art. 53, *caput*, do Código Civil[68] ou as fundações do art. 62 e seguintes do Código Civil[69].

Tanto as pessoas jurídicas de direito público quanto de direito privado devem possuir, em sua missão institucional ou em seu objeto social, a pesquisa básica ou aplicada, de caráter histórico, científico, tecnológico ou estatístico.

15. Autoridade Nacional de Proteção de Dados - ANPD

É o órgão pertencente à União, responsável pela aplicação direta da LGPD, cuja estrutura, competências e atribuições estão dispostas no Anexo I do Decreto nº 10.474/20 e também no art. 55-A e seguintes da Lei, que serão comentados em momento oportuno.

[68] BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Art. 53: Constituem-se as associações pela união de pessoas que se organizem para fins não econômicos.

[69] Ibidem. Art. 62: Para criar uma fundação, o seu instituidor fará, por escritura pública ou testamento, dotação especial de bens livres, especificando o fim a que se destina, e declarando, se quiser, a maneira de administrá-la.

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

1. Princípios da LGPD

Nos sistemas que seguem a tradição legal romano-germânica, como é o sistema jurídico brasileiro, a boa-fé é o princípio que se assenta na fidelidade ao agir, que pode ser desdobrada em dois aspectos

principais: a lealdade no cumprimento exato da obrigação e a necessidade de observar os interesses da outra parte[70].

Portanto, é possível afirmar que o princípio da boa-fé pauta todo o ordenamento jurídico nacional, constituindo um verdadeiro imperativo ético de comportamento que impõe a todo cidadão, de maneira concreta, que atue nas suas relações com honestidade, lealdade e probidade.

Nesse sentido, o titular de dados tem a confiança de que as suas informações só serão utilizadas e tratadas em conformidade com as suas expectativas legítimas. Desta forma, o agente de tratamento, a fim de demonstrar a sua boa-fé no tratamento de dados pessoais perante a autoridade reguladora ou autoridade judicial, deverá pautar suas ações e comprovar através de documentos que está agindo de boa-fé e que está seguindo os princípios elencados pela LGPD[71].

2. Finalidade

A finalidade do tratamento é, possivelmente, o princípio que abarca a maior complexidade prática para a adequação à LGPD. Logo, a sua manipulação pode vir a influenciar diretamente nos modelos de

[70] LISBOA, Roberto Senise. **Manual de Direito Civil**. V.3. Contratos. 7ª ed. São Paulo: Saraiva, 2012. p. 234.
[71] SARLET, Ingo Wolfgang. Fundamentos Constitucionais: o Direito Fundamental à Proteção de Dados. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (orgs). **Tratado de Proteção de Dados Pessoais**. 1º ed. Rio de Janeiro: Forense, 2021. pp. 39-41.

negócios das empresas que realizem qualquer tipo de tratamento de dados, tendo em vista que este princípio compõe uma ampla restrição à coleta e processamento indiscriminados de dados pessoais.

Se em um cenário anterior à legislação de proteção de dados pessoais o tratamento poderia se dar sob qualquer pretexto, no cenário atual é necessário que os agentes de tratamento se adequem às finalidades especificadas pela própria Lei para qualquer tipo de tratamento de dados.

Danilo Doneda[72] considera que este princípio vincula o dado pessoal a determinado propósito, durante todo o ciclo de vida do tratamento daquela informação. Portanto, sendo o dado pessoal uma expressão direta da personalidade do titular, podendo o seu processamento refletir diretamente na sua vida, tem-se que esse elo de ligação entre a finalidade e o dado pessoal deve ser sempre mantido e protegido pela legislação.

Tal disposição inviabiliza o tratamento posterior com quaisquer outras finalidades sem a consequente alteração da base legal de tratamento, ou seja, torna qualquer tipo de tratamento, sem o propósito expresso, ilícito.

[72] DONEDA, Danilo. Princípios de Proteção de Dados Pessoais. In: LUCCA, Newton de. SIMÃO FILHO; Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III**: Marco civil da internet. São Paulo: Quartier Latin, 2015. T.1. p. 378.

Posto isto, é de suma importância que as empresas se atentem à finalidade do tratamento desde a concepção de um determinado projeto, o que é denominado *privacy by design*.

Uma exceção a esta vedação da mudança de finalidade que está contida na Lei pode ser encontrada no art. 7º, §7º da LGPD, o qual prevê a alteração da finalidade para os dados de acesso público ou tornados manifestamente públicos pelo titular "desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular". Trata-se de uma ampla margem legal de alteração da finalidade, sendo necessário respeitar, entretanto, os fundamentos e princípios contidos na legislação, o que será mais bem discutido nos comentários do art. 7º.

3. Adequação

A adequação trata do nexo estabelecido entre a finalidade de determinado tratamento e o contexto real em que os dados são tratados.

Assim, a título de exemplificação, poderia se dizer adequado o tratamento realizado por um aplicativo de saúde para dar informações a um usuário a partir dos dados sobre batimentos cardíacos de um indivíduo, se ele der o seu consentimento prévio e informado.

Por outro lado, considerando o mesmo cenário, tem-se que este tratamento seria inadequado se a empresa começasse a criar um perfil de saúde desta pessoa para outras finalidades, como no

desenvolvimento de um novo produto ou serviço ou, ainda, para demais fins comerciais, por exemplo, vez que fugiria totalmente do contexto inicial de tratamento[73].

Portanto, este princípio busca de certa forma limitar a elasticidade potencial que poderia se dar ao conceito de finalidade, convidando o intérprete legal a uma análise mais aprofundada da relação estabelecida entre o agente de tratamento e o titular de dados.

4. Necessidade

Este princípio também restringe as finalidades que podem ser eventualmente elencadas pelo agente de tratamento para a utilização de dados pessoais, tendo em vista que limita o tratamento ao mínimo necessário para a realização do serviço, limitando também o tempo com que estes dados poderão ser armazenados.

Este princípio busca inverter a lógica existente hoje no país, de uma coleta excessiva de dados para posterior averiguação da sua efetiva necessidade, alterando para uma lógica pautada na restrição, minimização e mitigação de riscos relacionados à coleta e ao tratamento indiscriminado de dados pessoais.

[46] VAINZOF, Rony. Capítulo I – Disposições Preliminares. In. MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). **LGPD** – Lei Geral de Proteção de Dados – Comentada. 2ª ed. São Paulo: Revista dos Tribunais, 2019. p. 143.

5. Livre acesso

O princípio do livre acesso visa efetivar os direitos dos titulares de dados previstos na Lei, permitindo ao titular acessar e, consequentemente, controlar o fluxo informacional de seus dados pessoais, avaliar eventuais incorreções que possam ser corrigidas e requerer o descarte dos seus dados pessoais se o tratamento se mostrar excessivo, inadequado ou ilícito.

6. Qualidade dos dados

Tendo em vista que os dados pessoais são cada vez mais utilizados para a vida de um indivíduo na sociedade contemporânea, é crucial que estes estejam sempre precisos e atualizados, a fim de proteger o indivíduo de quaisquer danos que possam ser causados pela imprecisão de seus dados, como uma exposição indevida ou até mesmo culminando em uma prisão injusta, por exemplo.

7. Transparência

Intimamente relacionado com a boa-fé, o princípio da transparência busca fomentar uma relação de confiança entre os agentes de tratamento e os titulares de dados, permitindo a compreensão pelos titulares acerca de todos os procedimentos de tratamento de dados e, inclusive, quais as possíveis consequências que tal tratamento pode acarretar para a esfera individual desses titulares.

Desta forma, o agente de tratamento deve sempre avaliar as melhores formas de efetivar este princípio, através do fornecimento de explicações claras, adequadas e ostensivas sobre as operações de tratamento realizadas.

A título de curiosidade, o Google está sendo processado pela autoridade europeia com uma possível sanção de 50 milhões de euros, tendo em base, justamente, a falta de transparência das suas operações de tratamento[74].

8. Segurança

Por estar positivada na base principiológica da LGPD, é possível notar que a segurança da informação vem ganhando contornos jurídicos cada vez mais expressivos, especialmente após a promulgação do Marco Civil da *Internet*[75], cuja norma regulamentadora, o Decreto nº 8.771/16[76], trouxe diversas diretrizes sobre os padrões de segurança a serem seguidos pelos provedores de conexão e de aplicações na *internet*.

---

[74] Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC. **CNIL**. Disponível em: <https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc>. Acesso em: 28/01/2021.

[75] BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

[76] Idem. **Decreto nº 8.771, de 11 de maio de 2016**. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.

O Banco Central do Brasil (BCB) também editou a Resolução nº 4.658/18[77], prevendo medidas para a segurança cibernética no âmbito das instituições financeiras.

Não diferentemente, a LGPD também trouxe diversas disposições específicas atinentes à segurança da informação, vide os artigos 46 a 49 da própria Lei, que tratam da segurança e do sigilo dos dados pessoais.

Desta forma, é recomendável que a empresa mantenha documentadas todas as medidas técnicas de segurança que foram tomadas internamente, o que pode ser feito através do estabelecimento de políticas e normativas internas, treinamentos de funcionários e campanhas de conscientização.

9. Prevenção

De maneira complementar ao princípio da segurança, as empresas devem agir para prevenir a ocorrência de incidentes, e não apenas para mitigá-los. Esta é a lógica por traz de todo o arcabouço jurídico relativo ao *compliance*: o reconhecimento pelas empresas de que é preferível cooperar com as autoridades e seguir a legislação a agir

[77] BRASIL. **Resolução BCB nº 4.658/18**. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

na reparação de danos com o pagamento de pesadas multas e indenizações.

Desta forma, é recomendável que os agentes de tratamento se atentem às questões sobre privacidade e proteção de dados desde a concepção de quaisquer novos produtos ou serviços, conforme aduz o conceito de *privacy by design*.

Nesse sentido, ressalta-se a relevância do DPO, vez que será essencial na efetivação do princípio da prevenção, tendo em vista que tem o papel de orientar os funcionários e ajudar na elaboração de relatórios de impacto à proteção de dados pessoais (RIPD).

10. Não-discriminação

O princípio da não-discriminação está intimamente ligado com o princípio da igualdade material, vedando que as pessoas tenham qualquer tipo de tratamento discriminatório com base em seus dados pessoais. Tal princípio é importante frente ao crescimento da utilização de algoritmos e de inteligência artificial, que por realizarem decisões automáticas, por muitas vezes acabam por refletir os vieses de seus criadores, o que é especialmente verdade se realizados recortes de classe e raça[78].

[78] HEILWEIL. Rebecca. Why algorithms can be racist and sexist. **VOX**, 2020. Disponível em: <https://www.vox.com/recode/2020/2/18/21121286/algorithms-bias-discrimination-facial-recognition-transparency>. Acesso em 29/01/2020.

Ressalte-se que algum nível de discriminação pode ser considerado lícito, mas apenas para a própria efetivação do princípio da isonomia, ou seja, naqueles casos em que é necessário tratar os desiguais de maneira desigual, na medida de sua desigualdade. É o caso de uma companhia aérea que necessite identificar os passageiros que possuem alguma restrição alimentar, para que possa assim servi-los com segurança.

11. Prestação de contas

A positivação da responsabilização e a prestação de contas como um princípio da LGPD serve de alerta para os agentes de tratamento, tendo em vista que a legislação busca deixar claro que os agentes serão devidamente responsabilizados se não entrarem em conformidade com a norma.

Por conseguinte, os controladores e operadores deverão tomar medidas que tornem os seus sistemas de segurança facilmente auditáveis por agentes internos e externos, bem como se dispor a ser amplamente transparentes com as autoridades na ocorrência de qualquer incidente de segurança da informação.

CAPÍTULO II - DO TRATAMENTO DE DADOS PESSOAIS

Seção I - Dos Requisitos para o Tratamento de Dados Pessoais

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019)

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

§ 1º (Revogado). (Redação dada pela Lei nº 13.853, de 2019)

§ 2º (Revogado). (Redação dada pela Lei nº 13.853, de 2019)

§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.

§ 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

§ 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos

legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei. (Incluído pela Lei nº 13.853, de 2019)

1. Hipóteses de tratamento

As hipóteses de tratamento legal dos dados dos titulares perfazem uma das disposições mais importantes da LGPD, pois legitimam o tratamento dos dados pessoais. Neste sentido, estas bases legais devem ser atentamente observadas, a fim de evitar quaisquer dissabores aos agentes de tratamento.

É importante também frisar que, diferentemente do senso comum, o consentimento é, para a LGPD, apenas uma dentre dez bases legais de tratamento.

Conforme já comentado, a criação destas outras bases foi um grande salto legislativo com relação ao Marco Civil da *Internet*, que possibilitava em seu art. 7º, inciso VII[79], o tratamento de dados pessoais apenas com base no consentimento.

[79] BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Art. 7º: O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: [...] VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei.

2. Consentimento

O consentimento é a primeira base legal citada no art. 7º da Lei. Entretanto, desde a década de 70, com a transformação tecnológica cada vez mais acelerada, o consentimento vem sofrendo uma ressignificação em seu escopo, sendo considerado cada vez mais insuficiente e falho para a efetivação da proteção dos dados pessoais contra formas de tratamento consideradas abusivas ou discriminatórias[80].

De fato, o consentimento deixou de ser uma simples manifestação de vontade para se tornar livre, informado, e inequívoco, conforme disposto na definição do art. 5º, inciso XII da LGPD.

Assim, para que o consentimento seja "livre", a sua recusa pelo titular não pode ensejar qualquer tipo de consequência negativa, sob pena de ser considerado ilícito. Em outras palavras, um determinado aplicativo que solicite que o titular "consinta" em oferecer uma quantidade maior de dados do que realmente necessite, apenas para que o usuário possa ter acesso ao aplicativo, poderá ser considerado abusivo nas circunstâncias do caso concreto[81].

Para que o consentimento seja "informado", devem ser dispostas as condições de tratamento de forma clara e simples ao titular,

---

[80] LIMA, Cíntia Rosa Pereira de Lima. Consentimento inequívoco *versus* expresso: o que muda com a LGPD?. **Revista do Advogado**. São Paulo, n. 144, nov. 2019. p. 62.
[81] BIONI, Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento. 2ª ed. Rio de Janeiro: Forense, 2018. p. 128.

adequando o termo de consentimento de acordo com o público-alvo, através de textos, vídeos e infográficos, em língua portuguesa, visando dar a maior compreensão possível ao titular.

Por sua vez, para que seja "inequívoco", o consentimento deve abarcar uma demonstração proativa do titular de dados, sendo vedadas opções pré-marcadas ou a aceitação pelo mero silêncio do indivíduo.

O consentimento deve ser especialmente observado nas relações trabalhistas, tendo em vista que o empregador e o empregado estão em uma relação assimétrica, que pode macular esta finalidade de tratamento. Assim, é recomendado que se utilize alguma das outras bases legais para o tratamento de dados de empregados, tendo em vista que o consentimento pode ser considerado ilegítimo, com todas as consequências daí advindas.

O consentimento deve também ser disposto, o máximo possível, de maneira "granular", possibilitando ao titular consentir ou não para cada finalidade específica de tratamento de seus dados, sob pena de ser considerado inválido, garantindo assim a transparência e a boa-fé necessárias nessa relação[82].

[82] LIMA, Caio César Carvalho. Capítulo II – Do Tratamento de Dados Pessoais. MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). **LGPD** – Lei Geral de Proteção de Dados – Comentada. 2ª ed. São Paulo: Revista dos Tribunais, 2019. pp. 182-183.

Em suma, é recomendável que o controlador crie um sistema de gerenciamento do consentimento, para que possa demonstrar sua boa-fé em caso de ações judiciais ou fiscalizações.

3. Cumprimento de obrigação legal ou regulatória

Na existência de uma determinação legal ou regulamentar, o controlador poderá realizar operações de tratamento com base nesta hipótese legal. É o caso do tratamento de dados pessoais de empregados, como para o preenchimento de fichas de registro [83] e entrega de obrigações acessórias do e-Social [84], do FGTS e da Previdência Social[85], dentre outras obrigações. Também é o caso de tratamento de dados pessoais de consumidores, como para a geração de

[83] BRASIL. **Consolidação das Leis do Trabalho**, 1943. Art. 41: Em todas as atividades será obrigatório para o empregador o registro dos respectivos trabalhadores, podendo ser adotados livros, fichas ou sistema eletrônico, conforme instruções a serem expedidas pelo Ministério do Trabalho.

[84] Idem. **Decreto nº 8.373, de 11 de dezembro de 2014.** Institui o Sistema de Escrituração Digital das Obrigações Fiscais, Previdenciárias e Trabalhistas - eSocial e dá outras providências. Art. 2º: O eSocial é o instrumento de unificação da prestação das informações referentes à escrituração das obrigações fiscais, previdenciárias e trabalhistas e tem por finalidade padronizar sua transmissão, validação, armazenamento e distribuição, constituindo ambiente nacional composto por: I - escrituração digital, contendo informações fiscais, previdenciárias e trabalhistas; [...]

[85] Idem. **Lei nº 8.212, de 24 de julho de 1991**. Dispõe sobre a organização da Seguridade Social, institui Plano de Custeio, e dá outras providências. Art. 32: A empresa é também obrigada a: [...]

IV – declarar à Secretaria da Receita Federal do Brasil e ao Conselho Curador do Fundo de Garantia do Tempo de Serviço – FGTS, na forma, prazo e condições estabelecidos por esses órgãos, dados relacionados a fatos geradores, base de cálculo e valores devidos da contribuição previdenciária e outras informações de interesse do INSS ou do Conselho Curador do FGTS;

notas fiscais[86] e de tratamento de registros de conexão por provedores de conexão à *internet*[87].

4. Pela Administração Pública

A administração pública é regida pelo princípio da legalidade, ou seja, apenas pode atuar balizada em uma disposição legal. A LGPD define um capítulo inteiro, o Capítulo IV, para o tratamento de dados envolvendo a execução de políticas de interesse público, relacionadas principalmente com a educação, cultura, saúde, desenvolvimento econômico, dentre outros.

O inciso III do art. 7º é omisso nas disposições em que a Administração Pública necessite tratar dados pessoais para realizar suas próprias funções, como por exemplo no gerenciamento de recursos humanos. Alguns autores afirmam que, para solucionar esta questão, deve-se valer da leitura do art. 23 da LGPD, não havendo outras bases de tratamento possíveis de serem aplicadas ao poder público[88].

---

[86] BRASIL. **Lei nº 8.846, de 21 de janeiro de 1994**. Dispõe sobre a emissão de documentos fiscais e o arbitramento da receita mínima para efeitos tributários, e dá outras providências. Art. 1º: A emissão de nota fiscal, recibo ou documento equivalente, relativo à venda de mercadorias, prestação de serviços ou operações de alienação de bens móveis, deverá ser efetuada, para efeito da legislação do imposto sobre a renda e proventos de qualquer natureza, no momento da efetivação da operação.

[87] Idem. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

[88] WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo Poder Público. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo

Entretanto, o art. 7º, inciso II da Lei, que trata da hipótese de tratamento por obrigação legal ou regulamentar, oferece uma solução a esta problemática, possibilitando que a Administração Pública trate dados pessoais não só para a execução de políticas públicas, mas também para o cumprimento de suas atribuições ou competências legais. Ou seja, se bem observado o disposto no inciso II não faz qualquer menção de que esta hipótese de tratamento deva ser utilizada apenas por entes privados, possibilitando a utilização desta base pela Administração Pública.

Passadas estas considerações, é certo que todos os entes da administração direta e indireta, em todos os níveis da federação, terão que se adequar à LGPD, utilizando-se também das disposições do Capítulo IV, salvo para as hipóteses de tratamento contidas no art. 4º da Lei, que serão objeto de normativa própria[89].

Wolfgang; RODRIGUES JR., Otávio Luiz (orgs). **Tratado de Proteção de Dados Pessoais**. 1º ed. Rio de Janeiro: Forense, 2021. p. 280: "O deslinde dessa questão se dá pela leitura do art. 23 da LGPD, que estabelece a hipótese complementar dos arts. 7º e 11 o objetivo de 'executar as competências legais ou cumprir as atribuições legais do serviço público".

[89] Já existe, no âmbito da Câmara dos Deputados, um Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal, elaborado pelo Grupo de Trabalho da Comissão de Juristas (Dados Pessoais/ Segurança Pública). A íntegra do Anteprojeto se encontra disponível em: < https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf >. Acesso em: 06/01/2020.

5. Órgãos de pesquisa

A base legal de tratamento para a realização de estudos por órgão de pesquisa deve respeitar a delimitação do conceito contido no art. 5º, inciso XVIII da LGPD, sendo recomendado o tratamento com os dados anonimizados, conforme disposições do art. 12 da Lei.

Alguns exemplos incluem pesquisas eleitorais ou pesquisas de opinião, que podem ser analisadas de forma agregada e sem identificar os indivíduos, ou seja, compõem uma análise quantitativa dos dados. Entretanto, a lei não proíbe que sejam realizadas análises qualitativas com dados pessoais, que são análises que envolvem diretamente a identificação dos titulares[90].

6. Execução de contrato

O contrato e os seus procedimentos preliminares perfazem a base legal do inciso V do art. 7º. Trata-se de um acordo de vontades entre duas ou mais partes, podendo dispor sobre qualquer matéria que não seja manifestamente ilegal[91], podendo ser escritos ou verbais, expressos ou tácitos, e sob qualquer forma não vedada em lei.

[90] BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. **Revista do Advogado**. São Paulo, n. 144, nov. 2019. p. 25.
[91] BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Art. 425. É lícito às partes estipular contratos atípicos, observadas as normas gerais fixadas neste Código.

Já os procedimentos preliminares relacionados ao contrato envolvem os procedimentos que precedem a contratação, tais como a apresentação das propostas pelas partes, por exemplo.

Em ambas as fases de contratação, pode ser realizado o tratamento de dados pessoais sem o termo de consentimento do titular, desde que necessários para a contratação e que o titular seja uma das partes. Pode-se citar como exemplos desta base legal: (i) o caso de aquisição de um produto pelo titular em uma loja virtual, em que o vendedor deverá conhecer seu endereço para o cálculo do frete; (ii) a consulta a ser realizada por uma instituição financeira antes da concessão de crédito, o que deve se tornar ainda mais relevante com a efetivação do *open banking* no país[92]; e (iii) as análises preliminares de risco por seguradoras, necessárias para a determinação das condições da apólice de seguro[93].

Apesar de se aproximar do consentimento, tendo em vista que o ato de contratar envolve uma manifestação de vontade, esta hipótese se diferencia daquela contida no inciso I do art. 7º, vez que o titular não poderá solicitar a eliminação dos seus dados pessoais ao agente de tratamento, que estará legalmente autorizado a retê-los, enquanto forem necessários para a execução do contrato. Entretanto, nos casos em que

---

[92] SANTOS, Gilmara. Open banking possibilita simplificação dos serviços. **Folha de São Paulo**. Disponível em: <https://www1.folha.uol.com.br/mercado/2020/11/open-banking-possibilita-simplificacao-dos-servicos.shtml>. Acesso em 02.12.2020.

[93] LIMA, Caio César Carvalho. Capítulo II – Do Tratamento de Dados Pessoais. In. MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). **LGPD** – Lei Geral de Proteção de Dados – Comentada. 2ª ed. São Paulo: Revista dos Tribunais, 2019.

não houver a efetivação do negócio jurídico, o controlador deverá exclui-los tão logo se encerre a finalidade para a qual eles foram fornecidos.

A título exemplificativo, no caso de uma proposta de seguro cuja contratação não tenha sido efetivada, a seguradora – que no caso é a controladora – deverá eliminar os dados pessoais, considerando a não consumação da relação jurídica entre as partes.

7. Exercício regular de direitos

A base legal do inciso VI busca proteger os direitos fundamentais da ampla defesa e do contraditório, possibilitando ao agente de tratamento reter determinados dados, se demonstrar que eles servirão como elemento de prova para o exercício de direitos em eventuais demandas judiciais, desde que haja a real necessidade e sejam utilizados somente para esta finalidade específica.

Assim, o agente de tratamento estaria autorizado a reter dados pessoais dos indivíduos, mesmo após o fim do contrato, conforme os prazos prescricionais previstos na legislação, tendo em vista que estes dados poderiam ser necessários em possíveis demandas judiciais.

Tome-se o exemplo da seguradora, acima mencionado: no caso de não ser contratada a apólice, a seguradora poderia reter os dados do titular a partir da base legal mencionada no inciso VI, ou seja, com

a finalidade de constituir prova e se isentar de responsabilidades na ocorrência de um eventual sinistro.

Outro exemplo se daria no âmbito do MCI, em que um provedor de conexão estaria obrigado a reter os registros de acesso a conexões de *internet* pelo prazo de 01 ano, conforme já comentado, retendo-os com base no inciso II do art. 7º da Lei.

Entretanto, o provedor também estará autorizado a reter estes dados por 05 anos, tendo em vista o prazo prescricional previsto no art. 27 do CDC[94], o que passaria a realizar com base neste inciso VI deste artigo. Por fim, caso houvesse algum tipo de litígio judicial, o controlador poderia ainda reter estes dados até o final desta demanda judicial, com base no mesmo inciso[95].

---

[94] BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Art. 27: Prescreve em cinco anos a pretensão à reparação pelos danos causados por fato do produto ou do serviço prevista na Seção II deste Capítulo, iniciando-se a contagem do prazo a partir do conhecimento do dano e de sua autoria.

[95] Idem. Superior Tribunal de Justiça. **Recuso Especial nº 1.398.985 MG 2013/0273517-8**. CIVIL E CONSUMIDOR. INTERNET. RELAÇÃO DE CONSUMO. CDC. INCIDÊNCIA. PROVEDOR DE CONTEÚDO. USUÁRIOS. IDENTIFICAÇÃO. DEVER. GUARDA DOS DADOS. OBRIGAÇÃO. PRAZO. 03 ANOS APÓS CANCELAMENTO DO SERVIÇO. OBTENÇÃO DE DADOS FRENTE A TERCEIROS. DESCABIMENTO. DISPOSITIVOS LEGAIS ANALISADOS: ARTS. 5.º, IV, DA CF/1988; 6.º, III E 17 DO CDC; 206, § 3.º, V, E 1.194 DO CC/2002; E 358, I, DO CPC. [...] 2. Recurso especial que discute a responsabilidade dos gerenciadores de fóruns de discussão virtual pelo fornecimento dos dados dos respectivos usuários. 3. A exploração comercial da Internet sujeita as relações de consumo daí advindas à Lei nº 8.078/90. Precedentes. [...] 6. As informações necessárias à identificação do usuário devem ser armazenadas pelo provedor de conteúdo por um prazo mínimo de 03 anos, a contar do dia em que o usuário cancela o serviço. 7. Não há como exigir do provedor de conteúdo que diligencie junto a terceiros para obter os dados que inadvertidamente tenha apagado dos seus arquivos, não apenas pelo fato dessa medida não estar inserida nas

Por esta razão, é recomendável que os agentes de tratamento tenham normas e políticas que estruturem a retenção dos mais variados tipos de dados pessoais que eventualmente processar, como parte dos procedimentos de adequação à LGPD.

8. Proteção da vida

A base legal contida no inciso VII, por sua vez, busca relativizar a privacidade e a proteção de dados pessoais a fim de proteger a vida. Assim, deverá ser utilizada apenas de forma emergencial, como por exemplo na utilização de dados de geolocalização para encontrar pessoas desaparecidas em meio a escombros de um acidente grave[96].

9. Tutela da saúde

A base legal prevista no inciso VIII visa efetivar o direito fundamental à saúde, previsto no art. 6º da CF[97], e pode ser utilizado

providências cabíveis em sede de ação de exibição de documentos, mas sobretudo porque a empresa não dispõe de poder de polícia para exigir o repasse dessas informações. Por se tratar de medida cautelar de natureza meramente satisfativa, não há outro caminho senão reconhecer a impossibilidade de exibição dos documentos, sem prejuízo, porém, do direito da parte de buscar a reparação dos prejuízos decorrentes da conduta desidiosa. 8. Recurso especial parcialmente provido. (STJ – REsp 1398985 MG 2013/0273517-8, Relator: Ministra Nancy Andrighi, Data de Julgamento: 19/11/2013, T3 – Terceira Turma, Data de Publicação DJe 26/11/2013).

[96] COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais** – Comentada. 3º ed. São Paulo, Revista dos Tribunais, 2019. pp. 88-89.

[97] BRASIL. **Constituição da República Federativa do Brasil**, 1988. Art. 6º São direitos sociais a educação, a saúde, a alimentação, o trabalho, a moradia, o transporte,

tanto por pessoas físicas (profissionais de saúde), quanto por pessoas jurídicas de direito público (autoridades sanitárias que compõem o Sistema Único de Saúde – SUS e o Sistema Nacional de Vigilância Sanitária - SNVS) e de direito privado (serviços de saúde, regulados pela Agência Nacional de Saúde Suplementar – ANS).

10. Interesse legítimo

Por se tratar de um dos incisos mais discutidos pela doutrina e imbuídos de interrogações, o interesse legítimo do controlador ou de terceiro é abordado na análise do art. 10 desta Lei.

11. Proteção do crédito

O tratamento de dados pessoais para a proteção do crédito, base legal contida no inciso X, busca estimular o desenvolvimento econômico e mitigar os riscos inerentes a esta atividade, sendo de interesse público a ampliação de oferta de crédito para o maior número possível de pessoas.

Esta base legal tem relação com a Lei do Cadastro Positivo (Lei nº 14.414/11), que buscou corrigir falhas sistêmicas no sistema de proteção de crédito, possibilitando o cadastro não apenas dos maus pagadores, mas também dos bons pagadores, para que estes fossem beneficiados pelas suas condutas.

---

o lazer, a segurança, a previdência social, a proteção à maternidade e à infância, a assistência aos desamparados, na forma desta Constituição.

12. Dados de acesso público

Os dados de acesso público também se incluem nas proteções conferidas pela LPGD, de acordo com o §3º deste artigo, ou seja, são também protegidos todos os dados pessoais que constam em bases de dados de livre acesso.

Isso é especialmente importante se considerado o potencial de dano de cruzamentos sequenciais de bases de dados públicas, vez que é possível, através deste procedimento, a criação de perfis comportamentais complexos e que revelem inclusive informações sensíveis do indivíduo[98].

Esta disposição reforça a ideia de que a LGPD busca vedar a criação e a utilização de modelos preditivos de comportamento a partir da coleta indiscriminada de dados pessoais, ainda que se faça menção aos segredos industriais e comerciais que podem envolver a utilização de algoritmos para fins de *profilling*, ou seja, para fins e criação de perfis detalhados dos indivíduos.

Entretanto, a concordância expressa com determinados tipos de tratamento e, inclusive, cruzamento de bases de dados, a partir do consentimento em termos de uso, poderia ser uma saída para que possa ser realizado este tipo de tratamento por parte dos controladores.

[98] LIMA, Caio César Carvalho. Capítulo II – Do Tratamento de Dados Pessoais. In: MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). **LGPD** – Lei Geral de Proteção de Dados – Comentada. 2ª ed. São Paulo: Revista dos Tribunais, 2019. p. 187.

13. Dados tornados públicos pelo titular

Já o §4º do art. 7º dispõe que os dados tornados manifestamente públicos pelos titulares dispensam a utilização da base legal do consentimento contido no caput do art. 7º.

A redação deste dispositivo pode causar certa confusão, vez que o consentimento está contido no inciso I do referido artigo, e não no seu *caput*, como se refere o mencionado parágrafo. Tal contradição é ainda mais evidente se observada esta disposição em conjunto com o §5º, que menciona explicitamente o consentimento contido no inciso I do art. 7º da Lei.

Uma outra disposição que causa estranheza é a dispensa do consentimento para estes casos. Trata-se, possivelmente, de um erro de redação legislativa, que dá o entendimento de que nesta hipótese não seria necessário o enquadramento em qualquer outra base legal. Isso apenas faria sentido se fosse considerado que o titular tivesse dado o seu consentimento, de maneira espontânea, quando da disponibilização destes dados.

Independentemente do erro redacional e da confusão oferecida por este parágrafo, deve-se considerar, para a manutenção da harmonia com os princípios previstos na própria LGPD, que a dispensa do consentimento apenas significa que o controlador deverá enquadrar o tratamento em alguma das outras nove bases legais contidas no próprio art. 7º da Lei.

14. Alteração da finalidade dos dados pessoais de acesso público

Ademais, tem-se que as disposições dos §§ 3º e 4º do art. 7º devem ser observadas em conjunto. A partir do momento em que o próprio titular torna públicas as informações sobre si, logo estas informações se tornam de acesso público, e devem também respeitar as disposições do §3º, sobre os dados contidos em bases de acesso público.

Entretanto, não está claro qual seria o escopo de abrangência destes dados pessoais de acesso público, especialmente aqueles dados tornados manifestamente públicos pelos indivíduos através das redes sociais, que podem ser livremente acessadas por qualquer pessoa ou empresa.

Basta notar o famigerado escândalo da Cambridge Analytica, em que houve o aproveitamento de um algoritmo desenvolvido pela Universidade de Oxford e também de brechas nas políticas de compartilhamento de dados do Facebook, para criar perfis de milhões de cidadãos americanos, a fim de identificar quais destes cidadãos estariam mais propensos a acreditar em *fake news*, e assim possibilitar a manipulação deles para fins políticos[99].

Desta forma, o §7º do art. 7º, que trata sobre a mudança de finalidade dos dados referidos nos §§ 3º e 4º, abre uma brecha para este

[99] WONG, Julia Carrie. The Cambridge Analytica scandal changed the world – but it didn't change Facebook. **The Guardian**, 2019. Disponível em: <https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook>. Acesso em: 28/01/2021.

tipo de práticas abusivas pelos agentes de tratamento, nos mesmos moldes do escândalo da Cambridge Analytica, tendo em vista a amplitude de interpretação dos termos utilizados no dispositivo, tais como "os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular". Portanto, expõe sobremaneira os titulares de dados a este tipo de conduta, permitindo que agentes de tratamento mal intencionados se beneficiem desta brecha legislativa.

Tome-se o exemplo de uma incorporadora, que possua uma base de dados dos compradores de terrenos de um novo empreendimento imobiliário em decorrência da necessidade de execução do contrato, sendo a base legal de tratamento aquela contida no art. 7º, inciso V da LGPD.

Caso esta incorporadora desejasse tratar os dados fornecidos para a sua estratégia de marketing, cruzando-os com outras bases de dados de acesso público, poderia realizar este novo tratamento com base no legítimo interesse, disposto no inciso IX do art. 7º.

Nesse caso, a incorporadora poderia entender que não estaria realizando um tratamento ilegal, tendo em vista o seu propósito legítimo e específico para o novo tratamento, ainda que tivesse que se atentar aos princípios dispostos no art. 6º desta Lei, bem como se adequar às disposições específicas dessa base de tratamento, contidas no art. 10.

Diante desta situação é de suma importância que o titular se atente ao tratamento que está sendo realizado e, entendendo que houve

a alteração da finalidade de forma incompatível com as suas expectativas legítimas, opor-se a esta forma de tratamento, com respaldo no art. 18, §2º da Lei[100].

[100] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Art. 18: O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: [...] § 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.

Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.

§ 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

§ 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.

§ 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

§ 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.

§ 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

1. Da forma do consentimento

O art. 8º trata especificamente de disposições acerca do consentimento. Deste modo, seguindo o princípio da boa-fé, este consentimento do titular deve ser coletado de forma que permita uma fácil comprovação, pelo agente de tratamento, de sua efetiva coleta, seja por meio físico (assinatura) ou seja por meio eletrônico (certificado digital, biometria, vídeo).

Também é recomendável que o destaque contratual do consentimento, mencionado no §1º, seja acompanhado de imagens, infográficos ou vídeos que auxiliem o titular a realizar a sua escolha. Inclusive, para os casos em que os textos forem muito longos, é recomendável apresentar ao titular uma síntese de todos os pontos sobre o tratamento de seus dados pessoais, documento que também deve ser assinado pelo titular[101].

[101] COTS, Márcio; OLIVEIRA, Ricardo**. Lei Geral de Proteção de Dados Pessoais** ¬– Comentada. 3º ed. São Paulo, Revista dos Tribunais, 2019. p. 92.

Também, em conformidade com o princípio da adequação, o §4º proíbe qualquer tipo de permissão genérica para o tratamento de dados. O uso de permissões genéricas hoje é muito comum pelos agentes de tratamento, e geralmente incluem disposições como a "utilização de dados pessoais para a melhoria de produtos e serviços" e a "utilização de dados pessoais para a melhoria da experiência do usuário". É recomendável que tais disposições sejam reformuladas nos procedimentos de adequação à LGPD.

2. Da prova do consentimento

É importante que, durante todo o período de retenção de dados pessoais, não importa a finalidade, o controlador mantenha documentação que comprove que obteve o consentimento dos titulares, para que possa constituir provas no caso de surgimento de uma demanda judicial por parte de algum titular ou algum tipo de fiscalização por parte da ANPD.

Da mesma forma, devem ser armazenadas todas as evidências e documentações relacionadas ao fornecimento do consentimento pelo titular, a fim de mitigar riscos judiciais e regulatórios relacionados com os vícios de consentimento previstos em diversos dispositivos do

Código Civil, como o erro[102], o dolo[103], a coação[104], o estado de perigo[105], a lesão[106], a fraude contra credores[107] e a simulação[108].

3. Revogação do consentimento

A revogação do consentimento deve se dar de forma tão simples quanto tenha se dado a sua coleta pelo agente de tratamento, vedando-se qualquer manobra que dificulte esse direito do titular. A revogação também deve se dar de forma gratuita e deve ser passível de ser exigida a qualquer momento.

A revogação do consentimento implica na interrupção imediata do tratamento dos dados do titular após a sua solicitação, os

[102] BRASIL, **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Art. 138: São anuláveis os negócios jurídicos, quando as declarações de vontade emanarem de erro substancial que poderia ser percebido por pessoa de diligência normal, em face das circunstâncias do negócio.
[103] Ibidem. Art. 145: São os negócios jurídicos anuláveis por dolo, quando este for a sua causa.
[104] Ibidem. Art. 151: A coação, para viciar a declaração da vontade, há de ser tal que incuta ao paciente fundado temor de dano iminente e considerável à sua pessoa, à sua família, ou aos seus bens.
[105] Ibidem. Art. 156: Configura-se o estado de perigo quando alguém, premido da necessidade de salvar-se, ou a pessoa de sua família, de grave dano conhecido pela outra parte, assume obrigação excessivamente onerosa.
[106] Ibidem. Art. 157: Ocorre a lesão quando uma pessoa, sob premente necessidade, ou por inexperiência, se obriga a prestação manifestamente desproporcional ao valor da prestação oposta.
[107] Ibidem. Art. 158: Os negócios de transmissão gratuita de bens ou remissão de dívida, se os praticar o devedor já insolvente, ou por eles reduzido à insolvência, ainda quando o ignore, poderão ser anulados pelos credores quirografários, como lesivos dos seus direitos.
[108] Ibidem. Art. 167: É nulo o negócio jurídico simulado, mas subsistirá o que se dissimulou, se válido for na substância e na forma.

quais deverão ser devidamente excluídos, salvo nas hipóteses mencionadas no art. 16 da Lei.

4. Alteração da base legal de tratamento

A redação do §6º pode levar o intérprete a entender que a disposição ali contida deveria ser aplicada a qualquer das bases de tratamento previstas no art. 7º, tendo em vista a colocação, ao final, da disposição de que o referido parágrafo também se aplicaria "nos casos em que o consentimento é exigido". Entretanto, trata-se de outro erro de redação legislativa, tendo em vista a subscrição do referido parágrafo ao art. 8º, que trata de detalhar as disposições acerca da base legal do consentimento, ou seja, tal disposição somente seria válida quando utilizada a base legal do consentimento.

Para realizar estas alterações, entretanto, é recomendável que o agente de tratamento as documente na forma devida, realizando a comunicação ao titular de forma explícita e específica, com destaque para o que foi modificado entre o texto anterior e a nova versão.

5. Uso compartilhado de dados obtidos através do consentimento

O uso compartilhado de dados obtidos através do consentimento necessita de uma interpretação conjunta do §5º do art. 7º e do §6º do art. 8º.

Assim, nos termos do §5º do art. 7º, para que se dê a comunicação ou uso compartilhado dos dados obtidos através do consentimento, é necessário o fornecimento de um consentimento específico por parte do titular.

Entretanto, caso haja alguma alteração nas informações acerca do uso compartilhado de dados, o controlador deverá apenas dar ciência ao titular, que poderá revogar o seu consentimento, conforme a redação deste §6º do art. 8º, em conjunto com o inciso V do art. 9º[109].

Trata-se, pois, de um subterfúgio legal que poderá ser utilizado pelos agentes de tratamento para o compartilhamento de dados obtidos com base no inciso I do art. 7º, driblando a necessidade de obtenção do consentimento específico, disposto no §5º do art. 7º, sendo apenas necessário que o controlador informe esta alteração ao titular.

[109] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: [...] V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade.

Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

I - finalidade específica do tratamento;

II - forma e duração do tratamento, observados os segredos comercial e industrial;

III - identificação do controlador;

IV - informações de contato do controlador;

V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

VI - responsabilidades dos agentes que realizarão o tratamento; e

VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

§ 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não

tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

§ 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

§ 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.

1. Direito de acesso

Os direitos do titular estão mais bem discriminados no Capítulo III da Lei. Entretanto, o artigo 9º busca garantir ao usuário o direito de acesso às informações acerca do tratamento de seus dados pessoais.

Tais informações devem ser fornecidas de forma clara, adequada e ostensiva, tão logo seja estabelecido o contato do titular com o agente de tratamento.

Também devem ser informados o propósito, a forma e a duração do tratamento, ressalvados os segredos comerciais e industriais guardados pela empresa. A proteção destes segredos, por sua vez, deverá obedecer à estratégia geral da empresa, e ser devidamente justificada e documentada.

Em outras palavras, a previsão de proteção aos segredos comerciais e industriais, no caso concreto, não pode ensejar um empecilho à efetivação dos direitos do titular de dados, sob pena de violar os princípios da transparência e do livre acesso.

Entende-se que, com essa disposição, a Lei busca, de forma indireta, coibir a utilização de modelos preditivos de comportamento, tendo em vista que um titular de dados dificilmente ficaria satisfeito com tamanha invasão de sua privacidade criada por essas práticas de mercado.

Nos casos em que existe mais de um agente de tratamento, ou nos casos em que o agente compartilhar ou transferir os dados pessoais do titular, todas as atribuições e responsabilidades devem ser indicadas com a maior transparência possível, havendo também a inclusão da finalidade deste compartilhamento dos dados pessoais.

Logo, todos os demais agentes de tratamento que participarem da operação, sejam eles controladores ou operadores, deverão ser devidamente discriminados pelos controladores, para possibilitar o efetivo controle do titular sobre os seus dados.

2. Nulidade do consentimento

O §1º do art. 9º deixa claro que, caso exista algum vício na manifestação de vontade do titular, o termo de consentimento será considerado nulo, o que tornará o tratamento ilegal e passível de indenização ao titular de dados pessoais. Esta nulidade deverá retroagir ao início do tratamento, ou seja, será integralmente desconsiderado o tratamento realizado pelo controlador.

Tome-se o exemplo em que um controlador inicie o tratamento com determinada finalidade, diga-se, para o envio de uma *newsletter* diária ao titular. Caso altere a finalidade para a criação de um perfil de consumo, sem informar devidamente o titular, o consentimento original será considerado nulo, tão logo seja identificado o vício do negócio jurídico.

O §2º do art. 9º também vem nesta linha e traz uma disposição semelhante ao art. 8º, §6º, pela qual o agente de tratamento deve informar ao titular de dados qualquer alteração de finalidade, situação em que o titular poderá retirar o seu consentimento, caso essa nova finalidade seja incompatível com a original.

3. Condição de fornecimento

Por fim, o §3º do art. 9º enfatiza a necessidade de o controlador demonstrar ao titular a razão do tratamento, além de mencionar os direitos do titular, elencados no art. 18 desta Lei.

Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I - apoio e promoção de atividades do controlador; e

II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

1. Legítimo interesse

O legítimo interesse se presta a possibilitar o tratamento de dados pessoais quando não for possível o tratamento sob nenhuma das outras hipóteses legais. Marca uma importante inovação legislativa, tendo em vista que o ordenamento anterior, calcado no Marco Civil da *Internet*, permitia o tratamento de dados pessoais apenas sob a hipótese do consentimento, conforme já comentado.

Entretanto, por se tratar de uma hipótese muito ampla, o legislador inseriu alguns limites para a sua aplicação pelos agentes de tratamento, condicionando a utilização desta base legal apenas para finalidades legítimas, ou seja, lícitas e morais, e colocando justificativas concretas para o tratamento. Tais disposições buscam vedar a coleta e o processamento indiscriminado de dados pessoais[110].

2. Necessidade de apresentação de um relatório de impacto

A Lei define no §3º do art. 10 que, nas hipóteses de tratamento que tenham base no legítimo interesse, a ANPD poderá solicitar um relatório de impacto à proteção de dados pessoais (RIPD), tendo em vista a elasticidade desta base de tratamento, que pode incluir formas de tratamento potencialmente nocivas à proteção de dados pessoais dos titulares.

[110] BIONI, Bruno Ricardo. Legítimo interesse: aspectos gerais a partir de uma visão obrigacional. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (orgs). **Tratado de Proteção de Dados Pessoais.** 1º ed. Rio de Janeiro: Forense, 2021. p. 172.

Considerando que a ANPD não estipulou um prazo para o atendimento dessa solicitação pelo agente de tratamento, subentende-se que deveria ser realizado de forma imediata, até posterior regulamentação.

Posto isto, é recomendável que o relatório já tenha sido elaborado com todas as informações pertinentes, contendo de forma discriminada as justificativas para a realização do tratamento, as medidas técnicas e administrativas adotadas e o atendimento das legítimas expectativas do titular.

Para auxiliar no entendimento sobre o que constituiria esta base legal do legítimo interesse, o legislador optou por apontar exemplos de operações de tratamento nos incisos do artigo, relacionando esta forma de tratamento seja com as vantagens que podem ser auferidas pelo próprio agente de tratamento, seja com as vantagens que podem ser conferidas ao titular de dados.

Muito embora a hipótese de tratamento de dados pessoais com base no legítimo interesse configure um avanço ao ordenamento jurídico brasileiro, quando analisado o art. 7º, inciso IX, pode-se notar um grande problema, que se dá na menção de que esse tratamento também poderia ocorrer com base no legítimo interesse de terceiro.

Todavia, não restou claro quem seria este sujeito, estranho à relação jurídica estabelecida entre o agente de tratamento e o titular, tampouco se este terceiro seria considerado um agente de tratamento pela Lei, o que pode causar muita insegurança à proteção de dados dos

titulares e acabar por atingir o seu direito de autodeterminação informativa.

Por fim, nas agências europeias de proteção de dados, já existe uma outra situação, desta vez relacionada à realização de um teste de ponderação do legítimo interesse frente às expectativas dos titulares, em um documento que se convencionou chamar "*Legitimate Interest Assessment* - LIA" (Análise do Legítimo Interesse, em tradução livre)[111].

Em um momento futuro, é possível que este tipo de documento seja também solicitado pela autoridade brasileira, tendo em vista a necessidade de impor maiores restrições à natureza subjetiva do legítimo interesse, sendo recomendável, neste meio tempo, que os agentes ajam com total cautela ao invocar esta base legal para o tratamento dos dados que eventualmente possuírem.

[111] BIONI, Bruno Ricardo. Legítimo interesse: aspectos gerais a partir de uma visão obrigacional. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (orgs). **Tratado de Proteção de Dados Pessoais.** 1º ed. Rio de Janeiro: Forense, 2021. p. 175.

Seção II - Do Tratamento de Dados Pessoais Sensíveis

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019)

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

§ 2º Nos casos de aplicação do disposto nas alíneas "a" e "b" do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.

§ 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional,

ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.

§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: (Redação dada pela Lei nº 13.853, de 2019)

I - a portabilidade de dados quando solicitada pelo titular; ou (Incluído pela Lei nº 13.853, de 2019)

II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo. (Incluído pela Lei nº 13.853, de 2019)

§ 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários. (Incluído pela Lei nº 13.853, de 2019)

1. Dados pessoais sensíveis

O tratamento de dados pessoais sensíveis é essencial para a efetivação de diversas categorias de direitos constitucionalmente protegidos, dentre os quais se destacam o direito à saúde (dados genéticos ou sanitários), o direito à liberdade de expressão e comunicação (dados sobre opiniões pessoais), o direito à liberdade religiosa (dados sobre convicção religiosa) e o direito à associação (dados sobre convicções político-ideológicas).

Entretanto, tal tratamento também pode ensejar enormes riscos para os titulares de dados, tendo em vista o potencial discriminatório que estes dados sensíveis podem revelar. Desta forma, faz sentido a legislação prever hipóteses mais restritivas para o tratamento desta categoria de dados, quando comparadas com as hipóteses para os dados pessoais comuns.

2. Consentimento

Da mesma forma que o previsto no art. 7º, inciso I, o consentimento também é uma base legal para o tratamento de dados pessoais sensíveis. Além das qualificações comuns do consentimento, que deve continuar sendo livre, informado e inequívoco, também deve ser realizado de forma específica e informado de forma destacada ao titular de dados.

Isto significa dizer que as finalidades de tratamento dos dados pessoais sensíveis devem estar especificadas, de forma separada dos demais dados pessoais, e devem ser informadas de forma que chamem a atenção do titular para esta hipótese de tratamento, garantindo ao mesmo o efetivo controle sobre as suas informações.

3. Dispensa de consentimento

Há uma clara correspondência entre as bases legais contidas no art. 7º e no art. 11, o que ocorre com algumas diferenças significativas. Desta forma, as alíneas do inciso II do art. 11 contemplam quase todas as bases legais previstas no art. 7º, com exceção daquelas previstas nos incisos V, IX e X.

3.1. Obrigação legal ou regulamentar

A alínea "a" remete ao inciso II do art. 7º da Lei, ou seja, quando o controlador for obrigado por lei ou alguma outra regulação, terá embasamento legal para o tratamento de dados pessoais sensíveis.

3.2. Execução de políticas públicas

Já a alínea "b" remete ao inciso III do art. 7º da Lei, com a diferença de que os contratos, convênios e instrumentos congêneres, geralmente firmados com entes privados, não serão suficientes para

legitimar o tratamento compartilhado de dados pessoais sensíveis, diferentemente do que ocorre com os dados pessoais não-sensíveis.

Entretanto, nos termos do §2º do art. 11, o Poder Público, quando realizar o tratamento de dados sensíveis para o cumprimento de obrigação legal ou regulatória (alínea "a"), bem como para a execução de políticas públicas (alínea "b"), deverá dar ampla publicidade à dispensa do consentimento, conforme disposto no art. 23, inciso I, que é comentado no próprio artigo. A propósito, o tratamento de dados pessoais pela administração pública se encontra mais bem detalhado no Capítulo IV da Lei.

3.3. Órgãos de pesquisa

A alínea "c" remete ao inciso IV do art. 7º da Lei, sendo recomendado que, nestes casos, os órgãos de pesquisa se atentem ainda mais às medidas de mitigação de riscos, tendo em vista a natureza sensível destas informações.

3.4. Exercício regular de direitos

A alínea "d" possui algumas diferenças cruciais com o disposto nos incisos V e VI do art. 7º, tendo em vista que adiciona o termo "inclusive em contrato" ao rol de possibilidades de tratamento de dados pessoais sensíveis com base no exercício regular de direitos.

Perceba-se que o legislador, ao contrário da disposição do inciso V do art. 7º, não previu a possibilidade de tratamento de dados pessoais sensíveis em procedimentos pré-contratuais, restando apenas a base legal do consentimento para os casos em que for necessário tratar estes dados em um período anterior ao contrato.

Por outro lado, a redação dessa alínea também pode levar o intérprete a concluir que esses procedimentos preliminares estejam inseridos no "exercício regular de direito", no início da sentença, o que não deixa de ser uma verdade. O fato é que, caso não tenha sido este o real objetivo e interesse do legislador ao redigir esta alínea, isso certamente trará sérios problemas no exercício das atividades de algumas empresas, conforme se demonstra nas situações a seguir:

Considere-se o exemplo de uma pessoa com deficiência física que, querendo adquirir um carro adaptado às suas necessidades, se dirigisse a uma agência de automóveis. Caso a compra não fosse realizada pelo titular, o controlador teria realizado, em tese, um tratamento ilegal de dados pessoais sensíveis.

Outro exemplo seria o de uma loja direcionada ao público evangélico, que tivesse uma política de optar pela contratação de funcionários que também seguissem aquela determinada religião. Diante dessa situação, seria necessário que a loja realizasse um tratamento prévio destes dados pessoais sensíveis, a fim de identificar e selecionar pessoas com este perfil. Desta maneira, para os casos em

que os candidatos não forem selecionados, logo o controlador teria também realizado um tratamento ilegal desses dados pessoais.

Da mesma forma, considere-se o exemplo de uma grande empresa do setor varejista que decida abrir um programa de *trainee* apenas para candidatos negros. Caso um determinado candidato não seja contratado neste processo seletivo, o controlador acabaria por se encontrar em uma situação em que estaria realizando um tratamento ilegal destes dados pessoais sensíveis.

Estes exemplos buscam elucidar o embaraço que se criou com a supressão, no rol do art. 11 da Lei, daquelas disposições acerca dos procedimentos pré-contratuais. Consequentemente, tem-se que um controlador de boa-fé, ao menos teoricamente, poderia ser multado ou condenado a pagar pesadas indenizações por ter realizado tratamentos ilegais de dados pessoais sensíveis, caso não tivesse coletado o consentimento prévio dos titulares, o que em muitas situações inviabilizaria o negócio ou a operação de tratamento.

Tendo em vista a inviabilidade do termo de consentimento dos titulares em tratamentos preliminares, ainda que o objetivo do legislador não seja impedir determinadas operações, existem, entretanto, outras hipóteses preliminares de tratamento de dados sensíveis que ficaram totalmente desamparadas pela Lei.

É o caso de igrejas, cujos trabalhos ministeriais são voluntários, e a escolha e definição de um membro a uma função qualquer ocorre de maneira sigilosa, vez que existe a possibilidade

desse titular (o membro da Igreja, no caso) não ser aprovado para o cargo ou ministério.

Assim, tendo em vista a impossibilidade da coleta do termo de consentimento do titular para o tratamento de informações sensíveis, não teria como se enquadrar em qualquer das outras hipóteses do art. 11.

Ainda, do ponto de vista de impasses no tratamento de dados pessoais sensíveis nas igrejas, há uma outra situação, desta vez relacionada com o atendimento e apoio a pessoas com alguma dificuldade financeira. Mais uma vez o problema se dá em função do sigilo no tratamento das informações, ou seja, enquanto não for aprovado o auxílio a essa pessoa (titular de dados) esta não terá conhecimento da situação, o que inviabiliza o termo de consentimento como solução para o problema.

Na celeuma das igrejas, uma alternativa para estes casos seria a aprovação do PL nº 5.141/19 que, se aprovado, dispensaria o tratamento de dados para fins religiosos, inserindo-o junto com os fins jornalísticos, artísticos e acadêmicos do art. 4º, inciso II da LGPD. No entanto, isso poderia causar desproteção aos titulares, vez que agentes de tratamento mal-intencionados poderiam se escorar nessa nova hipótese de dispensa, alegando que tais tratamentos teriam sido realizados para fins religiosos[112]. Uma alternativa para solucionar esse

[112] O referido Projeto de Lei se encontra em discussão em uma Comissão da Câmara dos Deputados. Informação disponível em:

imbróglio seria dispor que esses tratamentos para fins religiosos ocorressem apenas no âmbito das igrejas.

Semelhantemente ao que ocorre nas igrejas, é possível encontrar este tipo de situação em outros setores, como no caso de uma empresa que, visando reafirmar seu compromisso com políticas afirmativas de igualdade racial, buscasse selecionar pessoas negras para alguns cargos de liderança, o que certamente faria de forma sigilosa, a fim de evitar possíveis especulações ou constrangimentos dentro da instituição.

Entretanto, tendo em vista a inexistência de outras bases de tratamento, a exemplo daquela prevista no inciso IX do art. 7º, esta empresa não poderia fazer este tipo de tratamento de forma sigilosa, e estaria obrigada a colher o consentimento dos titulares para que estivesse adequada à LGPD.

Diante destas considerações, é recomendável que os controladores tenham máxima cautela ao coletar quaisquer informações que possam revelar a natureza sensível de dados de titulares, e se atentem ao fornecimento de termos de consentimento quando não identificarem outra base legal de tratamento destes dados.

<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2244082>. Acesso em: 29/01/2021.

Já nos pontos em que o tratamento através do consentimento não for possível, espera-se que haja uma adequação legislativa ou um pronunciamento breve da ANPD.

3.5. Proteção da vida e tutela da saúde

Nas alíneas "e" e "f", de forma respectiva, se repete o que está disposto nos incisos VII e VIII do art. 7º da Lei. Entretanto, não está claro qual o escopo destes procedimentos de saúde mencionados na alínea "f".

Considere-se o exemplo de um casal que esteja em uma relação homoafetiva e, procurando ter um filho, procure uma clínica de reprodução humana assistida. Não está claro se a clínica estaria autorizada a tratar os dados sensíveis sobre a sexualidade e sobre a intenção destes titulares de terem um filho com base na alínea "f" do inciso II, tendo em vista que, até a coleta, não teria sido realizado nenhum procedimento relacionado à saúde deles.

Poder-se-ia aventar a possibilidade de tratamento com base legal no consentimento até que fosse efetivamente iniciado o procedimento de reprodução assistida, o que não deixaria de gerar inseguranças aos agentes de tratamento, tendo em vista a natureza delicada do consentimento no âmbito da proteção de dados.

3.6. Prevenção a fraudes e segurança do titular

A alínea "g" dispõe que dados pessoais sensíveis podem ser utilizados para fins específicos de prevenção a fraudes e para a própria segurança do titular, como por exemplo o recolhimento de dados biométricos (digitais) dos titulares para o acesso a um sistema bancário.

Outro exemplo de uso da biometria está nos sistemas de controle e autenticação de acesso utilizados por condomínios, empresas e hospitais, os quais buscam proteger não só a segurança dos titulares, mas também de todos os demais ativos da instituição.

4. Compartilhamento de dados pessoais sensíveis

O compartilhamento e a comunicação de dados pessoais sensíveis com o objetivo de obtenção de vantagens econômicas perfaz, atualmente, uma parte crucial da economia da informação, vez que é utilizado pelos agentes de tratamento para a criação de modelos preditivos de comportamento dos titulares, o que é realizado, por sua vez, através de instrumentos de análise de *Big Data*[113].

Nesse sentido, conforme interpretação que se dá ao §1º do art. 11, é possível que sejam considerados sensíveis aqueles dados resultantes do uso compartilhado de dados pessoais entre agentes de tratamento, caso estes resultados revelem qualquer tipo de informação

[113] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 2ª ed. Rio de Janeiro: Forense, 2018. pp. 26-27.

sensível dos titulares que seja capaz de lhes causar danos. Ainda, tendo em vista que este uso compartilhado de dados poderia se revelar nocivo aos direitos dos titulares, o §3º asserta que a ANPD poderá vedar ou regulamentar estas operações em um momento futuro.

Buscando ilustrar a situação acima descrita, pode-se citar o exemplo de uma empresa de transporte por aplicativo que, ao cruzar os dados referentes à geolocalização dos usuários com parâmetros previamente estabelecidos, poderia atribuir a esses titulares informações como a sua orientação sexual ou religiosa.

Havendo uma conduta desta espécie por parte do agente de tratamento, tal fato seria considerado uma grave violação de dados pessoais, o que poderia lhe acarretar diversos danos reputacionais e econômicos, além de dar ensejo a vultuosas indenizações e multas. Esta forma específica de tratamento só seria possível caso o agente de tratamento tivesse solicitado o consentimento do titular, segundo a base legal do art. 11, inciso I desta Lei.

Outra conduta que deve ser observada, principalmente com relação às empresas de transporte por aplicativo, é a criação de políticas que exijam o sigilo por parte dos seus motoristas contratados. Neste contexto, a título de exemplificação, imagine-se a situação em que um famoso ator, casado, utilize o aplicativo para o levar até um encontro extraconjugal. Caso o motorista reconheça o indivíduo e divulgue esta informação a terceiros, a empresa poderá ser demandada judicialmente pelo titular e responsabilizada, caso comprovada a sua culpa.

Daí a importância de serem realizadas campanhas de conscientização sobre a privacidade dos titulares, além das demais medidas de *compliance* com a proteção de dados[114].

4.1. Dados sensíveis no setor da saúde

Já o §4º busca impor limitações específicas ao compartilhamento de dados sensíveis atinentes à saúde dos titulares que tenham por objeto a obtenção de vantagens econômicas, entendendo-se como vantagens inclusive aquelas que não tenham caráter estritamente monetário[115].

Entretanto, excetuam-se a essa proibição as operações que, de alguma forma, possam trazer benefícios aos titulares de dados, possibilitem a portabilidade de dados do titular com o seu consentimento, ou possibilitem a própria prestação do serviço de saúde.

No mesmo sentido, no §5º é possível observar a positivação da Súmula Normativa nº 27, de 10 de junho de 2015, da Agência Nacional de Saúde Suplementar (ANS)[116], a qual dispõe que: "É vedada

[114] MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. **Revista do Advogado**. São Paulo, n. 144, nov. 2019. p. 49.
[115] LIMA, Caio César Carvalho. Capítulo II – Do Tratamento de Dados Pessoais. In. MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). **LGPD** – Lei Geral de Proteção de Dados – Comentada. 2ª ed. São Paulo: Revista dos Tribunais, 2019. p. 201.
[116] BRASIL. **Súmula Normativa ANS nº 27, de 10 de junho de 2015**. "É vedada a prática de seleção de riscos pelas operadoras de plano de saúde na contratação de qualquer modalidade de plano privado de assistência à saúde. Nas contratações de planos coletivo empresarial ou coletivo por adesão, a vedação se aplica tanto à

a prática de seleção de riscos pelas operadoras de plano de saúde na contratação de qualquer modalidade de plano privado de assistência à saúde".

Portanto, a referida disposição restringe a utilização de análise de riscos baseada em dados de saúde para a contratação, exclusão ou aumento do valor do convênio dos beneficiários. Entretanto, a própria ANS permite que as operadoras realizem esta seleção de forma regulada, tendo em vista a possibilidade de modularem o valor dos planos com a aplicação de carências, de coberturas parciais temporárias e de agravos.

Tal disposição está intimamente relacionada com a privacidade e a proteção de dados dos titulares, vez que os dados sobre a sua saúde poderiam ser facilmente manipulados pelas operadoras, resultando em práticas abusivas por parte destes agentes de tratamento.

Considere-se, a título de exemplo, o caso em uma grande rede de farmácias que começasse a fornecer informações sobre os remédios comprados pelos seus clientes a uma determinada operadora de planos de saúde. Esta operadora conseguiria traçar um perfil daquele indivíduo e poderia impor limitações ou mesmo aumentar o valor do plano, o que

totalidade do grupo quanto a um ou alguns de seus membros. A vedação se aplica à contratação e exclusão de beneficiários". Disponível em: <http://www.ans.gov.br/component/legislacao/?view=legislacao&task=PDFAtualizado&format=raw&id=Mjk5NA==>. Acesso em 02.12.2020.

atacaria de forma frontal os direitos do titular como consumidor e o seu direito constitucional de acesso à saúde[117].

[117] LIMA, Caio César Carvalho. Capítulo II – Do Tratamento de Dados Pessoais. In. MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). **LGPD** – Lei Geral de Proteção de Dados – Comentada. 2ª ed. São Paulo: Revista dos Tribunais, 2019. p. 202.

Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

§ 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

§ 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.

A Lei deixa claro que os dados anonimizados não são considerados dados pessoais. Estes tipos de dados são utilizados majoritariamente quando o controlador deseja obter informações para fins estatísticos, sem necessariamente precisar identificar o titular, como no caso em que o proprietário de uma loja de calçados faz um

levantamento dos produtos comprados em um determinado mês para saber quais as marcas seriam as mais consumidas por seus clientes.

Entretanto, os dados anonimizados utilizados para a criação de perfis de comportamento devem ser considerados como dados pessoais, caso possibilitem a reidentificação do indivíduo dentro da instituição. Por esta razão, é recomendável que se proceda com a anonimização dos dados por agentes externos à organização, a fim de diminuir os riscos internos de "reidentificação" dos dados anonimizados, tendo em vista a possibilidade de cruzamentos com outras bases de dados que possibilitem a identificação do titular[118].

Caso não seja possível a terceirização da operação de anonimização dos dados, devem ser tomadas medidas adicionais de proteção, avaliando, sobretudo, a natureza dos dados e os riscos que podem trazer aos titulares. Isto posto, é de grande valia o §3º do artigo 12, que prevê que a ANPD poderá agir no estabelecimento de padrões técnicos para a anonimização dos dados, o que decerto acontecerá para que os agentes de tratamento possam usufruir de maior segurança jurídica.

Entretanto, deve-se ressaltar que, na hipótese de ocorrência de algum tipo de fiscalização pela autoridade nacional, caso ela consiga proceder com a reversão do processo de anonimização, utilizando-se de

[118] LIMA, Caio César Carvalho. Capítulo II – Do Tratamento de Dados Pessoais. In. MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). **LGPD** – Lei Geral de Proteção de Dados – Comentada. 2ª ed. São Paulo: Revista dos Tribunais, 2019. p. 204.

esforços razoáveis e de acordo com as tecnologias disponíveis, o agente de tratamento poderá ser penalizado por estar infringindo a legislação.

Como se pode notar, o §1º do artigo 12 dispõe sobre o que seriam esses "esforços razoáveis" na anonimização dos dados por parte do agente de tratamento, tendo em vista que nenhum método de anonimização pode ser considerado 100% eficaz[119].

Ainda que já mencionado, a título de curiosidade, Pesquisadores da Universidade do Texas, por exemplo, conseguiram identificar os usuários de uma base de dados anonimizada da Netflix, contendo apenas a data e a nota das avaliações dos filmes presentes em seu catálogo, a partir de informações públicas acessíveis no site do IMDB[120].

Daí a importância de uma definição de parâmetros de anonimização pela ANPD, a fim de fornecer subsídios para o tratamento desses dados de forma mais segura pelos agentes de tratamento, além de prover uma salvaguarda contra possíveis indenizações por parte dos titulares.

Enquanto não há tal regulação, é recomendável que os agentes de tratamento tomem o máximo de cuidado nos procedimentos de

---

[119] COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais** ¬– Comentada. 3º ed. São Paulo, Revista dos Tribunais, 2019. p. 118.

[120] NARAYANAN, Arvind. SHMATIKOV, Vitaly. **Robust De-anonymization of Large Sparce Datasets**. The University of Texas at Austin, 2008. p. 6. Disponível em < https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf >. Acesso em 29/12/2020.

anonimização dos dados pessoais, tendo em vista a sua fragilidade frente ao avanço cada vez maior das técnicas de inversão destes tipos de procedimento.

Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

§ 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais.

§ 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro.

§ 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.

§ 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um

indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

O art. 13 da Lei possui eficácia contida, pois o próprio acesso pelos órgãos de pesquisa aos dados de saúde dos titulares, nos termos do §3º, será objeto de regulamentação posterior pela ANPD e das demais autoridades sanitárias que compõem o Sistema Único de Saúde – SUS[121].

O artigo também sugere que o tratamento, no mínimo, seja feito com os dados pseudonimizados, e que não poderão ser transferidos pelo órgão de pesquisa a terceiros, em hipótese alguma.

A pseudonimização também é tratada pela primeira vez de forma direta pela legislação neste artigo, sendo definida como o processo que retira a associação de um dado a determinado indivíduo, mantendo-o em outra base de dados separada e protegida, tendo em vista a consideração de que alguém que detenha o algoritmo de

[121] BRASIL. **Lei nº 8.080, de 19 de setembro de 1990.** Dispõe sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes e dá outras providências. Art. 4º: O conjunto de ações e serviços de saúde, prestados por órgãos e instituições públicas federais, estaduais e municipais, da Administração direta e indireta e das fundações mantidas pelo Poder Público, constitui o Sistema Único de Saúde (SUS).
§ 1º Estão incluídas no disposto neste artigo as instituições públicas federais, estaduais e municipais de controle de qualidade, pesquisa e produção de insumos, medicamentos, inclusive de sangue e hemoderivados, e de equipamentos para saúde.

anonimização consiga reverter esse processo e, assim, consiga "reidentificar" um indivíduo[122].

[122] LIMA, Caio César Carvalho. Capítulo II – Do Tratamento de Dados Pessoais. In. MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). **LGPD** – Lei Geral de Proteção de Dados – Comentada. 2ª ed. São Paulo: Revista dos Tribunais, 2019. p. 208.

Seção III - Do Tratamento de Dados Pessoais de Crianças e de Adolescentes

Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

§ 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.

§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.

§ 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo

em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

§ 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.

§ 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

1. Tratamento de dados de crianças e adolescentes

Conforme disposto no Estatuto da Criança e do Adolescente – ECA, considera-se criança a pessoa com até 12 (doze) anos incompletos, e adolescente a pessoa que possui entre 12 (doze) e 18 (dezoito) anos incompletos. O ECA também dispõe que, no caso de interesses conflitantes, deve-se considerar a condição especial da criança e do adolescente como pessoas em desenvolvimento, o que

pode conflitar de maneira frontal com os interesses dos agentes de tratamento[123].

Portanto, faz sentido o estabelecimento de um regramento próprio de proteção de dados de crianças e adolescentes, tendo em vista que ainda são seres humanos em formação e não possuem o discernimento necessário para tomarem decisões acerca de seus dados pessoais[124].

Importante ressaltar que a ANPD possivelmente atuará em conjunto com o Conselho Nacional dos Direitos da Criança e do Adolescente (CONANDA), além de outros órgãos públicos, para uma melhor regulamentação desta normativa presente no art. 14[125].

---

[123] BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Art. 6º: Na interpretação desta Lei levar-se-ão em conta os fins sociais a que ela se dirige, as exigências do bem comum, os direitos e deveres individuais e coletivos, e a condição peculiar da criança e do adolescente como pessoas em desenvolvimento.

[124] HENRIQUES, Isabela; PITA, Marina; HARTUNG Pedro. A proteção de dados pessoais de crianças e adolescentes. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (orgs). **Tratado de Proteção de Dados Pessoais**. 1º ed. Rio de Janeiro: Forense, 2021. p. 200.

[125] BRASIL. **Lei nº 8.242, de 12 de outubro de 1991.** Cria o Conselho Nacional dos Direitos da Criança e do Adolescente (Conanda) e dá outras providências. Art. 2º: Compete ao Conanda:

I - elaborar as normas gerais da política nacional de atendimento dos direitos da criança e do adolescente, fiscalizando as ações de execução, observadas as linhas de ação e as diretrizes estabelecidas nos arts. 87 e 88 da Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente);

II - zelar pela aplicação da política nacional de atendimento dos direitos da criança e do adolescente; [...]

2. Consentimento no tratamento de dados de crianças e adolescentes

O §1º do art. 14 prevê que, para a realização do tratamento de dados pessoais de crianças, ou seja, pessoas com até 12 anos incompletos, este só será realizado com a obtenção do consentimento de algum dos seus pais ou responsáveis legais.

Este consentimento deverá ser obtido de forma específica e em destaque, assim como o consentimento necessário para o tratamento de dados pessoais sensíveis disposto no art. 11, inciso I da Lei, podendo-se inferir uma equiparação legal entre os dados pessoais de crianças e os dados pessoais sensíveis. Assim, aconselha-se que os procedimentos nas tratativas de dados pessoais de menores de 12 anos sejam semelhantes àqueles previstos para os dados pessoais sensíveis.

Ressalte-se que os adolescentes, diferentemente das crianças, apenas foram mencionados no *caput* do art. 14, sem qualquer disposição específica para as suas particularidades. Assim, o consentimento dos pais poderia ser considerado facultativo nestes casos, por ausência expressa de disposição legal em contrário.

Entretanto, é relevante sugerir uma interpretação extensiva deste §1º, equiparando-se os dados pessoais de adolescentes a dados pessoais sensíveis, considerando a sua posição de vulnerabilidade, contemplada no próprio Estatuto da Criança e do Adolescente[126].

[126] "Pode-se dizer, a propósito, tendo-se em vista o mencionado tratamento legal, que para fins de direito, os dados pessoais de crianças e adolescentes serão sempre considerados sensíveis [...]". HENRIQUES, Isabela; PITA, Marina; HARTUNG

Para tal, seria necessário realizar uma remissão ao §1º do art. 11, pelo qual os dados pessoais de adolescentes poderiam ser considerados sensíveis, tendo em vista o dano em potencial que tal tratamento poderia lhes causar. Esta parece ser a posição mais coerente com a intenção do legislador, esperando-se, no entanto, que a ANPD se manifeste a respeito em um futuro próximo.

Tecidas estas considerações, embora seja louvável esta intenção do legislador em permitir o tratamento de dados pessoais de crianças e adolescentes apenas sob a base do consentimento dos pais ou responsáveis legais, tal situação poderá gerar uma celeuma, tanto para os agentes públicos quanto privados.

Tome-se o caso de uma escola, a qual não poderia tratar os dados dos seus alunos sem o consentimento prévio dos respectivos pais ou responsáveis legais, mesmo que para o cumprimento das suas obrigações legais enquanto instituição de ensino ou para a execução do próprio contrato de prestação de serviços. Caso estes pais se recusassem em consentir, ou pior, retirassem o consentimento no meio do período letivo, a escola não teria escolha senão interromper o tratamento destes dados.

Neste mesmo sentido, a realização de consultas médicas de rotina também restaria prejudicada, caso os pais ou responsáveis legais

---

Pedro. A proteção de dados pessoais de crianças e adolescentes. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (orgs). **Tratado de Proteção de Dados Pessoais**. 1º ed. Rio de Janeiro: Forense, 2021. p. 214.

decidissem por retirar o consentimento no decorrer de um procedimento médico, por exemplo.

Tal situação também se repete para as mais variadas categorias de empresas, naqueles casos em que os empregadores tiverem que tratar os dados dos dependentes dos seus empregados para o cumprimento de obrigações legais, tais como o pagamento de salário-família, ou o pagamento de pensão alimentícia. Nestas situações, caso o funcionário se recusasse em consentir com o tratamento dos dados de seu filho para receber o salário integral, sem os descontos da pensão, o empregador não poderia se opor e teria que interromper o tratamento dos dados daquela criança, situação que poderia, inclusive, ensejar uma disputa judicial.

Já a Administração Pública estaria desautorizada a tratar dados de crianças e adolescentes sem o consentimento dos pais ou responsáveis mesmo para a execução de políticas públicas ou para o cumprimento do seu dever legal, o que poderia impedir sobremaneira o exercício da cidadania pelas próprias crianças e adolescentes.

Ainda existe outra questão controversa, tendo em vista que, conforme analisado nos comentários do art. 23, o consentimento no tratamento de dados pela Administração Pública só poderia ser utilizado nas circunstâncias em que o tratamento for facultativo ao titular. Logo, a ausência de possibilidade de tratamento de acordo com outras bases legais acabaria por tornar qualquer forma de tratamento de

dados de crianças e adolescentes pela Administração Pública ilegal, mesmo após o prévio consentimento dos pais ou responsáveis legais.

Uma rápida leitura do art. 14 permite interpretar que o legislador visava atingir situações específicas, relacionadas com a utilização de serviços disponíveis na *internet* por parte das crianças e adolescentes, conforme se depreende da menção expressa a "jogos, aplicações de *internet*" no seu §4º. Entretanto, deixou de visualizar as atividades rotineiras que poderiam prescindir da autorização prévia dos pais ou responsáveis, conforme os exemplos narrados acima, o que acaba por revelar um verdadeiro abismo entre a teoria e a prática na proteção dos dados pessoais.

De todo modo, é certo que a ANPD deverá se pronunciar de maneira aprofundada sobre o art. 14, tendo em vista que esta previsão possibilita um controle por parte dos pais ou responsáveis legais que pode se revelar excessivo e inconstitucional, vez que permitiria que fossem tomadas condutas contra o melhor interesse dos menores de idade, justamente os sujeitos de proteção da referida norma.

3. Forma do consentimento

O §2º do art. 14 busca dar ênfase à forma como este consentimento será informado, devendo essas informações estar amplamente disponíveis aos pais ou responsáveis legais, de forma que eles possam exercer de maneira ampla os direitos do titular previstos no art. 18 da Lei.

Já os §§ 5º e 6º buscam colocar ênfase à transparência na utilização de dados de crianças, exigindo que o controlador realize todos os esforços possíveis para:

(i) comprovar que foram os pais que efetivamente concederam o consentimento; e

(ii) informar de maneira simples, clara e acessível, tanto aos pais ou responsáveis quanto às crianças, sobre a utilização de seus dados, o que poderia ser realizado através de jogos, vídeos e infográficos, dentre outras formas que sejam adequadas às características do receptor destas informações, assim como já ocorre em outras normas que exigem o tratamento específico a determinados grupos, como o Estatuto da Pessoa com Deficiência[127].

Por possuírem uma baixa capacidade de discernimento, as crianças devem ser protegidas de possíveis práticas predatórias que possam ser empregadas por controladores para a obtenção de seus dados.

[127] BRASIL. **Lei nº 13.146, de 6 de julho de 2015**. Institui a Lei Brasileira de Inclusão da Pessoa com Deficiência (Estatuto da Pessoa com Deficiência). Art. 63: É obrigatória a acessibilidade nos sítios da internet mantidos por empresas com sede ou representação comercial no País ou por órgãos de governo, para uso da pessoa com deficiência, garantindo-lhe acesso às informações disponíveis, conforme as melhores práticas e diretrizes de acessibilidade adotadas internacionalmente.

O §4º do art. 14, por exemplo, faz referência aos jogos eletrônicos que, se não monitorados, podem ser uma ampla porta de coleta e utilização abusiva de dados de crianças, o que a Lei visa justamente proteger. Ademais, os controladores devem sempre se atentar ao princípio da necessidade no tratamento de dados de crianças, reduzindo a sua utilização ao mínimo possível.

Apesar dos avanços trazidos por estas disposições da Lei, tem-se que elas ainda não protegem totalmente as crianças e seus responsáveis de algumas condutas que podem ser realizadas por agentes de tratamento mal-intencionados. Tome-se o caso, por exemplo, de um determinado controlador que entrasse em contato com os responsáveis de uma criança para a confirmação do seu consentimento e, nesse processo, angariasse seus dados para utilizá-los em outras finalidades não relacionadas.

Outro exemplo, muito comum inclusive, se dá nos casos em que crianças acessam determinados conteúdos disponíveis na *internet* através dos perfis de usuário de seus pais ou responsáveis.

Assim, o controlador poderia identificar que se trataria de crianças e poderia começar a mostrar propagandas de produtos direcionados ao público infantil, sem necessariamente solicitar previamente o consentimento dos seus pais ou responsáveis, como determina a Lei[128].

[128] HENRIQUES, Isabela; PITA, Marina; HARTUNG Pedro. A proteção de dados pessoais de crianças e adolescentes. In: MENDES, Laura Schertel; DONEDA,

Logo, é possível concluir que este tratamento constituiria uma prática abusiva por parte do controlador, tendo em vista que a Lei considera como dados pessoais aqueles que possibilitem identificar ou tornar identificável uma determinada pessoa. Ora, se o controlador poderia identificar se tratar de uma criança, não poderia se furtar de cumprir a Lei com a justificativa de que o acesso ao conteúdo teria sido realizado pelo usuário de um adulto.

4. Dispensa do consentimento

De acordo com o §3º do art. 14, há uma exceção ao disposto no §1º, no que diz respeito a esse consentimento dos pais ou responsáveis, visando a proteção da própria criança.

Assim, quando necessário o tratamento de dados de uma criança para realizar contato com os seus pais ou responsáveis, deverão ser estas informações tratadas uma única vez, sem qualquer tipo de armazenamento, sendo eminentemente vedada a transferência a terceiros sem o devido consentimento.

Entretanto, o fato de o agente de tratamento não poder armazenar os dados pessoais de crianças nestas situações pode acarretar uma grande insegurança jurídica aos agentes de tratamento e inclusive às crianças que se deseja proteger, considerando que os controladores

Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (orgs). **Tratado de Proteção de Dados Pessoais**. 1º ed. Rio de Janeiro: Forense, 2021. p. 219.

não teriam condições de constituir provas para a sua própria defesa em processos judiciais ou administrativos, por exemplo.

Haveria, portanto, um flagrante desincentivo para que os agentes de tratamento se utilizassem desta prerrogativa, sendo, assim, esperado que a ANPD se posicione sobre esta questão em um futuro próximo.

Já para a proteção da criança, entretanto, entende-se que os dados poderiam ser coletados mais de uma vez e armazenados, a depender do caso concreto, o que só poderia acontecer em situações excepcionais, em seu melhor interesse[129]. A interpretação que se dá é de que essa única exceção deve ser utilizada apenas para emergências, de maneira semelhante com que são tratados dados pessoais para a proteção da vida ou da saúde dos titulares[130], não podendo ser utilizadas para a proteção da criança ou do adolescente em circunstâncias cotidianas, como para a realização de exames e consultas médicas de rotina.

[129] "Princípio do melhor interesse é, pois, o norte que orienta todos aqueles que se defrontam com as exigências naturais da infância e juventude. Materializá-lo é o dever de todos". MACIEL, Kátia Regina Ferreira Lobo Andrade (Coord.). **Curso de direito da criança e do adolescente** – aspectos teóricos e práticos. 7ª ed. São Paulo: Saraiva, 2014. p. 70.

[130] COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais** ¬– Comentada. 3º ed. São Paulo, Revista dos Tribunais, 2019. p. 122.

Seção IV - Do Término do Tratamento de Dados

Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

II - fim do período de tratamento;

III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou

IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

1. Do ciclo de vida dos dados

É comum se referir, no jargão técnico, ao "ciclo de vida dos dados", que envolve todo o período desde a coleta ou criação do dado até a sua respectiva eliminação ou descarte.

Neste sentido, a Seção IV deste Capítulo II dita as hipóteses de encerramento do tratamento de dados pessoais, que estão elencadas nos incisos do art. 15.

Assim, o inciso I do art. 15 diz respeito a duas hipóteses de término de um determinado tratamento: (i) o alcance da finalidade pretendida; ou (ii) quando os dados deixarem de ser necessários ou pertinentes ao alcance dessa finalidade.

Pode-se citar, por exemplo, a coleta de dados sobre as preferências dos clientes sobre determinados tipos de hamburgueres em uma rede de *fast food*, o que certamente se daria com o consentimento dos clientes, para a criação de uma campanha publicitária.

Nesse contexto, após a finalização bem sucedida da pesquisa, em tese, a rede de restaurantes teria que eliminar os dados coletados, tendo em vista que a finalidade pretendida teria sido alcançada. Entretanto, caso queira alterar a finalidade do tratamento e mesmo assim continuar tratando os dados, o agente de tratamento deverá realizar o disposto no art. 8º, inciso VI, informando ao titular acerca da mudança de finalidade.

2. Retenção dos dados

De acordo com o inciso II do art. 15, é recomendável que o agente de tratamento detenha uma política específica de retenção de dados para dispor por quanto tempo os dados pessoais que detenha serão tratados e armazenados, tendo em vista a observação do princípio da necessidade. Assim, ao fim do período específico, exclui-se automaticamente estes dados, mitigando os riscos relacionados com o tratamento.

Entretanto, pode ser necessário que o agente de tratamento mantenha os dados para o exercício regular de direitos, base de tratamento prevista no art. 7º, inciso VI e no art. 11, inciso II, alínea "d", ocasião em que ela deveria manter os dados pessoais até o preenchimento dos prazos de prescrição ou decadência previstos no ordenamento jurídico, a fim de se resguardar em eventuais processos judiciais.

3. Revogação do consentimento

O inciso III do art. 15 parece deixar claro que, nas hipóteses em que for necessário o consentimento do titular, a mera revogação disposta no §5º do art. 8º desta Lei não ensejará a eliminação automática dos seus dados pessoais, sendo necessária a sua comunicação explícita para tal.

4. Determinação da ANPD

Por fim, o inciso IV aduz que, nos casos em que houver violação à LGPD, a ANPD poderá determinar a eliminação dos dados pessoais como sanção administrativa, conforme disposto no art. 52, inciso VI, o que ocorrerá após terminado o processo administrativo com direito à ampla defesa e contraditório.

As disposições acerca da função de fiscalização da autoridade nacional estão mais bem detalhadas no Capítulo VIII.

Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

I - cumprimento de obrigação legal ou regulatória pelo controlador;

II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou

IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

1. Exceções à eliminação de dados pessoais

O art. 16 determina que, após preenchidas as hipóteses previstas no art. 15, deverá haver, pelo agente de tratamento, a eliminação dos dados pessoais por ele tratados.

Entretanto, este artigo também prevê algumas exceções a esta determinação, que deverão ser limitadas ao contexto das atividades de tratamento realizadas, não podendo o agente de tratamento se valer destas exceções de forma indiscriminada.

2. Cumprimento de obrigação legal ou regulatória

A primeira exceção, no inciso I, se refere à necessidade de cumprimento de obrigação legal ou regulatória, ocasiões em que o controlador poderá manter os dados pessoais especificamente para estes fins, momento este em que passará a tratar os dados de acordo com as bases de tratamento contidas no artigo 7º, inciso II e no artigo 11, inciso II, alínea "a".

3. Estudos por órgãos de pesquisa

A segunda exceção, no inciso II, diz respeito ao armazenamento de dados para a realização de estudos por órgãos de pesquisa. Existe uma recomendação legal para que estes dados sejam anonimizados, ou seja, não se constitui em uma obrigação ao controlador. Entretanto, caso a ANPD, em uma eventual fiscalização, julgue que os dados poderiam ter sido anonimizados utilizando-se de técnicas razoáveis e disponíveis à época da anonimização, poderá impor algum tipo de sanção contra este agente de tratamento.

4. Transferência de dados a terceiros

A terceira exceção, contida no inciso III, possui uma redação um tanto confusa, pois permitiria um armazenamento de dados sem qualquer limitação temporal, bastando que houvesse uma transferência posterior a outro agente de tratamento e que fossem respeitados os "requisitos de tratamento de dados dispostos na Lei".

Assim, um agente de tratamento mal-intencionado poderia manter armazenados dados dos titulares por 20 anos, por exemplo, sob a justificativa de que iria transferi-los a um terceiro após passado este lapso temporal, o que certamente ocorreria ao arrepio do princípio da necessidade e das demais disposições previstas na Lei.

É possível, entretanto, uma interpretação deste dispositivo de forma mais adequada às disposições da LGPD, o que somente ocorreria em algumas situações específicas. Poderia ser o caso de uma determinada empresa que, após ser comprada por outra empresa, retivesse os dados dos titulares, mesmo após o fim do período de tratamento, apenas para realizar a transferência destes dados antes de ser adquirida.

Desta maneira, no exemplo em questão, a empresa compradora ficaria responsável por realizar o devido enquadramento na LGPD, optando por reter tais dados de acordo com outra disposição do art. 16, ou para tratá-los em outras bases legais, alterando assim a finalidade do tratamento.

5. Uso exclusivo pelo controlador

A quarta exceção, contida no inciso IV do art. 16, diz respeito à retenção de dados pessoais para o uso exclusivo do controlador, com a condição de que estes dados passem por um processo de anonimização. Este inciso também proíbe que qualquer terceiro tenha acesso a estes dados anonimizados, o que implica dizer que estariam

proibidas também quaisquer operações de transferência e de uso compartilhado.

Primeiramente, cumpre destacar a contradição existente entre a concepção de dados anonimizados deste inciso IV com aquela prevista no art. 12 da Lei. Isto porque, de acordo com o referido artigo, os dados anonimizados não seriam considerados dados pessoais e não entrariam no escopo de proteção da LGPD, podendo ser transferidos livremente pelo controlador.

Nesse sentido, parece razoável supor que o legislador estaria querendo incluir uma exceção ao art. 12 com este inciso IV, vedando o acesso e, consequentemente, a transferência a terceiros destas bases de dados anonimizadas, com o fim de evitar cruzamentos que pudessem revelar a identidade dos titulares.

Entretanto, embora tenha uma finalidade primorosa, tal exceção acaba por se revelar inócua e até mesmo contraditória, tendo em vista que a Lei permitiria a transferência de dados pessoais enquanto proibiria que o mesmo fosse feito com dados anonimizados, os quais, teoricamente, protegeriam muito mais a privacidade dos titulares.

Independentemente destas contradições presentes na Lei, é certo que os controladores deverão agir com bastante cautela ao se valerem desta exceção contida no inciso IV do art. 16, tendo em vista o risco de o procedimento de anonimização não ser considerado adequado em uma eventual fiscalização realizada pela ANPD, conforme os critérios estabelecidos pelo §2º do mencionado art. 12.

CAPÍTULO III - DOS DIREITOS DO TITULAR

Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

O capítulo III da Lei elenca os direitos dos titulares de dados pessoais. Nesse sentido, o art. 17 reforça a noção de que tais dados pertencem exclusivamente aos titulares de dados. Isto quer dizer que a ligação de um indivíduo aos seus dados pessoais é indissociável, ou seja, o simples fato de o agente de tratamento deter a posse dos dados pessoais para que possa tratá-los, não significa que houve uma ruptura na relação existente entre titular e os seus dados pessoais, o que condiz com o que está disposto no Código Civil[131].

Este artigo também coloca um foco especial nos direitos fundamentais do titular que deverão ser observados com maior atenção, incluindo a liberdade, intimidade e privacidade.

[131] BRASIL, **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Art. 11: Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I - confirmação da existência de tratamento;

II - acesso aos dados;

III - correção de dados incompletos, inexatos ou desatualizados;

IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;

VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.

§ 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.

§ 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.

§ 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:

I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou

II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

§ 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.

§ 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional. (Redação dada pela Lei nº 13.853, de 2019)

§ 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.

§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor. O titular tem o direito de receber algum tipo de resposta dos agentes de tratamento, o que quer dizer que o agente de tratamento não pode ignorar qualquer requisição acerca dos seus dados pessoais, por mais absurda ou ilegítima que seja.

1. Direitos dos titulares

Alguns dos direitos dos titulares estão discriminados no rol do art. 18, mas também podem ser encontrados em diversas outras disposições da Lei. Dito isto, é importante que os controladores detenham uma plataforma centralizada para processar todas as eventuais solicitações dos titulares no que diz respeito aos seus dados pessoais, também conhecida como "canal do titular".

Com este canal centralizado, torna-se possível a documentação de todas as solicitações e respostas dos titulares, o que é especialmente importante para fins de constituição de provas, em processos judiciais e administrativos, tendo em vista que o ônus da prova recai sobre o controlador, além de compreender uma boa prática de *compliance* com a Lei.

Não obstante, embora a utilização deste "canal do titular" seja uma excelente alternativa, os controladores devem se atentar principalmente com eventuais fraudes, que possam ser realizadas para a obtenção de dados sigilosos dos titulares.

A título de exemplificação, imagine-se uma situação em que um indivíduo se passasse pelo verdadeiro titular perante um controlador, resultando no risco deste titular pleitear indenizações pela divulgação não autorizada dos seus dados a terceiros. A fim de evitar situações deste tipo e de se resguardar contra eventuais condenações, recomenda-se que os controladores criem instrumentos robustos de verificação da identidade dos titulares como, por exemplo, a

necessidade de o titular apresentar solicitação formal assinada, com reconhecimento de firma em cartório.

Esta situação certamente pode se alterar futuramente, com a regulamentação de uma identidade digital pela ANPD ou por outro órgão do Poder Público que permita uma identificação simples e segura dos titulares[132].

2. Confirmação de existência do tratamento e acesso aos dados

Os direitos previstos nos incisos I e II do art. 18, impõem ao controlador, mediante requisição do titular, a obrigação de informar a existência ou inexistência do tratamento de dados pessoais.

Caso haja este tratamento, o titular poderá ter acesso a todos os dados tratados e também a todas as informações relacionadas ao tratamento, como as finalidades, as categorias, as transferências realizadas a terceiros, os prazos de retenção, a origem dos dados e a existência de decisões automatizadas.

[132] "[...] a identidade digital indiana funcionou justamente como "fundação" para o processo de inclusão social e financeira. Sua principal característica é a simplicidade. O Aadhaar utiliza só quatro dados básicos: nome, data de nascimento, sexo e endereço (ou outro identificador, como telefone). A esses quatro dados a identidade agrega até três identificadores biométricos únicos (digital, íris e rosto). A conjugação desses elementos leva à geração de um número único de 12 algarismos. Esse sistema torna-se, então, o passaporte único das relações entre cidadãos e governo, contrastando com o Brasil, que vive uma multiplicação de cadastros administrativos e documentos ". LEMOS, Ronaldo. Identidade digital, pergunte à Índia. **Folha de São Paulo**, 2020. Disponível em <https://www1.folha.uol.com.br/colunas/ronaldolemos/2020/05/identidade-digital-pergunte-a-india.shtml>. Acesso em: 29/01/2020.

3. Retificação dos dados

Conforme previsão do inciso III do art. 18, existindo quaisquer dados incompletos, inexatos ou desatualizados, o controlador terá a obrigação de corrigi-los, a pedido do titular. Tal disposição se revela pertinente frente ao potencial de dano que estes dados incorretos podem causar ao titular, considerando que, na atualidade, os dados pessoais são essenciais para o acesso à saúde ou ao crédito bancário, apenas para citar alguns exemplos.

4. Anonimização, bloqueio e eliminação dos dados

No caso de os dados serem desnecessários, excessivos ou tratados de maneira ilegal, o titular poderá requerer ao agente de tratamento que proceda com a anonimização, o bloqueio ou a eliminação dos dados, conforme disposto no inciso IV do art. 18.

Ressalte-se que este inciso faz referência a três direitos diferentes, cujas definições se encontram, respectivamente, nos incisos XI (anonimização), XIII (bloqueio) e XIV (eliminação) do art. 5º da LGPD.

5. Direito de portabilidade dos dados

O inciso V do art. 18, por sua vez, diz respeito ao direito de portabilidade dos dados pelos titulares, permitindo que eles transportem livremente os seus dados pessoais entre diferentes agentes de

tratamento. Para melhor regular este direito, a ANPD poderá criar protocolos de interoperabilidade de dados, conforme previsão do art. 40 da Lei[133].

Entretanto, o exercício deste direito de portabilidade deverá observar a proteção da propriedade intelectual dos controladores, a qual inclui os seus segredos comerciais e industriais.

A título de complementação, pode-se observar uma outra ressalva, desta vez no §7º deste artigo, aduzindo que o titular não possui este direito de portabilidade sobre os dados anonimizados, tendo em vista que estes tipos de dados não seriam dados pessoais, conforme dispõe o caput do art. 12 da Lei.

6. Eliminação dos dados obtidos com o consentimento do titular

O direito previsto no inciso VI do art. 18 complementa a disposição contida no art. 15, §3º da Lei, vez que reforça a necessidade de o titular solicitar expressamente a eliminação de seus dados, naquelas circunstâncias em que o tratamento se der com base no seu consentimento.

Entretanto, tal eliminação não será realizada caso subsista alguma das exceções à eliminação de dados contidas no art. 16 da Lei,

[133] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Art. 40: A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.

ou quando houver alteração na fundamentação legal para o tratamento daqueles dados.

7. Informações sobre o uso compartilhado

O inciso VII do art. 18 diz respeito ao direito de o titular obter informações sobre os compartilhamentos de dados pessoais realizados pelo agente de tratamento, o que está associado a sua capacidade de autodeterminação informacional.

Desta forma, é possível considerar que o titular poderá obter todas as informações de contato dos agentes de tratamento aos quais seus dados tiverem sido eventualmente compartilhados.

Esta disposição pode criar algumas dificuldades para aqueles agentes de tratamento que necessitarem realizar, no exercício de suas funções, um grande volume de consultas, se utilizando de dados pessoais de titulares. É o caso de escritórios de advocacia, os quais, em um único dia, podem realizar diversas consultas a tribunais ou empresas de serviços voltados para análises de pessoas físicas, por exemplo.

Logo, é recomendável que os agentes de tratamento mantenham um registro adequado de todas as suas operações de compartilhamento de dados pessoais, para que possam fornecer estas informações nas ocasiões em que os titulares as solicitarem.

8. Recusa do consentimento

Para que o consentimento seja realmente livre, o inciso VIII do art. 18 prevê que o titular deve ser informado, de maneira clara, de todas as consequências do não fornecimento do seu consentimento. Uma boa medida neste sentido se daria em uma solicitação "granular" do consentimento do titular, ou seja, que a solicitação do consentimento fosse desmembrada em diversas finalidades distintas, possibilitando ao titular exercer um maior controle sobre os dados que serão eventualmente tratados[134].

9. Oposição ao tratamento de dados

Já nos tratamentos realizados através das bases legais que não sejam o consentimento, o titular tem o direito de exercer sua oposição ao agente de tratamento, nos termos do §2º do art. 18. Nesta disposição, o que busca se proteger é o próprio direito de oposição a determinado tratamento, mesmo que em um momento posterior essa oposição se revele inócua. Além disso, é um direito do titular ser informado das justificativas do controlador em não haver coletado o seu consentimento para determinada operação de tratamento.

Caso não julgue satisfatória a resposta do controlador, o §1º do art. 18 prevê a possibilidade de peticionamento contra quaisquer

[134] MALDONADO, Viviane Nóbrega. Capítulo III – Dos Direitos do Titular. In. MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). **LGPD** – Lei Geral de Proteção de Dados – Comentada. 2ª ed. São Paulo: Revista dos Tribunais, 2019. p. 233.

agentes de tratamento perante a Agência Nacional de Proteção de Dados Pessoais – ANPD. Pode-se conceber que essa esfera administrativa deverá se tornar uma via mais célere e eficiente para a proteção dos direitos do titular, quando comparada com a via judicial. Cabe destacar ainda que este direito de petição deverá ser regulamentado pela ANPD, conforme comentários do Capítulo IX.

Entretanto, deve-se frisar que, mesmo antes da constituição dessa regulação futura, os titulares já poderão exercer os seus direitos através do Poder Judiciário, conforme dispõe o art. 21 da Lei. Também, nos termos do §8º do art. 18, o titular de dados poderá realizar o direito de petição frente aos órgãos de defesa do consumidor, como a Fundação de Proteção e Defesa do Consumidor (PROCON), por exemplo.

10. Forma de exercício de direitos do titular

Tendo em vista que os direitos do titular possuem natureza personalíssima, ou seja, são indissociáveis do indivíduo, o §3º do art. 18 certifica, de forma expressa, que somente o titular ou o seu representante legal serão capazes de exercer aqueles direitos previstos neste artigo.

Contudo, a referência que o §3º faz ao "agente de tratamento", revela uma contradição terminológica com o *caput* do referido artigo, tendo em vista que este se refere apenas ao controlador, assim como o fazem as demais disposições do art. 18. Logo, considerando que o operador não realiza qualquer decisão pertinente ao tratamento de

dados do titular, decisão esta que cabe apenas ao controlador, é de se concluir que o legislador quis se referir apenas a este agente nesta disposição do §3º.

Por outro lado, quando analisado este dispositivo em conjunto com o próprio inciso I deste artigo, tem-se que ao menos uma resposta negativa deveria ser dada ao titular, ou seja, se o agente de tratamento for o operador este necessitaria ao menos dar este tipo de resposta ao titular, informando-o de que apenas processa seus dados na condição de operador e, desta feita, faria sentido a menção ao "agente de tratamento" neste parágrafo.

Sobretudo, a Lei teria sido omissa por não ter determinado se o operador deveria informar quem é o controlador, vez que isso poderia, inclusive, comprometer a estratégia do negócio do próprio agente de tratamento.

Como bem se observa, a única menção existente nesse sentido está no §4º, inciso I deste artigo, entretanto, esta referência diz respeito aos casos que o agente não realiza qualquer tratamento, diferente desta situação em que o agente é o operador.

Passadas estas questões, tem-se que o controlador, em algumas circunstâncias, poderia se ver impossibilitado de responder às solicitações do titular de forma imediata, seja pela complexidade da solicitação, seja pelo fato de não ser o agente de tratamento daquela operação. Nestas situações, conforme já exposto, ainda assim deverá lhe oferecer uma resposta negativa, que teria que conter, ao menos, a

comunicação de que não seria o agente de tratamento naquele caso, ou a indicação das exatas razões que o impediriam de responder de forma imediata a solicitação do titular.

Tal disposição reforça, uma vez mais, a necessidade de criação de um canal do titular para o gerenciamento destas solicitações, considerando que a recusa pelo agente de tratamento poderá resultar na condenação ao pagamento de multas e indenizações.

11. Obrigação de comunicação pelo controlador

Os controladores são autorizados a fazer o uso compartilhado de dados pessoais com outros agentes de tratamento. Entretanto, o §6º do art. 18 impõe a obrigação de o controlador comunicar a estes agentes a eliminação, correção, bloqueio ou anonimização dos dados que foram compartilhados, para que estes agentes também realizem estas operações.

Tal comunicação só não será realizada caso se torne uma obrigação demasiadamente custosa ou mesmo impossível de ser realizada, sendo recomendável que o controlador registre as justificativas que levaram a esta decisão em um documento específico.

Ocorre que, não fica claro quem é realmente o agente de tratamento mencionado no começo do §6º, o qual dispõe que "o responsável" é quem deverá informar estes eventos aos agentes de tratamento. Desta forma, subentende-se que houve uma confusão

terminológica do legislador quando da redação do texto final da Lei, tendo em vista que em um momento anterior da sua tramitação os controladores eram referidos apenas como "responsáveis". Este lapso também pode ser encontrado na redação do parágrafo único do art. 33 da LGPD[135].

[135] Vide redação original do Projeto de Lei nº 4.060 de 2012 que deu origem à LGPD. "Art. 7º. Para os fins da presente lei, entende-se como: [...] V - responsável: a pessoa natural ou jurídica, de direito público ou privado, a quem compita, na qualidade de possuidora de arquivo, registro, base ou banco de dados, a tomada de decisões referentes à realização de tratamento de dados pessoais; [...]". Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1001750&filename=PL+4060/2012>. Acesso em: 28/01/2020.

Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:

I - em formato simplificado, imediatamente; ou

II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

§ 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.

§ 2º As informações e os dados poderão ser fornecidos, a critério do titular:

I - por meio eletrônico, seguro e idôneo para esse fim; ou

II - sob forma impressa.

§ 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que

permita a sua utilização subsequente, inclusive em outras operações de tratamento.

§ 4º A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos.

1. Forma de exercício dos direitos do titular

O exercício dos direitos previstos nos incisos I e II do art. 18 poderá ser realizado por meio eletrônico ou impresso, de maneira a melhor efetivar os direitos dos titulares, conforme disposição do §1º do art. 19. Nesse sentido, os incisos do caput do art. 19 determinam dois modos distintos de resposta: o modo simplificado e o modo completo.

A forma de resposta simplificada, prevista no inciso I, deverá ser respondida de forma imediata, ou seja, assim que o agente de tratamento recepcionar a requisição do titular. Consequentemente, caso o titular pergunte ao agente de tratamento se está tratando algum de seus dados, a resposta afirmativa ou negativa deverá ser fornecida de maneira imediata.

Como se pode notar, essa operação poderá ser mais bem coordenada através do canal do titular, uma plataforma específica de gerenciamento dos dados pessoais dos titulares, já mencionado neste capítulo.

Já aquela forma de resposta completa, prevista no inciso II, deve conter todas as informações atinentes ao tratamento dos dados pessoais, incluindo as finalidades com que estão sendo tratados, a fundamentação legal e os prazos de retenção, e deverá ser respondida dentro de 15 dias. Imperioso ressaltar que a ANPD poderá regular este prazo de modo diferente, a depender de necessidades setoriais específicas, nos termos do §5º do art. 18.

Por fim, é importante que a empresa detenha consigo todos os registros detalhados das operações de tratamento, para que seja possível realizar a gestão efetiva destas respostas ao titular.

2. Cópia eletrônica integral de dados pessoais

Conforme disposto no §3º do art. 19, há também a possibilidade de o titular receber uma cópia eletrônica integral dos seus dados pessoais, quando o tratamento for baseado no seu consentimento ou em um contrato, a fim de que o titular possa ter melhor acesso a estas informações e possa exercer, inclusive, o direito de portabilidade de seus dados.

Entretanto, não restou claro se essa cópia integral seria apenas uma lista dos dados pessoais ou se significaria uma cópia de todo o instrumento contratual.

Anteriormente à vigência da LGPD, um titular que demandasse o acesso às informações presentes em um determinado

contrato, por exemplo, teria que se valer de uma ação judicial de exibição de documentos, caso houvesse uma recusa no fornecimento destas informações pelo controlador.

Com a vigência da Lei, entretanto, o titular terá como evitar a via judicial, bastando que estabeleça contato com o controlador e exercite o seu direito de acesso aos seus dados tratados, sem prejuízo do direito de petição perante a ANPD, previsto no art. 55-J, inciso V.

Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

As decisões automatizadas são cada vez mais comuns no cotidiano, e são geralmente implementadas pelos agentes de tratamento com o intuito de redução dos custos de mão-de-obra ou para a melhoria da produtividade. Essa tomada de decisão de forma automatizada pressupõe a criação de um perfil comportamental dos titulares de dados, com o estabelecimento de critérios de acesso ou restrição a determinados produtos, serviços, ou até mesmo a vagas de emprego.

Neste sentido, considerando o potencial de discriminação evidenciado por esta forma de tratamento, o *caput* do art. 20 busca prover ao titular de dados o direito de solicitar que o controlador revise qualquer decisão automatizada. Nesse sentido, o titular também possui o direito de ser informado de todos os critérios e atributos analisados para a tomada daquela decisão, respeitando-se o segredo comercial e industrial.

Considerando que os controladores podem se valer do caráter abstrato sobre os seus direitos de propriedade intelectual, a disposição contida no §2º prevê uma medida repressiva, reforçando que a ANPD poderá dispor de auditorias, com o intuito de analisar eventuais condutas discriminatórias ou abusivas por parte dos controladores que procederem com formas de tomada de decisão automatizadas.

Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

O art. 21 ressalta que o exercício regular de direitos interessa tão somente aos titulares, sendo vedada a utilização dos seus dados por terceiros, principalmente quando este tratamento puder lhes causar algum prejuízo.

A título de ilustração, cite-se um cenário em que um potencial empregador, após consultar algumas bases de dados de acesso público, se recusasse a contratar um indivíduo em virtude de uma reclamação trabalhista movida por ele. Nesse caso, este tratamento poderia ser considerado abusivo e eivado de má-fé, expondo o empregador ao risco de ser condenado em danos morais e materiais, decorrentes da infringência da LGPD e das demais normas trabalhistas[136].

[136] MALDONADO, Viviane Nóbrega. Capítulo III – Dos Direitos do Titular. In. MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). **LGPD** – Lei Geral de Proteção de Dados – Comentada. 2ª ed. São Paulo: Revista dos Tribunais, 2019. p. 242.

Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

O art. 22 trata dos aspectos processuais da LGPD, inserindo-a no microssistema de tutela dos direitos coletivos. Assim, existindo alguma lacuna normativa na LGPD, seria possível a sua integração através da aplicação de uma norma presente em outra lei, como o CDC[137], a Lei nº 7.347/85 (Lei de Ação Civil Pública)[138] ou a Lei

[137] BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Art. 81: A defesa dos interesses e direitos dos consumidores e das vítimas poderá ser exercida em juízo individualmente, ou a título coletivo. Art. 82: Para os fins do art. 81, parágrafo único, são legitimados concorrentemente: I - o Ministério Público, II - a União, os Estados, os Municípios e o Distrito Federal; III - as entidades e órgãos da Administração Pública, direta ou indireta, ainda que sem personalidade jurídica, especificamente destinados à defesa dos interesses e direitos protegidos por este código; IV - as associações legalmente constituídas há pelo menos um ano e que incluam entre seus fins institucionais a defesa dos interesses e direitos protegidos por este código, dispensada a autorização assemblear.
[...] Art. 91. Os legitimados de que trata o art. 82 poderão propor, em nome próprio e no interesse das vítimas ou seus sucessores, ação civil coletiva de responsabilidade pelos danos individualmente sofridos, de acordo com o disposto nos artigos seguintes.
[138] Idem. **Lei nº 7.347, de 24 de julho de 1985**. Disciplina a ação civil pública de responsabilidade por danos causados ao meio-ambiente, ao consumidor, a bens e direitos de valor artístico, estético, histórico, turístico e paisagístico (VETADO) e dá outras providências. Art. 1º: Regem-se pelas disposições desta Lei, sem prejuízo da ação popular, as ações de responsabilidade por danos morais e patrimoniais causados: [...] IV - a qualquer outro interesse difuso ou coletivo.

4.717/65 (Lei de Ação Popular)[139], esta última válida apenas para os casos de tratamento ilegal ou abusivo perpetrado pelo Poder Público.

Desta maneira, não somente o titular, mas também os demais atores mencionados na Lei nº 7.347/85 poderão ingressar com ações coletivas contra o agente de tratamento. Ainda, tendo em vista o princípio da inafastabilidade da jurisdição e a natureza transindividual do direito à proteção de dados pessoais, o agente de tratamento poderá ser demandado por ações individuais ou coletivas, independentemente da existência de processo administrativo perante a ANPD[140].

Entretanto, é importante ressaltar que este procedimento na ANPD poderia se revelar mais célere e efetivo à proteção dos direitos dos titulares, tendo em vista a natureza eminentemente técnica e específica da autoridade nacional.

---

[139] BRASIL. **Lei nº 4.717, de 29 de junho de 1965**. Regula a ação popular. Art. 5º: Têm legitimidade para propor a ação principal e a ação cautelar: I - o Ministério Público; II - a Defensoria Pública; III - a União, os Estados, o Distrito Federal e os Municípios; IV - a autarquia, empresa pública, fundação ou sociedade de economia mista;
V - a associação que, concomitantemente: a) esteja constituída há pelo menos 1 (um) ano nos termos da lei civil; b) inclua, entre suas finalidades institucionais, a proteção ao patrimônio público e social, ao meio ambiente, ao consumidor, à ordem econômica, à livre concorrência, aos direitos de grupos raciais, étnicos ou religiosos ou ao patrimônio artístico, estético, histórico, turístico e paisagístico.

[140] BESSA, Leonardo Roscoe; NUNES, Ana Luísa Tarter. Instrumentos Processuais de Tutela Individual e Coletiva: Análise do art. 22 da LGPD. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (orgs). **Tratado de Proteção de Dados Pessoais**. 1º ed. Rio de Janeiro: Forense, 2021. p. 672

CAPÍTULO IV - DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

Seção I - Das Regras

Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;

II - (VETADO); e

III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei;

IV - (VETADO).

§ 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento.

§ 2º O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no caput deste artigo de instituir as autoridades de que trata a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

§ 3º Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data), da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo), e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

§ 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei.

§ 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo.

1. Princípios que regem a atividade da Administração Pública

O tratamento de dados pessoais está na essência das atividades do Estado, e constitui uma condição indispensável para o cumprimento das suas atribuições constitucionais e para o exercício da cidadania pelos próprios titulares. Assim, diante da crescente sofisticação e complexidade das tecnologias utilizadas na execução de políticas públicas, aumenta a importância da discussão sobre o tratamento de dados pessoais pelo Poder Público[141].

É importante ressaltar que o caput deste artigo 23 menciona que as pessoas jurídicas elencadas no art. 1º da Lei de Acesso à Informação – LAI, quais sejam, os órgãos públicos integrantes da administração direta e indireta, de todos os níveis da federação, deverão seguir as regras dispostas no Capítulo IV da Lei. Tal disposição é estendida aos órgãos de serviço notarial e de registro exercidos por delegação do Poder Público, conforme disposto nos §§5º e 6º do art. 23.

Desta forma, no contexto trazido pela LGPD, deverá a Administração Pública observar o princípio da legalidade, o que significa dizer que ela só tratará os dados dos cidadãos quando houver expressa autorização legal para tal. No mais, deverão ser observados também os outros princípios que regem a Administração Pública,

[141] WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo Poder Público. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (orgs). **Tratado de Proteção de Dados Pessoais**. 1º ed. Rio de Janeiro: Forense, 2021. p. 271.

mencionados no art. 37 da Constituição Federal [142], tais como a impessoalidade, a moralidade, a publicidade e a eficiência, além daqueles previstos no art. 2º da Lei 9.784/99[143], dentre os quais pode-se destacar a razoabilidade, a proporcionalidade, a segurança jurídica e o interesse público.

2. Publicidade e a LGPD

A Lei de Acesso à Informação prevê que o acesso às informações sobre os atos realizados pela Administração Pública é de interesse coletivo. Isto quer dizer que qualquer cidadão tem o direito de fiscalizar os processos licitatórios, as execuções de obras e as prestações de contas, dentre outros exemplos que se pode citar[144].

Portanto, a LAI se fundamenta sobre o princípio da publicidade dos atos administrativos nas três esferas de poder, fundamento que possui congruência com o princípio da transparência previsto no art. 6º, inciso VI da LGPD. Neste mesmo sentido, a LAI

---

[142] BRASIL. **Constituição da República Federativa do Brasil**, 1988. Art. 37: A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência [...]

[143]Idem. **Lei nº 9.784, de 29 de janeiro de 1999**. Regula o processo administrativo no âmbito da Administração Pública Federal. Art. 2º: A Administração Pública obedecerá, dentre outros, aos princípios da legalidade, finalidade, motivação, razoabilidade, proporcionalidade, moralidade, ampla defesa, contraditório, segurança jurídica, interesse público e eficiência.

[144] WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo Poder Público. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (orgs). **Tratado de Proteção de Dados Pessoais**. 1º ed. Rio de Janeiro: Forense, 2021. p. 277.

inclui a obrigação de o Poder Público observar a proteção de dados pessoais[145], o que acaba por ser complementado pela proteção prevista na LGPD.

3. Finalidade dos atos administrativos

Há também um paralelo interessante existente entre o princípio da finalidade na LGPD, que deve ser observado tanto por entes privados quanto por entes públicos, e o princípio da finalidade no Direito Administrativo, que deve ser observado apenas pelos entes públicos no exercício dos seus atos administrativos.

O princípio da finalidade trazido pela LGPD, aduz que o tratamento de dados só será realizado através das hipóteses contidas na Lei, sendo vedados tratamentos posteriores incompatíveis com os propósitos originais.

Por sua vez, o princípio da finalidade pública asserta que o administrador público será obrigado a praticar determinado ato administrativo para o atendimento do seu fim legal, e que esta prática se dará de forma impessoal.

[145] BRASIL. **Lei nº 12.527, de 18 de novembro de 2011.** Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Art. 4º: Para os efeitos desta Lei, considera-se: [...]IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável.

Entende-se que esta finalidade pública é indicada, de forma expressa ou implícita, através dos objetivos contidos na norma[146], não podendo o administrador se furtar em realizá-los, sob pena de incorrer em improbidade administrativa ou em crime de prevaricação[147].

Assim, só será considerado lícito o tratamento realizado pela Administração Pública caso cumpridas as duas condicionantes previstas nos incisos do art. 23 da Lei, que dizem respeito à transparência das condições de tratamento ao titular, que se encontra mais bem regulamentada no art. 8º da LAI[148], e à nomeação de um encarregado pelo tratamento de dados pessoais.

Neste último caso, sobre a nomeação do encarregado, é interessante notar o erro na redação legislativa ao fazer-se referência ao art. 39 da Lei, que dispõe acerca do tratamento pelo operador de dados. Na realidade, é o RGPD[149] que disserta sobre a figura do encarregado

---

[146] MEIRELLES, Hely Lopes. **Direito Administrativo Brasileiro**. 43º ed. São Paulo: Malheiros, 2018. p.96.

[147] BRASIL. **Decreto-lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Art. 319: Retardar ou deixar de praticar, indevidamente, ato de ofício, ou praticá-lo contra disposição expressa de lei, para satisfazer interesse ou sentimento pessoal: Pena - detenção, de três meses a um ano, e multa.

[148] Idem. **Lei nº 12.527, de 18 de novembro de 2011.** Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Art. 8º: É dever dos órgãos e entidades públicas promover, independentemente de requerimentos, a divulgação em local de fácil acesso, no âmbito de suas competências, de informações de interesse coletivo ou geral por eles produzidas ou custodiadas.

[149] UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção**

de dados em seu art. 39, enquanto a LGPD faz esta referência em seu art. 41.

Malgrado este erro, pode-se interpretar que o legislador queria fazer referência a este art. 41 da Lei, devendo o Poder Público, em vista disso, nomear um encarregado nos termos do referido artigo.

Tal disposição está consoante com o flagrante interesse público relacionado à proteção dos dados pessoais, tratados pelo Estado, como bem demonstra a existência de um remédio constitucional específico para proteger os direitos dos titulares nesta relação, qual seja, o *habeas data*.

---

de Dados). Artigo 39º: Funções do encarregado da proteção de dados. 1. O encarregado da proteção de dados tem, pelo menos, as seguintes funções: a) Informa e aconselha o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do presente regulamento e de outras disposições de proteção de dados da União ou dos Estados-Membros; b) Controla a conformidade com o presente regulamento, com outras disposições de proteção de dados da União ou dos Estados-Membros e com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes; c) Presta aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controla a sua realização nos termos do artigo 35.o; d) Coopera com a autoridade de controlo; e)Ponto de contacto para a autoridade de controlo sobre questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo 36.o, e consulta, sendo caso disso, esta autoridade sobre qualquer outro assunto. 2. No desempenho das suas funções, o encarregado da proteção de dados tem em devida consideração os riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento. Disponível em: < https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>. Acesso em 28/01/2021.

4. Base legal de tratamento pela Administração Pública

A Administração Pública poderá realizar operações de tratamento de dados pessoais sempre observando os princípios previstos na LGPD e em conformidade com as demais normas de Direito Administrativo, especialmente no tocante aos princípios da finalidade, adequação e necessidade.

É possível afirmar que a Administração Pública poderá realizar atividades de tratamento de dados para duas finalidades específicas, quais sejam: (i) para a execução das competências legais ou para o cumprimento das atribuições legais do próprio serviço público, hipótese em que os dados poderão ser tratados segundo a base legal prevista no art. 7º, inciso II da LGPD e; (ii) para a execução de políticas públicas, em que os dados serão tratados segundo a base legal prevista no art. 7º, inciso III desta Lei.

A fim de ilustrar melhor esta questão, pode-se dizer que os dados pessoais tratados com base no inciso II do art. 7º estariam relacionados principalmente com a gestão de servidores públicos e o pagamento de salários, enquanto aqueles tratados com base do inciso III estariam enquadrados nas atividades de fiscalização ou de imposição de sanções pela Administração.

Ademais, a LGPD não veda a utilização das demais bases legais permitidas pela legislação nos artigos 7º e 11 para a Administração Pública. Todavia, é importante observar o Considerando

43 do RGPD[150], que proíbe de forma explícita a utilização da base legal do legítimo interesse pelo Poder Público, tendo em vista a posição de vulnerabilidade do titular de dados pessoais frente ao Estado, que tornaria esta base legal incongruente com a persecução do interesse público.

O tratamento com base no consentimento também deve ser observado com cautela pelo Poder Público, vez que só poderia ser realizado quando a relação entre o cidadão e o Estado pudesse ser considerada facultativa. Isto quer dizer que a recusa do cidadão em consentir não poderia prejudicar, de forma alguma, o seu acesso a bens e serviços públicos[151].

---

[150] UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Consideranda (43) A fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa. Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução. Disponível em: < https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>. Acesso em 28/01/2021.

[151] WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo Poder Público. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (orgs). Tratado de Proteção de Dados Pessoais. 1º ed. Rio de Janeiro: Forense, 2021. p .281.

Art. 24. As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.

Parágrafo único. As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos deste Capítulo.

O Estado, em diversas ocasiões, atua diretamente na esfera econômica e o faz através de empresas públicas ou através de sociedades de economia. Entretanto, quando atua em regime concorrencial com agentes privados, a Constituição veda que os órgãos da Administração Pública gozem de quaisquer privilégios fiscais, pois, se assim fosse, a livre concorrência seria prejudicada[152].

Nesse sentido, a LGPD delineou a disciplina de proteção de dados pessoais que deverá ser seguida pelas empresas públicas e as sociedades de economia mista da seguinte forma: (i) caso atuem em

[152] BRASIL. **Constituição da República Federativa do Brasil**, 1988. Art. 173. Ressalvados os casos previstos nesta Constituição, a exploração direta de atividade econômica pelo Estado só será permitida quando necessária aos imperativos da segurança nacional ou a relevante interesse coletivo, conforme definidos em lei. [...] § 2º As empresas públicas e as sociedades de economia mista não poderão gozar de privilégios fiscais não extensivos às do setor privado.

regime de concorrência, serão regidas pelo regime jurídico de direito privado, devendo observar as mesmas disposições aplicadas a este regime; (ii) caso atuem na efetivação de políticas públicas, em regime de monopólio, serão regidas pelo regime jurídico de direito público, e deverão observar o disposto no Capítulo IV.

Não obstante, algumas empresas estatais podem vir a realizar ambas as funções, como é o caso da Empresa de Correios e Telégrafos (ECT), que possui o monopólio dos serviços. Nestes casos, recomenda-se que a entidade pública segregue as suas bases de dados pessoais, a fim de que não possa obter qualquer tipo de vantagem indevida na competição com os entes privados[153].

[153] COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de dados pessoais comentada**. São Paulo: Thomson Reuters, 2018. P. 183. No mesmo sentido: TASSO, Fernando Antônio. Capítulo IV – Do Tratamento de Dados Pessoais pelo poder Público. In. MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). **LGPD** – Lei Geral de Proteção de Dados – Comentada. 2ª ed. São Paulo: Revista dos Tribunais, 2019. p.267.

Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

A manutenção dos dados coletados pelo Estado, em formato interoperável e voltado para o uso compartilhado, imprime uma certa racionalidade ao tratamento de dados pessoais fundamentado no interesse público, e se relaciona diretamente com as intenções de simplificação e desburocratização dos serviços públicos.

Nesse sentido, já foram editadas diversas normativas que regem esta possibilidade de compartilhamento através de formatos interoperáveis pelo Poder Público.

Pode-se citar como exemplo o Decreto nº 10.046/19, que elenca entre as suas diretrizes a simplificação da oferta dos serviços públicos, e a melhoria da qualidade e da fidedignidade dos dados constantes das bases de dados do Poder Público[154].

[154] BRASIL. **Decreto Nº 10.046, de 9 de outubro De 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Art. 1º Este Decreto estabelece as normas e as diretrizes para o compartilhamento de dados entre os órgãos e as entidades da administração pública federal direta, autárquica e fundacional e os demais Poderes da União, com a finalidade de: I - simplificar a oferta de serviços públicos; II - orientar e otimizar a formulação, a implementação, a avaliação e o monitoramento de políticas públicas;

Outro exemplo pode ser verificado no Decreto nº 9.094/17, que proíbe a solicitação, pelos órgãos do Executivo Federal, de quaisquer dados ou documentos que já estiverem contidos em suas próprias bases de dados, exceto se houver disposição legal em contrário[155].

III - possibilitar a análise das condições de acesso e manutenção de benefícios sociais e fiscais; IV - promover a melhoria da qualidade e da fidedignidade dos dados custodiados pela administração pública federal; e V - aumentar a qualidade e a eficiência das operações internas da administração pública federal.

[155] BRASIL. **Decreto nº 9.094, de 17 de julho de 2017**. Regulamenta dispositivos da Lei nº 13.460, de 26 de junho de 2017 Art. 2º: Exceto se houver disposição legal em contrário, os órgãos e as entidades do Poder Executivo federal que necessitarem de documentos comprobatórios de regularidade da situação de usuários dos serviços públicos, de atestados, de certidões ou de outros documentos comprobatórios que constem em base de dados oficial da administração pública federal deverão obtê-los diretamente do órgão ou da entidade responsável pela base de dados, nos termos do disposto no Decreto nº 10.046, de 9 de outubro de 2019, e não poderão exigi-los dos usuários dos serviços públicos., dispõe sobre a simplificação do atendimento prestado aos usuários dos serviços públicos, institui o Cadastro de Pessoas Físicas - CPF como instrumento suficiente e substitutivo para a apresentação de dados do cidadão no exercício de obrigações e direitos e na obtenção de benefícios, ratifica a dispensa do reconhecimento de firma e da autenticação em documentos produzidos no País e institui a Carta de Serviços ao Usuário.

Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:

I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);

II - (VETADO);

III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.

IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou (Incluído pela Lei nº 13.853, de 2019)

V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do

titular dos dados, desde que vedado o tratamento para outras finalidades. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Os contratos e convênios de que trata o § 1º deste artigo deverão ser comunicados à autoridade nacional.

1. Uso compartilhado entre agentes públicos

O compartilhamento de dados entre agentes públicos, regulado pelo caput do art. 26, aduz que este compartilhamento deve "atender as finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas". Assim, devem ser observados os princípios de proteção de dados pessoais e os demais princípios que regem a Administração Pública, bem como a análise sistemática com o art. 23 da Lei.

No entanto, as circunstâncias que permitem o compartilhamento entre órgãos públicos, por serem um tanto abstratas, devem ser mais bem delineadas no caso concreto, como se observou no recente julgado sobre a inconstitucionalidade da Medida Provisória nº 954/20.

Esta MP determinava o compartilhamento de dados entre empresas de telecomunicação e o Instituto Brasileiro de Geografia e Estatística (IBGE) para a realização de controle epidemiológico da

COVID-19, incluindo as relações de nomes, números de telefone e endereços de seus consumidores[156].

Como se pode notar a partir do voto da Ministra Relatora, entendeu-se por reconhecer a existência de um direito autônomo à proteção de dados pessoais e a necessidade de observação dos princípios da finalidade nas operações de tratamento pelo Poder Público, reputando que tal medida provisória seria inconstitucional:

> embora não se possa subestimar a gravidade da crise sanitária nem a necessidade de formulação de políticas públicas que demandam dados específicos para seu enfrentamento, não se pode legitimar, no combate a pandemia, o atropelo de garantias fundamentais consagradas na Constituição[157].

---

[156] BRASIL. **Medida provisória nº 954, de 17 de abril de 2020.** (Vigência encerrada). Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Art. 2º: As empresas de telecomunicação prestadoras do STFC e do SMP deverão disponibilizar à Fundação IBGE, em meio eletrônico, a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas.

[157] Idem. Supremo Tribunal Federal. **Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387 Distrito Federal**. Medida cautelar em ação direta de inconstitucionalidade. Referendo. Medida Provisória nº 954/2020. Emergência de saúde pública de importância internacional decorrente do novo coronavírus (COVID-19). Compartilhamento de dados dos usuários do serviço telefônico fixo comutado e do serviço móvel pessoal, pelas empresas prestadoras, com o Instituto Brasileiro de Geografia e Estatística. *Fumus boni juris. Periculum in mora.* Deferimento. Relator: Ministra Rosa Weber. Data de Julgamento: 07/05/2020. Disponível em: < http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949214&ext=.pdf>. Acesso em: 28/01/2021.

2. Uso compartilhado entre agentes públicos e privados

O compartilhamento de dados pessoais entre agentes públicos e privados é vedado, salvo algumas exceções contidas no §1º do art. 26, podendo-se destacar: (i) execução descentralizada da atividade pública que exija a transferência para uma finalidade específica e determinada; (ii) quando os dados pessoais forem de acesso público, respeitando-se o previsto na Lei, sempre observando a finalidade do tratamento desses dados pessoais; (iii) quando houver respaldo legal ou em contratos, convênios ou outros instrumentos congêneres, cuja existência deverá ser comunicada à ANPD, nos termos do §2º do art. 26; e (iv) para prevenção de fraudes e irregularidades ou proteção do titular, no caso de não existirem outras bases legais de tratamento.

Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto:

I - nas hipóteses de dispensa de consentimento previstas nesta Lei;

II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; ou

III - nas exceções constantes do § 1º do art. 26 desta Lei.

Parágrafo único. A informação à autoridade nacional de que trata o caput deste artigo será objeto de regulamentação.

O *caput* do art. 27 afirma a possibilidade de que os titulares consintam com a comunicação de seus dados pessoais às pessoas jurídicas de direito privado, devendo o Estado informar este compartilhamento à ANPD e também observar todas as regras atinentes ao termo de consentimento, contidas no art. 7º, inciso I, art. 8º e art. 11, inciso I da LGPD.

O Poder Público somente se eximirá de coletar o termo de consentimento dos titulares e informar o compartilhamento à ANPD nas hipóteses contidas nos incisos I e III do art. 27, quais sejam: (i) no

tratamento previsto nas demais bases legais previstas nos artigos 7º e 11 da legislação; e (ii) nas exceções constantes do §1º do artigo 26 da Lei, já comentado.

Já o inciso II do artigo 27 encerra uma tautologia, e não possui qualquer significado prático, tratando-se de um possível erro de redação legislativa, podendo ser interpretado como: "o uso compartilhado de dados pessoais de pessoa jurídica de direito público à pessoa jurídica de direito privado será possível, sem o consentimento do titular, nos casos de uso compartilhado de dados", ou seja, há apenas uma repetição da mesma disposição[158].

[158] WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo Poder Público. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (orgs). **Tratado de Proteção de Dados Pessoais**. 1º ed. Rio de Janeiro: Forense, 2021. p. 285.

Art. 28. (VETADO).

Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do poder público a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei. (Redação dada pela Lei nº 13.853, de 2019)

O art. 29 prevê que, no âmbito de tratamento de dados pelo Poder Público, a ANPD poderá atuar na requisição de informes específicos e elaborar pareceres técnicos, de forma muito semelhante aos demais órgãos de controle presentes na Administração Pública.

Deve-se dar atenção à utilização da expressão "poderá solicitar" presente no referido artigo da Lei, utilizado ao invés de "exigir", tendo em vista que qualquer tipo de exigência pela autoridade nacional, órgão do Poder Executivo, criaria uma invasão de competências dos outros Poderes.

Art. 30. A autoridade nacional poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais.

Conforme já foi mencionado quando da análise do caput do art. 26, nas hipóteses de compartilhamento de dados, a ANPD poderá estabelecer normativas complementares às tratadas neste Capítulo IV.

Seção II - Da Responsabilidade

Art. 31. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.

O envio de informes pela ANPD a determinado órgão público, com recomendações para fazer cessar determinada violação à Lei, possivelmente servirá para a dosimetria das sanções previstas no art. 52 da LGPD, que serão aplicadas de acordo com os parâmetros de demonstração de boa-fé ou com a colaboração do infrator. Ainda, por expressa autorização legal contida no §3º do artigo 52, a Administração Pública poderá sofrer sanções da ANPD, o que está mais bem detalhado no Capítulo VIII.

O informe da ANPD, mencionado pelo art. 31, também poderá servir de fundamentação para interposição de ações por particulares ou pelo Ministério Público, nas hipóteses em que atuar como *custus legis*, ou seja, fiscal da Lei[159].

[159] BRASIL. **Lei nº 13.105, de 16 de março de 2015**. Código de Processo Civil. Art. 176: O Ministério Público atuará na defesa da ordem jurídica, do regime democrático e dos interesses e direitos sociais e individuais indisponíveis. [...] Art. 178: O Ministério Público será intimado para, no prazo de 30 (trinta) dias, intervir como fiscal da ordem jurídica nas hipóteses previstas em lei ou na Constituição Federal e nos processos que envolvam: I - interesse público ou social; II - interesse de incapaz; III - litígios coletivos pela posse de terra rural ou urbana.

Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

A redação do art. 32 leva a crer que os agentes públicos também seriam obrigados a elaborar o RIPD, assim como os agentes privados, podendo a ANPD solicitar a publicação destes ao público em geral, a depender do caso concreto. Além disso, a ANPD poderá sugerir aos órgãos públicos que adotem ações de conformidade e de boas práticas de governança na matéria de proteção de dados pessoais.

CAPÍTULO V - DA TRANSFERÊNCIA INTERNACIONAL DE DADOS

Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:

I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;

II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:

a) cláusulas contratuais específicas para determinada transferência;

b) cláusulas-padrão contratuais;

c) normas corporativas globais;

d) selos, certificados e códigos de conduta regularmente emitidos;

III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de

inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

V - quando a autoridade nacional autorizar a transferência;

VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;

VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou

IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de

2011 (Lei de Acesso à Informação), no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.

1. Transferência Internacional de Dados Pessoais

A *internet* possibilitou que as operações de tratamento de dados ganhassem um aspecto instantâneo, com o cruzamento de informações de forma transnacional em uma velocidade jamais vista. Ao permitir um mundo sem fronteiras, a *internet* também cria toda uma complexidade acerca da jurisdição competente para regular o tratamento de dados pessoais, tendo em vista que os dados não necessariamente são tratados nos mesmos países onde são coletados[160].

A título exemplificativo, para um usuário localizado no Brasil, no momento em que é realizado o upload de uma foto no Facebook, existe uma grande possibilidade de estes dados serem enviados a servidores localizados fora do país. De fato, para garantir o acesso dos usuários e a eficiência das suas operações, diversos provedores de serviços de armazenamento em nuvem possuem bancos de dados espalhados em múltiplos países e em diferentes fusos horários, com o

[160] MARQUES, Fernanda Mascarenhas; AQUINO, Theófilo Miguel de. O regime de transferência internacional de dados da LGPD: delineando as opções regulatórias em jogo. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (orgs). **Tratado de Proteção de Dados Pessoais**. 1º ed. Rio de Janeiro: Forense, 2021. p. 299-300.

intuito de permitir a alocação dos recursos disponíveis de acordo com as demandas de tráfego dos usuários[161].

Diante desta problemática, os países mais desenvolvidos passaram a se reunir através de *frameworks* de legislação internacional, a fim de superar eventuais barreiras protecionistas que poderiam se fundamentar na necessidade de proteção de dados pessoais. Como exemplos, pode-se citar as "Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais", elaboradas pela Organização para a Cooperação e Desenvolvimento Econômico – OCDE na década de 80 e, mais recentemente, o *Privacy Shield*, elaborado entre os Estados Unidos e a União Europeia, para facilitar a transferência internacional de dados, para fins comerciais.

Neste contexto, a LGPD busca trazer, no Capítulo V, a regulação sobre estas transferências instantâneas de dados que ocorrem no âmbito digital, com o intuito maior de tornar o país internacionalmente reconhecido como um território seguro de recebimento de dados[162].

Preliminarmente, é importante ressaltar a diferenciação entre "trânsito" e "transferência" de dados, trazida pela autoridade de proteção de dados do Reino Unido (*Information Comissioner's Office*

[161] CHEUNG, Anne S. Y.; WEBER, Rolf H. (orgs). **Privacy and Legal Issues in Cloud Computing**. Cheltenham: Edward Elgar Publishing, 2016. p. 36.
[162] CHAVES, Luís Fernando Prado. Capítulo V – da Transferência Internacional de Dados. In. MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). **LGPD** – Lei Geral de Proteção de Dados – Comentada. 2ª ed. São Paulo: Revista dos Tribunais, 2019. p.292.

– ICO). Neste sentido, uma simples troca de *e-mails* entre duas áreas de um escritório no Brasil, mas cujo processamento se dê nos Estados Unidos, por exemplo, não teria o condão de ser enquadrada como uma operação de transferência internacional de dados, situação que, se ocorresse, certamente acarretaria um enorme fardo aos agentes de tratamento, devido a interconectividade inerente da *internet*.

Por outro lado, poderiam ser considerados exemplos de transferência internacional de dados pessoais:

(i) o compartilhamento de base de dados de RH entre uma matriz localizada no Brasil e uma filial localizada em outro país;

(ii) o armazenamento de dados em *data centers* fisicamente localizados no exterior;

(iii) a terceirização de serviços de atendimento ao consumidor para empresa localizada no exterior;

(iv) a contratação de provedor de *cloud* de país estrangeiro[163].

Portanto, pode-se dizer que a regulação da transferência internacional, através das disposições do Capítulo V da LGPD, visa

[163] CHAVES, Luís Fernando Prado. Capítulo V – da Transferência Internacional de Dados. In. MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). **LGPD** – Lei Geral de Proteção de Dados – Comentada. 2ª ed. São Paulo: Revista dos Tribunais, 2019.. p. 296.

criar regras para qualquer comunicação de dados pessoais à pessoa física ou jurídica que não se submeta à jurisdição brasileira, em decorrência do fato de estarem em outro território que não o brasileiro.

Exemplificando, sob a ótica da LGPD, se uma empresa norte-americana, instalada no Brasil, necessitar transferir os dados pessoais coletados no país para outras empresas localizadas nos Estado Unidos, tal comunicação será considerada como uma transferência internacional de dados, tendo em vista que estes dados estariam saindo da jurisdição brasileira e sendo encaminhados a outra jurisdição, no caso, a norte-americana.

Além disso, existem outras normas setoriais que regulam a transferência internacional, como a Resolução nº 4.658/2018 do Banco Central do Brasil (BACEN), que deve ser aplicada, pelas instituições financeiras, de maneira suplementar ao disposto na LGPD.

A referida resolução prevê, por exemplo, quais seriam as disposições específicas que devem estar contidas nos contratos de processamento, armazenamento de dados e computação em nuvem firmados pelas instituições financeiras, incluindo:

(i) a indicação dos países e da região em cada país onde os serviços poderão ser prestados e os dados armazenados, processados e gerenciados;

(ii) a adoção de medidas de segurança para a transmissão e armazenamento destes dados a outros países;

(iii) a permissão de acesso do Banco Central do Brasil aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações, dentre outras disposições[164].

[164] BRASIL. **Resolução BCB nº 4.658/18**. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. Art. 17: Os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever: I - a indicação dos países e da região em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados; II - a adoção de medidas de segurança para a transmissão e armazenamento dos dados citados no inciso I; III - a manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes; IV - a obrigatoriedade, em caso de extinção do contrato, de: a) transferência dos dados citados no inciso I ao novo prestador de serviços ou à instituição contratante; e b) exclusão dos dados citados no inciso I pela empresa contratada substituída, após a transferência dos dados prevista na alínea "a" e a confirmação da integridade e da disponibilidade dos dados recebidos; V - o acesso da instituição contratante a: a) informações fornecidas pela empresa contratada, visando a verificar o cumprimento do disposto nos incisos I a III; b) informações relativas às certificações e aos relatórios de auditoria especializada, citados no art. 12, inciso II, alíneas "d" e "e"; e c) informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados, citados no art. 12, inciso II, alínea "f"; VI - a obrigação de a empresa contratada notificar a instituição contratante sobre a subcontratação de serviços relevantes para a instituição; VII - a permissão de acesso do Banco Central do Brasil aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações; VIII - a adoção de medidas pela instituição contratante, em decorrência de determinação do Banco Central do Brasil; e IX - a obrigação de a empresa contratada manter a instituição contratante permanentemente informada sobre

2. Bases legais de transferência de dados

Antes de se ater sobre as bases legais constantes dos incisos do art. 33 da Lei, é importante esclarecer que o tratamento de acordo com as bases legais dos artigos 7º e 11 não implica em uma obtenção automática de autorização para a transferência internacional de dados pessoais. Pela redação da Lei, pode-se interpretar que seriam etapas distintas do tratamento de dados, necessitando-se, pois, de uma avaliação separada para o enquadramento na hipótese legal do art. 33 que melhor se encaixasse às necessidades do agente de tratamento.

Desta feita, é possível dividir as hipóteses legais de transferência internacional em três grandes categorias[165]. A primeira, presente no inciso I do art. 33, diz respeito à possibilidade de transferência a países ou organismos internacionais com nível adequado de proteção de dados. Este nível deverá ser determinado pela ANPD seguindo os critérios contidos no art. 34 da Lei.

Uma segunda categoria, presente no inciso II do art. 33, é pertinente àquelas transferências a países que não possuem nível adequado de dados, fazendo-se necessária a apresentação de garantias contidas nas alíneas "a" a "d" do referido inciso.

---

eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

[165] CHAVES, Luís Fernando Prado. Capítulo V – da Transferência Internacional de Dados. In. MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). **LGPD** – Lei Geral de Proteção de Dados – Comentada. 2ª ed. São Paulo: Revista dos Tribunais, 2019. p. 294.

Já a terceira categoria, presente nos incisos III a IX do art. 33, diz respeito às outras hipóteses legais de transferência internacional de dados pessoais, independentemente do nível de proteção dos dados pessoais no país de destine, sendo que algumas encontram eco nas bases legais de tratamento do art. 7º e do art. 11 da Lei, enquanto outras tratam de hipóteses exclusivas para a realização de transferências internacionais, tais como aquelas presentes nos incisos V, VI e VIII deste artigo.

3. Nível adequado de proteção de dados

Inicialmente, cumpre destacar, conforme já comentado, que a própria LGPD busca enquadrar o Brasil como sendo um país com grau adequado de proteção de dados perante o cenário internacional, principalmente com relação à União Europeia, que através do RGPD buscou impor barreiras para a realização de transações entre o bloco econômico e os países que não possuem grau adequado de proteção de dados.

É interessante mencionar o caso dos Estados Unidos, que por não possuírem uma legislação federal de proteção de dados, não são considerados, pela União Europeia, um país que tenha um nível adequado de proteção de dados pessoais. Para tentar contornar essa situação, em 2015, foi estabelecido um acordo bilateral entre os EUA e a UE, o *Safe Harbour Agreement*, que foi posteriormente declarado insuficiente pela Corte de Justiça da União Europeia, após reclamações

de um cidadão europeu contra práticas de proteção de dados do Facebook, no que ficou conhecido como o caso *Schrems*[166].

Em 2016, foi então aprovado um novo acordo bilateral, o *Privacy Shield*, com disposições mais rígidas de proteção de dados, mas que também acabou por ser declarado inválido pela Corte de Justiça da EU em uma decisão de julho de 2020. Nesta decisão, a referida Corte enfrentou duas questões principais: (i) se os mecanismos existentes neste acordo estariam em conformidade com o nível de proteção exigido pelo RGPD, tendo em vista que nos EUA as autoridades podem vir a requerer dados de cidadãos europeus, sem indicativo de que a privacidade será protegida; e (ii) se as cláusulas padrão contratuais (*Standard Contractual Clauses*, em inglês) seriam instrumentos válidos para a transferência internacional de dados a países que possuem níveis inadequados de proteção de dados[167].

Diante destas considerações, considerando a possibilidade de tratamento ilegal de dados pessoais de cidadãos europeus por autoridades americanas, e também a impossibilidade de oposição dos

[166] UNIÃO EUROPEIA. **Corte de Justiça da União Europeia**. PRESS RELEASE Nº 117/15. Luxembourg, October 6, 2015. Judgment in Case C-362/14 Maximillian Schrems v Data Protection Commissioner. Disponível em: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf>. Acesso em: 28/01/2020.

[167] UNIÃO EUROPEIA. **Corte de Justiça da União Europeia**. Acórdão do Tribunal de Justiça (Grande Secção) de 16 de julho de 2020 (pedido de decisão prejudicial apresentado pela High Court – Irlanda) – Data Protection Commissioner / Facebook Ireland Limited, Maximillian Schrems. Disponível em: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=230683&pageIndex=0&doclang=pt&mode=req&dir=&occ=first&part=1&cid=1877782>. Acesso em: 28/01/2020.

cidadãos europeus a esta forma de tratamento feita pelos EUA, a Corte decidiu por invalidar a decisão da Comissão da União Europeia, a qual havia considerado adequado o nível de proteção de dados dos EUA, deixando praticamente sem efeitos as disposições do *Privacy shield* neste sentido.

Já com relação às cláusulas padrão contratuais, a Corte não as invalidou, considerando-as como sendo meios aptos a proteger os dados pessoais dos cidadãos europeus em transferências a países considerados inadequados, embora tenha expandido as obrigações dos controladores que queiram realizar transferências internacionais nestes termos, em consonância com o Considerando 109 do RGPD. Não existindo ou não sendo efetivas estas cláusulas, no entendimento da Corte, o controlador deverá ser devidamente responsabilizado por desconformidade com a legislação de proteção de dados pessoais[168].

[168] UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Considerando 109: A possibilidade de o responsável pelo tratamento ou o subcontratante utilizarem cláusulas-tipo de proteção de dados adotadas pela Comissão ou por uma autoridade de controlo não os deverá impedir de incluírem estas cláusulas num contrato mais abrangente, como um contrato entre o subcontratante e outro subcontratante, nem de acrescentarem outras cláusulas ou garantias adicionais desde que não entrem, direta ou indiretamente, em contradição com as cláusulas contratuais-tipo adotadas pela Comissão ou por uma autoridade de controlo, e sem prejuízo dos direitos ou liberdades fundamentais dos titulares dos dados. Os responsáveis pelo tratamento e os subcontratantes deverão ser encorajados a apresentar garantias suplementares através de compromissos contratuais que complementem as cláusulas-tipo de proteção.

Tomando por conta estas decisões paradigmáticas do tribunal europeu acerca dos acordos bilaterais com os Estados Unidos, tem-se que eles dificilmente serão considerados como parâmetros para a adaptação dos países não-adequados ao exigente nível europeu de proteção de dados, admitindo risco de decisões judiciais futuras declarando inválidas estas tratativas, assim como ocorreu na situação norte-americana. O Brasil, entretanto, está em uma boa posição para ser considerado adequado, tendo em vista que a LGPD encontra muitos paralelos com o RGPD, tendo inclusive sido nele inspirada[169].

4. Garantias de proteção de dados

Uma das disposições semelhantes entre a LGPD e o RGPD é justamente a previsão de garantias contratuais de proteção de dados, as quais, inclusive, estavam envolvidas na mencionada decisão europeia sobre o *Privacy Shied*.

Portanto, a LGPD prevê que a transferência internacional para os países que não possuírem nível adequado de proteção de dados poderá ser embasada em alguns documentos previstos nas alíneas do inciso II do artigo 33, cujo conteúdo deverá ser regulado pela ANPD em momento posterior, conforme disposto no artigo 35 da Lei.

[169] PERRONE, Christian. Dados internacionais na encruzilhada e o contexto brasileiro. **JOTA**, 2020. Disponível em <https://www.jota.info/coberturas-especiais/liberdade-de-expressao/dados-internacionais-na-encruzilhada-e-o-contexto-brasileiro-21072020#_ftn3>. Acesso em: 28/01/2020.

Já o RGPD exige que, para a transferência de dados a países que não possuem nível adequado de proteção de dados pessoais, sejam tomadas garantias adicionais nos contratos de transferência, tais como:

a) regras vinculativas aplicáveis às empresas;

b) cláusulas-tipo de proteção de dados adotadas pela Comissão;

c) cláusulas-tipo de proteção de dados adotadas por uma autoridade de controlo e aprovadas pela Comissão;

d) adoção de um código de conduta acompanhado de compromissos vinculativos e força executiva pelos controladores ou subcontratantes no país terceiro, no sentido de aplicarem as garantias adequadas;

e) um procedimento de certificação igualmente aprovado nos termos do RGPD, acompanhado de compromissos vinculativos e com força executiva assumidos pelos responsáveis pelo tratamento ou pelos subcontratantes no país terceiro no sentido de aplicarem as garantias adequadas[170].

[170] UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Artigo 46º: 1. Não tendo sido tomada qualquer decisão nos termos do artigo 45º, nº 3, os responsáveis pelo tratamento ou subcontratantes só podem transferir dados pessoais para um país terceiro ou uma organização internacional se tiverem apresentado garantias adequadas, e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes. 2. Podem

Considerando que o Brasil tem um grande superávit na balança comercial com a União Europeia, que em 2018 somou a quantia de 7,3 bilhões de dólares[171], não é de se estranhar que a LGPD tenha sido aprovada no mesmo ano, em um manifesto esforço para enquadrar o país como um "porto seguro" de dados pessoais perante a comunidade internacional.

Como já afirmado, a LGPD posiciona o Brasil como forte candidato a ser considerado um país com nível adequado de proteção de dados pessoais perante a comunidade internacional, o que, certamente, livraria os controladores brasileiros de um aumento de custos criados pelas diversas exigências do RGPD, que impactam diretamente a oferta de bens e serviços ao mercado europeu.

---

ser previstas as garantias adequadas referidas no n.º 1, sem requerer nenhuma autorização específica de uma autoridade de controlo, por meio de: a) Um instrumento juridicamente vinculativo e com força executiva entre autoridades ou organismos públicos; b) Regras vinculativas aplicáveis às empresas em conformidade com o artigo 47º; c) Cláusulas-tipo de proteção de dados adotadas pela Comissão pelo procedimento de exame referido no artigo 93.o, nº 2; d) Cláusulas-tipo de proteção de dados adotadas por uma autoridade de controlo e aprovadas pela Comissão pelo procedimento de exame referido no artigo 93.o, nº 2; e) Um código de conduta, aprovado nos termos do artigo 40.o, acompanhado de compromissos vinculativos e com força executiva assumidos pelos responsáveis pelo tratamento ou pelos subcontratantes no país terceiro no sentido de aplicarem as garantias adequadas, nomeadamente no que respeita aos direitos dos titulares dos dados; ou f) Um procedimento de certificação, aprovado nos termos do artigo 42.o, acompanhado de compromissos vinculativos e com força executiva assumidos pelos responsáveis pelo tratamento ou pelos subcontratantes no país terceiro no sentido de aplicarem as garantias adequadas, nomeadamente no que respeita aos direitos dos titulares dos dados. [...]

[171] Brasil teve superávit de US$ 7,3 bi em comércio com UE em 2018. **UOL**. Disponível em: <https://economia.uol.com.br/noticias/reuters/2019/06/28/brasil-teve-superavit-de-us73-bi-em-comercio-com-ue-em-2018.htm>. Acesso em 16.12.2020.

Entretanto, para que possa obter esse reconhecimento de maneira efetiva, é necessário impor barreiras para a exportação de dados pessoais a países que não forneçam nível adequado de proteção de dados.

Nesse sentido, o parágrafo único do artigo 33 permite o requerimento, tanto das pessoas jurídicas de direito público, mencionadas no artigo 1º da LAI, quanto dos controladores, para que a ANPD avalie o nível de proteção de determinado país ou organismo internacional[172].

Enquanto não é reconhecido pela União Europeia como um país que possui nível adequado de proteção de dados, o Brasil será considerado menos atrativo, em termos de investimentos e trocas comerciais, do que aqueles países que já contam com o reconhecimento da Comissão Europeia, o que é o caso da Argentina e do Uruguai, que inclusive fazem parte do Mercosul, tendo em vista a necessidade de adoção de arranjos contratuais ou mesmo submissão a processos de certificação por parte dos controladores brasileiros[173].

---

[172] Da mesma forma que no §6º do art. 18, a lei menciona o termo "responsáveis", tendo em vista a ocorrência de um lapso no processo legislativo. O que houve foi uma adaptação terminológica do termo no decorrer do processo legislativo, que foi substituído pelo termo "controladores".

[173] VIOLA, Maria. **Transferência de dados entre Europa e Brasil**: Análise da Adequação da Legislação Brasileira. Rio de Janeiro: ITS Rio, 2019. Disponível em: <https://itsrio.org/wp-content/uploads/2019/12/Relatorio_UK_Azul_INTERACTIVE_Justificado.pdf>. Acesso em: 16.12.2020.

5. Demais hipóteses legais de transferência

Sobre as demais bases legais de transferência internacional de dados, o inciso IV do art. 33 prevê que a proteção de dados pessoais será relativizada quando estiver em risco a vida ou a saúde do titular, assim como dispõem o inciso VII do art. 7º e o inciso II, alínea "e" do art. 11 da Lei.

O inciso V do artigo 33, por sua vez, prevê que a ANPD poderá autorizar diretamente determinadas transferências internacionais de dados. Embora não reste claro quais as circunstâncias exatas em que a autoridade nacional poderá autorizar estas transferências, caso se entenda que deve-se seguir, minimamente, as garantias previstas no referido inciso II, tal disposição legal restaria sem efeito prático.

Já os incisos III, VI e VII do artigo 33 dizem respeito à autorização para a transferência internacional de dados pela Administração Pública. Desta forma, o inciso III permite a transferência internacional na hipótese de cooperação jurídica com outros países, dando-se a entender uma certa semelhança na dispensa da aplicabilidade desta Lei, disposta no artigo 4º, inciso III.

Os incisos VI e VII do art. 33, no que lhes diz respeito, fazem alusão à transferência por força da execução de tratados e acordos internacionais, bem como para a execução de políticas públicas, hipótese esta que se assemelha também àquelas constantes dos artigos 7º e 11 da LGPD.

O inciso VIII trata do fornecimento de consentimento pelo titular para a transferência internacional de dados. Entretanto, o agente de tratamento deve sopesar bem a escolha da base legal do consentimento, como já comentado neste livro, tendo em vista todas as exigências e inseguranças decorrentes desta hipótese de tratamento, considerando ainda que além de ser livre, informado e inequívoco, o consentimento, em um contexto de transferência internacional, deverá ser destacado[174].

Ao invés de se utilizar do consentimento dos titulares, talvez possa ser considerado para os agentes de tratamento, como uma alternativa mais vantajosa e que importaria menos riscos, a utilização das garantias previstas no inciso II do art. 33, combinadas com o inciso IX do art. 7º da Lei.

Por fim, o inciso IX do art. 33 faz referência às bases legais contidas nos incisos II, V e VI do art. 7º desta Lei, que dizem respeito, respectivamente: (i) ao cumprimento de obrigação legal ou regulatória pelo controlador; (ii) à necessidade de execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular de dados; e (iii) ao exercício regular de direitos em processo judicial, administrativo ou arbitral.

[174] Conforme "Parecer da Comissão Especial Destinada a Proferir Parecer ao Projeto de Lei 4.060/2012". p. 39. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=>. Acesso em 18.19.2020.

Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do caput do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração:

I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;

II - a natureza dos dados;

III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;

IV - a adoção de medidas de segurança previstas em regulamento;

V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e

VI - outras circunstâncias específicas relativas à transferência.

A decisão da ANPD de enquadrar determinado país como tendo um nível adequado de proteção de dados pessoais deve ser fundamentada com base neste artigo, analisando-se inclusive a capacidade de efetivação da Lei no país estrangeiro (*enforcement*), conforme dispõe o inciso V.

De fato, pudessem os dados ser livremente transferidos do Brasil ao exterior, sem qualquer restrição, certamente haveria uma burla à proteção de dados pessoais instituída pela LGPD, pois bastaria que os dados fossem tratados em um país não adequado para que fosse possível fugir da incidência das regras protetivas nele previstas, o que tornaria totalmente inócuas as garantias concedidas aos titulares dos dados.

Art. 35. A definição do conteúdo de cláusulas-padrão contratuais, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, a que se refere o inciso II do caput do art. 33 desta Lei, será realizada pela autoridade nacional.

§ 1º Para a verificação do disposto no caput deste artigo, deverão ser considerados os requisitos, as condições e as garantias mínimas para a transferência que observem os direitos, as garantias e os princípios desta Lei.

§ 2º Na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação da autoridade nacional, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento, quando necessário.

§ 3º A autoridade nacional poderá designar organismos de certificação para a realização do previsto no caput deste artigo, que permanecerão sob sua fiscalização nos termos definidos em regulamento.

§ 4º Os atos realizados por organismo de certificação poderão ser revistos pela autoridade nacional e, caso em

desconformidade com esta Lei, submetidos a revisão ou anulados.

§ 5º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no caput deste artigo serão também analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos §§ 1º e 2º do art. 46 desta Lei.

Segundo o disposto neste artigo, a ANPD deverá definir o conteúdo das cláusulas-padrão contratuais, bem como validar cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais e selos, certificados e códigos de conduta, podendo, inclusive, requisitar informações suplementares ou realizar a verificação das próprias operações de transferência, quando bem entender necessário.

Também deverá ser observado, na determinação e validação dos instrumentos indicados no inciso II do art. 33 pela ANPD, o princípio da *privacy by design*, bem como os demais padrões de segurança da informação que envolvem medidas técnicas e organizacionais de proteção de dados, conforme previsão dos §§1º e 2º do art. 46 da Lei.

Art. 36. As alterações nas garantias apresentadas como suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no inciso II do art. 33 desta Lei deverão ser comunicadas à autoridade nacional.

O art. 36 coloca mais uma disposição acerca dos documentos elencados no inciso II do art. 33, devendo quaisquer alterações nas disposições constantes nestas garantias contratuais ser devidamente comunicadas à ANPD.

A Lei não impede que um controlador se utilize de cláusulas padrão que envolvam a contratação de seguros, por exemplo, enquanto aguarda uma autorização específica da ANPD, definida pelo inciso V do art. 33, para a realização de determinada transferência internacional. Embora os detalhes desta autorização específica ainda não estejam definidos, é certo que, uma vez autorizada a transferência diretamente pela autoridade nacional, o controlador poderia cancelar o seguro, tendo em vista a alteração da base legal, contanto que comunicasse este cancelamento à ANPD, por força deste art. 36.

CAPÍTULO VI - DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS

Seção I - Do Controlador e do Operador

Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

1. Controlador e operador

O capítulo VI visa tratar, de forma específica, as disposições atinentes ao controlador, ao operador e também ao encarregado de dados pessoais, individualizando as condutas e responsabilidades de cada um destes agentes no tratamento de dados pessoais.

Para deixar mais claras as atribuições de cada um, considere-se o exemplo de um titular que faça uma compra em um *e-commerce*, o qual solicita alguns de seus dados pessoais para a execução do contrato, como o seu nome, endereço e dados bancários. Nessa situação o *e-commerce* deverá compartilhar os dados pessoais do titular com uma empresa de gerenciamento de meios de pagamentos e com uma empresa de logística, a qual realizará a entrega do produto.

No caso narrado, as empresas de meios de pagamento e de logística seriam operadoras, pois agiriam apenas sob as estritas recomendações do controlador, no caso o *e-commerce*, que determinaria a forma e a finalidade com que os dados do titular deveriam ser tratados.

Importante ressaltar também que poderá haver algumas situações em que exista mais de um controlador simultaneamente, ou seja, pode haver mais de um agente de tratamento que tome as decisões pertinentes ao tratamento de dados dos titulares, o que, para fins de adequação à LGPD, deve ser observado em cada caso concreto.

2. Registros de tratamento

Os registros, que também são denominados "*logs*" ou "*logs* de sistemas" em uma linguagem mais técnica, são especialmente importantes para o rastreio de quaisquer alterações que podem ser realizadas nos sistemas da instituição, permitindo a investigação de incidentes de segurança e a responsabilização de eventuais infratores.

Nesse sentido, a disposição sobre os registros das operações de tratamento, contida no *caput* do art. 37, está intimamente relacionada com o princípio da responsabilização e prestação de contas, previsto no art. 6º, inciso X da LGPD, além de serem uma boa fonte de constituição de provas para a atuação dos agentes de tratamento em procedimentos administrativos ou judiciais.

No entanto, diferentemente da legislação europeia, que restringiu essa obrigação de manutenção dos registros a determinados agentes de tratamento[175], a LGPD não individualizou quais seriam os agentes de tratamento obrigados a manter os registros das operações de tratamento. Logo, todos os agentes de tratamento estariam obrigados, sendo necessária a criação ou alteração de procedimentos internos de registro de tratamento de dados pessoais.

Para tal, é aconselhável a criação de políticas e normas específicas para o armazenamento e categorização destes registros, a

[175] UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Artigo 30º: Registos das atividades de tratamento. 1. Cada responsável pelo tratamento e, sendo caso disso, o seu representante conserva um registo de todas as atividades de tratamento sob a sua responsabilidade. Desse registo constam todas seguintes informações: a) O nome e os contactos do responsável pelo tratamento e, sendo caso disso, de qualquer responsável conjunto pelo tratamento, do representante do responsável pelo tratamento e do encarregado da proteção de dados; b) As finalidades do tratamento dos dados; c) A descrição das categorias de titulares de dados e das categorias de dados pessoais; d) As categorias de destinatários a quem os dados pessoais foram ou serão divulgados, incluindo os destinatários estabelecidos em países terceiros ou organizações internacionais; e) Se for aplicável, as transferências de dados pessoais para países terceiros ou organizações internacionais, incluindo a identificação desses países terceiros ou organizações internacionais e, no caso das transferências referidas no artigo 49º, nº 1, segundo parágrafo, a documentação que comprove a existência das garantias adequadas; f) Se possível, os prazos previstos para o apagamento das diferentes categorias de dados; g) Se possível, uma descrição geral das medidas técnicas e organizativas no domínio da segurança referidas no artigo 32º, nº 1. 5. As obrigações a que se referem os nº s 1 e 2 não se aplicam às empresas ou organizações com menos de 250 trabalhadores, a menos que o tratamento efetuado seja suscetível de implicar um risco para os direitos e liberdades do titular dos dados, não seja ocasional ou abranja as categorias especiais de dados a que se refere o artigo 9º, nº 1, ou dados pessoais relativos a condenações penais e infrações referido no artigo 10º.

fim de que se possa rastrear e identificar os responsáveis por quaisquer alterações realizadas nos sistemas da organização.

Assim, na ocorrência de eventuais incidentes de segurança da informação, estes registros possibilitarão que o agente de tratamento eventualmente reivindique ações de regresso contra os culpados, conforme dispõe o art. 42, §4º da LGPD, que será a seguir analisado.

Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

1. Relatório de Impacto à Proteção de Dados Pessoais

O art. 38 trata de disposições específicas acerca do Relatório de Impacto à Proteção de Dados Pessoais – RIPD, cujo conceito se encontra no art. 5º, inciso XVII da Lei. À primeira vista, este art. 38 pode parecer redundante frente ao art. 37, considerando que ambos tratam de documentações referentes às operações da instituição.

Entretanto, os documentos mencionados possuem finalidades diferentes: enquanto o registro das operações de tratamento se presta a documentar o tratamento para fins de auditoria e prestação de contas pelo agente de tratamento, o mencionado relatório foca, de forma

específica, no mapeamento de riscos relacionados a todas as operações de tratamento de dados pessoais, sendo recomendável que os controladores o redijam à luz das disposições da norma técnica ISO/IEC 27001, que trata de um padrão internacional de gerenciamento da segurança da informação.

Embora a redação do art. 38 leve a entender que o controlador deva elaborar o RIPD apenas quando a ANPD o solicitar, é importante destacar que esta disposição não faria sentido se confrontada com a definição contida no inciso XVII do art. 5º da Lei. Isto porque o relatório deveria ser elaborado, em tese, quando existentes quaisquer riscos às liberdades civis ou aos direitos fundamentais dos titulares, direitos estes que incluem o próprio direito à privacidade e à proteção de dados. Deste modo, qualquer tipo de risco à privacidade poderia ser encarado como sendo um motivo determinante à elaboração de um RIPD.

Uma vez considerada a elaboração do RIPD, na prática, como obrigatória, pode-se imaginar um futuro em que a ANPD solicite estes documentos para ao menos realizar uma triagem de quais agentes de tratamento estariam minimamente adequados, com vistas a identificar potenciais infrações à Lei e aplicar as sanções previstas no art. 52.

2. Conteúdo do RIPD

As informações contidas no parágrafo único do art. 38 tratam das informações que devem necessariamente estar contidas no relatório

de impacto, que incluem os padrões de segurança utilizados no tratamento de dados pessoais – principalmente nas operações de transferência e compartilhamento de dados – além das avaliações acerca da necessidade e da proporcionalidade daquele determinado tratamento frente a finalidade almejada pelo controlador.

Importante salientar que o legislador não visou proibir o processamento de dados com alguns riscos, contanto que sejam estes riscos necessariamente mapeados, mitigados e, se possível, eliminados pelo agente de tratamento. Neste contexto, antes de iniciar qualquer tratamento que possa dar ensejo a um grau elevado de risco, é recomendável que a organização elabore um novo relatório de impacto e, de posse deste, realize uma consulta junto à ANPD, que possivelmente seguirá os mesmos trâmites de consultas tributárias perante a Receita Federal do Brasil (RFB).

Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

1. Operador de dados pessoais

O artigo 39 dispõe, de maneira mais clara, que o operador não poderá ter qualquer nível de discricionariedade no tratamento dos dados fornecidos pelo controlador. Ressalte-se que, independentemente de qualquer instrução do controlador, o operador deverá adotar todas as medidas adequadas de conformidade com a LGPD, incluindo aquelas boas práticas previstas no art. 46 da Lei.

Caso o operador atue com qualquer nível de discricionariedade, desvirtuada daquela finalidade específica definida pelo controlador, logo ele será considerado, para todos os fins contidos na Lei, como um controlador de dados pessoais, no que diz respeito aos dados tratados de forma ilícita.

A título de exemplificação, se a empresa de entregas, mencionada no comentário do art. 37, começasse a cruzar os dados recebidos do *e-commerce* com outras bases de dados, a fim de criar um perfil de consumo dos titulares, se converteria em uma controladora com relação aos dados que foram compartilhados.

Caso comprovado que o *e-commerce* em questão teria agido em conformidade com as melhores práticas de segurança e proteção de dados, poderia ser eximido da responsabilidade proveniente do tratamento indevido realizado pela empresa de entregas.

2. Adequação dos operadores à LGPD

As disposições contidas na LGPD devem ser especialmente observadas pelos operadores, cujos exemplos não se limitam apenas à área de tecnologia da informação, mas também podem incluir escritórios de contabilidade, corretoras de seguros e administradoras de planos de saúde, dentre outras.

No setor contábil, há uma observação interessante a ser feita, tendo em vista que a relação jurídica estabelecida entre os escritórios de contabilidade e os seus clientes pode ser entendida como uma relação de consumo, vez que, nestes casos, a pessoa contratante, seja ela física ou jurídica, seria hipossuficiente frente ao conhecimento técnico do escritório contábil, e também seria a destinatária final dos serviços.

Entretanto, a aplicação do CDC nestas relações acaba por revelar diversos riscos às atividades destes escritórios, incluindo a possibilidade de inverter-se o ônus probatório em favor da controladora, que seria considerada consumidora nesta relação[176]. Daí

[176] BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Art. 6º São direitos básicos do consumidor: VIII

a importância de os operadores tomarem todas as medidas cabíveis para se adequarem à LGPD.

- a facilitação da defesa de seus direitos, inclusive com a inversão do ônus da prova, a seu favor, no processo civil, quando, a critério do juiz, for verossímil a alegação ou quando for ele hipossuficiente, segundo as regras ordinárias de experiências.

Art. 40. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.

O art. 40 trata de outro dispositivo de eficácia contida, ou seja, de uma disposição que necessitará de posterior regulamentação pela ANPD, e diz respeito à portabilidade dos dados pessoais dos titulares, a fim de prover uma transferência eficiente de dados entre agentes de tratamento. Esta portabilidade acontecerá sempre a pedido do titular, com a finalidade de efetivação do seu direito de autodeterminação informacional e do controle sobre os seus dados pessoais.

A definição de padrões de interoperabilidade de dados já é uma realidade em alguns setores econômicos regulados, como o de telefonia móvel ou de planos de saúde, cujas respectivas agências reguladoras, a Agência Nacional de Telecomunicações (ANATEL) e a Agência Nacional de Saúde Suplementar (ANS), já vêm atuando a fim de definir as condições de portabilidade de dados pessoais dos usuários.

É de se ressaltar também as iniciativas recentes do Banco Central para efetivar a sistemática do "*open banking*" no Brasil, buscando justamente estabelecer padrões de interoperabilidade de dados entre as instituições participantes do sistema financeiro nacional. Portanto, tendo em vista estas iniciativas de outros órgãos, seria correto

afirmar que a ANPD ficaria incumbida de criar padrões de interoperabilidade para os setores não regulados da economia, enquanto forneceria o suporte técnico aos outros órgãos reguladores.

Seção II - Do Encarregado pelo Tratamento de Dados Pessoais

Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

§ 2º As atividades do encarregado consistem em:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - receber comunicações da autoridade nacional e adotar providências;

III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

§ 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o

porte da entidade ou o volume de operações de tratamento de dados.

1. Nomeação de um Encarregado pelo Tratamento de Dados Pessoais

Assim como aquela disposição sobre os registros de tratamento, a LGPD não determinou de forma detalhada quais controladores estariam obrigados a nomear um encarregado pelo tratamento de dados pessoais. Entretanto, quando analisado o §3º deste artigo fica claro que todos os agentes deverão nomear um DPO, até que haja algum pronunciamento por parte da ANPD sobre as eventuais dispensas deste sujeito responsável pela proteção de dados pessoais.

Importante ressaltar que na legislação europeia há uma discriminação clara de quais os agentes de tratamento estão obrigados a nomear um DPO, havendo inclusive a possibilidade de nomeação de um só DPO para todo um grupo econômico[177]. O regramento brasileiro

[177] UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).** Artigo 37º: Designação do encarregado da proteção de dados. 1. O responsável pelo tratamento e o subcontratante designam um encarregado da proteção de dados sempre que: a) O tratamento for efetuado por uma autoridade ou um organismo público, excetuando os tribunais no exercício da sua função jurisdicional; b) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou c) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados nos termos do artigo 9º e de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10º 2. Um grupo empresarial pode também designar um único encarregado da proteção de dados desde que haja

possivelmente seguirá estas disposições da legislação europeia, o que deverá ser feito a partir de uma regulamentação posterior da ANPD, conforme se depreende do §3º.

A única hipótese de dispensa de nomeação de um DPO presente na Lei, a princípio, diz respeito aos operadores de dados pessoais, tendo em vista a omissão do legislador em mencionar o operador no *caput* do artigo 41, enquanto faz alusão a ambos os agentes de tratamento de forma expressa em outros pontos da Lei, como no art. 7º, §6º, no art. 37, no art. 43 e no art. 50, §1º.

Contudo, esta hipótese de dispensa dificilmente poderia ser observada no caso concreto, sendo extremamente raro que uma empresa que seja operadora em determinada circunstância não seja enquadrada como controladora em outras situações, como nos casos em que houver qualquer tratamento de dados em seu âmbito interno, o que inclui o cumprimento de obrigações trabalhistas, por exemplo.

Desta forma, em relação a seus funcionários, seria aquele operador enquadrado como controlador, possuindo, pois, a obrigação de nomear um DPO. Uma outra situação seria nos casos de se manter uma base com os dados pessoais de representantes comerciais, situação em que o agente de tratamento também seria enquadrado como controlador com relação a estes dados. Diante destas considerações,

---

um encarregado da proteção de dados que seja facilmente acessível a partir de cada estabelecimento. Disponível em: < https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>. Acesso em 28/01/2021.

pode-se afirmar que as chances de uma determinada operadora não ter que nomear um encarregado de dados, nas condições que estão postas pela Lei, são muito remotas.

Portanto, a análise feita pelo agente de tratamento quanto à obrigatoriedade de nomeação de um DPO, deverá ser devidamente registrada e documentada. Também, sempre que a empresa optar por lançar no mercado novos produtos ou serviços que importem em um tratamento de dados pessoais, deverá reanalisar a sua decisão de nomear um encarregado.

Por último, é importante frisar que esta dispensa aos operadores não significa que eles não terão de obedecer a todas as outras disposições atinentes à proteção de dados pessoais.

2. Funções do Encarregado pelo Tratamento de Dados Pessoais

O §2º do artigo 41 discorre acerca de algumas das funções que poderão ser realizadas pelo encarregado de dados, dentre as quais podemos adicionar[178]:

> (i) o assessoramento na emissão do relatório de impacto à proteção de dados pessoais (RIPD);

[178] BRUNO. Marcos Gomes da Silva. Capítulo VI – Dos Agentes de Tratamento de Dados Pessoais. In. MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). **LGPD** – Lei Geral de Proteção de Dados – Comentada. 2ª ed. São Paulo: Revista dos Tribunais, 2019. p. 318.

(ii) a emissão opiniões e pareceres técnicos acerca da proteção de dados pessoais pela entidade;

(iii) o monitoramento da conformidade das atividades de tratamento de acordo com as legislações e regulamentações aplicáveis;

(iv) a recomendação de elaboração de relatórios de impacto à proteção de dados pessoais (RIPD) sempre que necessário.

Por ser uma figura tão importante para a efetivação dos direitos dos titulares, e também para a efetivação da Lei de maneira geral, o §1º prevê que todas as informações relacionadas ao DPO deverão estar facilmente disponíveis, de forma clara e objetiva, e de preferência no *site* da empresa.

Esta função poderá ser exercida por um funcionário da própria organização ou por uma empresa terceirizada, conforme o modelo conhecido como DPO *as a service*, muito comum nos países europeus.

Frise-se que para a nomeação deste DPO é importante a avaliação dos seus conhecimentos técnicos e jurídicos sobre segurança da informação e proteção de dados pessoais. A Lei também é omissa quanto a possibilidade de um DPO atender a mais de uma empresa ao mesmo tempo e, portanto, tal arranjo pode ser considerado permitido.

É importante que este encarregado possa exercer as suas funções de maneira independente, e que tenha acesso à alta

administração, a fim de se evitar eventuais conflitos de interesses e prover maior efetividade ao programa de *compliance* com a proteção e dados pessoais da organização.

Outrossim, a responsabilidade deste DPO é subjetiva, ou seja, só existirá caso comprovado que teria agido em flagrante má-fé, ou que teria se omitido de alguma forma em cumprir com os seus deveres na proteção da privacidade e dos dados pessoais dos titulares.

Seção III - Da Responsabilidade e do Ressarcimento de Danos

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:

I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

§ 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de

produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

§3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do *caput* deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.

§4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

1. Responsabilidade do agente de tratamento

Para a LGPD, a responsabilidade civil dos agentes de tratamento está relacionada diretamente com uma conduta lesiva a um determinado interesse juridicamente tutelado, seja este interesse patrimonial, moral, individual ou coletivo. Em geral, a responsabilidade do agente de tratamento será subjetiva; no entanto, nas situações em que ele também for considerado fornecedor no âmbito de uma relação de consumo, a sua responsabilidade será objetiva[179].

[179] BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Art. 12: O fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos.

O vínculo estreito existente entre a proteção de dados pessoais e o direito de consumidor deve ser muito bem avaliado pelos agentes de tratamento, tendo em vista que a aplicação do CDC pode tornar um eventual litígio, envolvendo dados pessoais, muito mais custoso para a organização.

Neste sentido, é possível inferir a multiplicação de processos relacionados com a utilização e tratamento de dados pessoais, tendo em vista que os aspectos jurídicos do que configura um dano a determinada pessoa perfaz uma questão controvertida na jurisprudência nacional, o que deve ser agravado com a existência de danos relacionados a violações de deveres de proteção de dados pessoais[180].

De fato, existem diversos tipos de danos que podem ocorrer nesta nova seara, relacionados com a divulgação de informações sigilosas ou constrangedoras pertencentes aos titulares, tais como receituários médicos, históricos de compras ou dados de geolocalização, que tem o condão de revelar as intimidades dos titulares e causar-lhes um eventual dano moral.

[180] SCHREIBER, Anderson. Resposnabilidade civil na Lei Geral de Proteção de Dados Pessoais. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (orgs**). Tratado de Proteção de Dados Pessoais**. 1º ed. Rio de Janeiro: Forense, 2021. p. 324.

2. Responsabilidade solidária e direito de regresso

A responsabilidade solidária existe para proteger o titular de dados pessoais, que, pela sua hipossuficiência técnica, pode encontrar dificuldades em determinar quem exatamente foi o causador do dano[181].

Nesse sentido, o §1º do artigo 42 preceitua algumas hipóteses de responsabilização solidária entre os agentes de tratamento, que remetem à lógica do Direito do Consumidor, a fim de assegurar a efetividade da indenização ao titular de dados na ocorrência de qualquer tipo de dano[182].

O inciso I prevê que o operador que não cumprir as determinações do controlador de maneira estrita, utilizando os dados para qualquer outra finalidade que não aquela que foi contratado, se equipara ao controlador. Portanto, para essa nova operação de tratamento realizada de maneira ilegal, o operador se torna, para todos os efeitos legais, um controlador de dados.

Já o inciso II, dispõe sobre a possibilidade de dois ou mais controladores atuarem conjuntamente, hipótese na qual eles responderão de maneira solidária. Como esta forma de

[181] BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002.** Institui o Código Civil. Art. 264. Há solidariedade, quando na mesma obrigação concorre mais de um credor, ou mais de um devedor, cada um com direito, ou obrigado, à dívida toda.
[182] SCHREIBER, Anderson. Resposnabilidade civil na Lei Geral de Proteção de Dados Pessoais. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (orgs). **Tratado de Proteção de Dados Pessoais**. 1º ed. Rio de Janeiro: Forense, 2021. pp. 333.

responsabilidade possibilita o pagamento de toda a dívida por qualquer um dos responsáveis, a parte que não deu causa ao dano pode efetuar seu direito de regresso contra a parte que deu causa ao dano. Seria o caso de um controlador que paga a indenização inteira por um incidente causado por conduta de um determinado operador de dados.

Nesse caso, conforme o disposto no §4º do artigo em comento, o controlador tem o direito de receber a quantia do operador em ação judicial de regresso, ou seja, em uma ação judicial autônoma.

3. Inversão do ônus da prova

Mais uma disposição que remete à lógica consumerista[183], o §2º prevê a possibilidade de inversão do ônus da prova, tendo em vista a presunção de vulnerabilidade do titular de dados. Desta feita, é de suma importância o registro e a documentação de todas as medidas de adequação e conformidade adotadas pelo agente de tratamento, para que, em um processo judicial, possa demonstrar que realizou o tratamento de forma adequada[184].

---

[183] BRASIL. **Lei nº 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Art. 6º: São direitos básicos do consumidor: [...] VIII - a facilitação da defesa de seus direitos, inclusive com a inversão do ônus da prova, a seu favor, no processo civil, quando, a critério do juiz, for verossímil a alegação ou quando for ele hipossuficiente, segundo as regras ordinárias de experiências.

[184] SCHREIBER, Anderson. Resposnabilidade civil na Lei Geral de Proteção de Dados Pessoais. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (orgs). **Tratado de Proteção de Dados Pessoais**. 1º ed. Rio de Janeiro: Forense, 2021. pp. 333-334.

Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:

I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;

II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou

III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

O artigo 43 invoca as excludentes de responsabilidade do agente de tratamento, de maneira muito similar às excludentes de responsabilidade contidas no CDC[185].

O inciso I diz respeito à ausência de autoria, ou seja, é excluída a responsabilidade se o dano não foi realizado por aquele agente determinado. Porém, a prova de que alguém não realizou algo é de

[185] BRASIL. **Lei nº 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Art. 12: O fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos. [...] §3° O fabricante, o construtor, o produtor ou importador só não será responsabilizado quando provar: I - que não colocou o produto no mercado; II - que, embora haja colocado o produto no mercado, o defeito inexiste; III - a culpa exclusiva do consumidor ou de terceiros.

difícil materialização, o que demonstra a importância de medidas de mitigação de riscos e adequação à Lei.

Tome-se o exemplo de um síndico de um prédio que transfere, de forma ilegal, a relação de moradores do condomínio a uma empresa que oferece serviços de TV por assinatura. Ao ser questionada por determinado titular de como teria conseguido seus dados, a empresa de TV por assinatura poderia apontar a construtora do condomínio, que não teria qualquer relação com o incidente de segurança.

Para provar que efetivamente não tratou ou transferiu quaisquer dados dos condôminos de forma ilegal, a construtora teria que, no mínimo, demonstrar a sua adequação à LGPD e todas as medidas de segurança que realiza no tratamento de dados pessoais.

Por sua vez, o inciso II diz respeito à ausência de violações à LGPD, ressaltando a importância de uma adequação bem feita à legislação para a mitigação de riscos patrimoniais e reputacionais. Se há um incidente de vazamento de dados, mas a empresa demonstra através de documentos e relatórios que realizou todas as medidas possíveis para evitar tal situação, é possível que seja absolvida ou tenha sua condenação reduzida com base nesse inciso.

Já o inciso III diz respeito à ausência de nexo causal entre a conduta do agente de tratamento e o dano. A doutrina, já há algum tempo, considera que a adoção de medidas de segurança eficientes e razoáveis tem o condão de excluir a responsabilidade por fato de

terceiros, tendo em vista que nenhum sistema de segurança pode ser considerado 100% eficaz[186].

[186] LAGO JR., Antônio. **Responsabilidade civil por atos ilícitos na Internet**. São Paulo: Ed. LTr, 2001.

Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

I - o modo pelo qual é realizado;

II - o resultado e os riscos que razoavelmente dele se esperam;

III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

O artigo 44 se relaciona de maneira direta com as hipóteses de excludente de responsabilidade prevista no inciso II do art. 43, pois a demonstração de que o tratamento de dados não teria sido irregular, ou seja, que teria observado a legislação e correspondido às expectativas de segurança do titular, teria o condão de afastar a responsabilidade do agente de tratamento.

Portanto, para a interpretação do artigo, deve-se observar a forma de tratamento dos dados pessoais, bem como as expectativas do titular quanto a este tratamento, que devem ser verificadas no caso

concreto[187]. Por exemplo, a expectativa de um titular no tratamento de seus dados por um banco digital é de que se tenha uma proteção muito maior do que no tratamento de seus dados por um pequeno comércio local.

Outra questão importante de análise é a verificação da aplicação do estado da técnica disponível à época do tratamento, ou seja, se foram tomadas as medidas razoáveis de proteção disponíveis.

Assim, o tratamento só será irregular se as medidas técnicas e organizacionais de segurança dos dados e mitigação de riscos estiverem defasadas e desatualizadas. Desta maneira, é importante o monitoramento e atualização periódicos das medidas de conformidade da entidade, para que se possa acompanhar o estado da técnica na área da segurança da informação e mitigar os riscos provenientes do tratamento de dados pessoais.

[187] BRUNO, Marcos Gomes da Silva. Capítulo VI – Dos Agentes de Tratamento de Dados Pessoais. In. MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). **LGPD** – Lei Geral de Proteção de Dados – Comentada. 2ª ed. São Paulo: Revista dos Tribunais, 2019. p. 330.

Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.

Este artigo deixa claro que a LGPD está inserta no microssistema de proteção dos direitos do consumidor, como alguns outros dispositivos de inversão do ônus da prova e previsão de responsabilidade objetiva também demonstram.

Importante destacar os artigos 2º e 17 do CDC[188], que invocam as figuras do consumidor como a pessoa ou coletividade de pessoas que adquire um produto ou serviço como sendo seu destinatário final, equiparando-se aos consumidores todas as vítimas de algum evento que acarrete algum tipo de dano. Portanto, uma instituição bancária que tem os dados de seus clientes vazados, por exemplo, deverá responder por uma responsabilidade frente aos danos causados aos indivíduos tanto como consumidores quanto como titulares de dados.

[188] BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Art. 2°: Consumidor é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final. Parágrafo único. Equipara-se a consumidor a coletividade de pessoas, ainda que indetermináveis, que haja intervindo nas relações de consumo. [...] Art. 17: Para os efeitos desta Seção, equiparam-se aos consumidores todas as vítimas do evento.

CAPÍTULO VII - DA SEGURANÇA E DAS BOAS PRÁTICAS

Seção I - Da Segurança e do Sigilo de Dados

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

1. Medidas técnicas e administrativas

A manutenção da segurança dos dados pessoais dos titulares se insere no escopo maior da segurança da informação, tendo em vista que esses dados são, em si, informações sobre determinados indivíduos. A definição comum que se costuma dar a segurança da informação é de que seria um conjunto de técnicas e medidas apropriadas para a proteção de algumas características da informação, como a sua confidencialidade, a sua integridade e a sua disponibilidade. Outras características podem também ser destacadas, como o não-repúdio, a autenticidade e a confiabilidade[189].

Neste diapasão, pode-se dizer que a característica da "confidencialidade" trata do grau com que a informação é protegida contra o acesso de terceiros não-autorizados, enquanto a característica da "integridade" trata do grau com que a informação mantém o seu caráter original de maneira intacta. Por fim, a característica da "disponibilidade" trata do grau com que as informações podem ser facilmente acessadas e recuperadas quando solicitado[190].

Para entender mais a fundo o que realmente constitui a segurança da informação, faz-se necessário delinear quatro conceitos, quais sejam:

---

[189] BEAL, Adriana. **Segurança da informação**: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo:Atlas, 2005. p. 52.
[190] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002**. Tecnologia da Informação. Código de Prática para Gestão da Segurança da Informação. Rio de Janeiro, 2013.

(i) vulnerabilidade, que pode ser entendida como qualquer fraqueza que atinja um determinado sistema, processo, ambiente ou protocolo de negócios;

(ii) ameaças, que são potenciais situações que podem vir a atingir determinada vulnerabilidade do negócio;

(iii) incidente, quando a ameaça se concretiza sobre determinada vulnerabilidade; e

(iv) controles, que são medidas utilizadas para impedir ou mitigar a ocorrência de incidentes, bem como para reduzir as suas consequências negativas[191].

Desta forma, muito do que é disposto no Capítulo VII da Lei, sobre segurança e boas práticas, encontra paralelos com o disposto nas normas da família ISO/IEC 27000, as quais dispõem, de forma geral, sobre a implementação de sistemas de gestão da segurança da informação no âmbito de qualquer organização, incluindo o estabelecimento de medidas físicas, técnicas e organizacionais para a proteção da confidencialidade, integridade e disponibilidade da informação.

[191] MENKE, Fabiano; GOULART, Guilherme Damásio. Segurança da Informação e Vazamento de Dados. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (orgs). **Tratado de Proteção de Dados Pessoais.** 1º ed. Rio de Janeiro: Forense, 2021.
BRASIL, Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil.

A congruência entre o disposto nas normas da família ISO/IEC 27000 com a LGPD pode ser observada no próprio *caput* do artigo 46, que dispõe a obrigatoriedade, para os agentes de tratamento, de disporem de medidas técnicas e administrativas capazes de proteger os dados pessoais de ameaças humanas e naturais[192].

Nesse sentido, para que estejam adequados à LGPD, não basta que os agentes de tratamento realizem algumas operações isoladas e pontuais de implementação de recursos tecnológicos ou elaboração de documentação interna. Pelo contrário, este enquadramento pressupõe o estabelecimento de um modelo de governança da segurança da informação que considere todos os riscos operacionais e implemente os controles adequados para gerenciá-los ou eliminá-los, sob o risco de o agente de tratamento incorrer em pesadas multas ou em condenações na esfera civil.

Inclusive, o §1º dispõe que a ANPD poderá dispor sobre os padrões técnicos mínimos a serem observados para o fornecimento de um nível adequado de proteção de dados pessoais. Imperioso citar a disposição já presente no Decreto nº 8.771/16, que poderá servir para balizar a adoção de padrões de segurança no tratamento de dados

[192] A obrigatoriedade imposta pelo legislador provém da utilização do vocábulo "devem", no *caput* do artigo 46. Como observam Márcio Cots e Ricardo Oliveira, "inicialmente, vale notar que o verbo 'devem' é impositivo da lei, ou seja, não se trata de faculdade: é uma obrigação legal que, se não cumprida poderá ensejar a aplicação de sanções administrativas e responsabilidade civil". In: COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais** - Comentada. São Paulo: Ed. Thomson Reuters Brasil, 2018. p. 238.

pessoais no âmbito digital, enquanto não houver regulamentação da ANPD nesse sentido[193].

2. Privacy by design

O §2º do artigo 46 dispõe que a privacidade e a proteção de dados deverão ser observadas desde a concepção de cada produto ou serviço, no âmbito dos agentes de tratamento, prática que se convencionou chamar de *privacy by design* e que se relaciona de forma direta com o princípio da prevenção.

A título de curiosidade, esta expressão foi cunhada por Ann Cavoukin, nos anos 90, e aborda a proteção da privacidade como

[193] BRASIL. **Decreto nº 8.771, de 11 de maio de 2016.** Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Art. 13: Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança: I - o estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários; II - a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros; III - a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014 ; e IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.

premissa na criação e no desenvolvimento de estruturas tecnológicas, modelos de negócio ou infraestruturas físicas[194].

Segundo a criadora da expressão, para a adoção do *privacy by design* em uma determinada organização, devem ser observados sete princípios, os quais dispõem que:

(i) deve ser almejada a proatividade nas questões que envolvem a privacidade;

(ii) a privacidade deve se dar como configuração-padrão em quaisquer produtos ou serviços;

(iii) a privacidade deve estar incorporada ao design desde a concepção de quaisquer produtos ou serviços;

(iv) os interesses do titular de dados pessoais devem ser necessariamente levados em consideração;

(v) deve haver segurança de ponta a ponta, abrangendo todo o ciclo de vida do produto ou serviço;

(vi) deve haver a preservação da visibilidade e da transparência ao titular;

(vii) deve haver o respeito à privacidade do titular.

[194] CAVOUKIAN, Ann. **Privacy by Design**: The 7 Foundational Principles - Implementation and Mapping of Fair Information Practices. Disponível em: . Acesso em: 21.12.2020.

Na prática, estes princípios visam alcançar uma mudança de mentalidade no âmbito dos agentes de tratamento, os quais deverão analisar, além das questões tributárias, trabalhistas, financeiras e operacionais, aquelas questões atinentes à proteção da privacidade dos titulares de dados pessoais.

Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

O dispositivo do artigo 47 da Lei prevê que a segurança da informação deve ser garantida por todos os agentes envolvidos no tratamento de dados, mesmo após o seu término, ou seja, os dados pessoais deverão ser protegidos em todo o seu ciclo de vida, sob pena de incorrerem em multas ou indenizações, conforme já mencionado.

É importante ressaltar o uso do verbo "obrigar" na redação do artigo, não havendo que se falar em garantia se não forem observados os controles e medidas de segurança discriminadas no caput do artigo 46 desta Lei.

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso de a comunicação não ter sido imediata; e

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

§ 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:

I - ampla divulgação do fato em meios de comunicação; e

II - medidas para reverter ou mitigar os efeitos do incidente.

§ 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

1. Comunicação em caso de incidente de segurança da informação

Em atenção ao princípio da transparência, positivado no art. 6º, inciso VI da Lei, e tendo em vista que não existe método de segurança à prova de falhas, o agente de tratamento deverá comunicar à ANPD e aos titulares afetados, qualquer incidente de segurança que possa acarretar risco ou dano relevante ao titular.

Essa comunicação pelo agente de tratamento deverá ser realizada o quanto antes, devendo conter todos os aspectos destacados no §1º do artigo 48, a fim de que a ANPD possa apurar a gravidade do vazamento para a aplicação de possíveis sanções, bem como avaliar os parâmetros de boa-fé do agente de tratamento, a adoção de políticas de boas práticas e governança e a pronta adoção de medidas corretivas, dentre outros critérios de mitigação da responsabilização previstos no art. 52, §1º da Lei.

2. Gravidade do incidente de segurança

Segundo o §2º, a ANPD realizará um juízo de ponderação acerca do incidente de segurança, podendo, aos seus próprios critérios, impor ao controlador que dê ampla divulgação ao incidente nos meios de comunicação, e que também tome todas as medidas necessárias para reverter ou mitigar as suas consequências.

Nessa mesma análise da gravidade do incidente, a ANPD verificará, nos termos do §3º, o grau de confidencialidade das informações vazadas, ou seja, se teriam sido aplicados métodos de criptografia, anonimização ou pseudonimização das informações, por exemplo, para que estas não pudessem ser legíveis a terceiros não autorizados.

O Decreto nº 8.771/16, em seu art. 13, inciso IV, coloca uma disposição semelhante, consignando que os provedores de conexão ou de aplicação devem, na guarda, armazenamento e tratamento de dados pessoais e de comunicações privadas, observar determinadas técnicas que garantam a inviolabilidade dos dados, dentre as quais a mencionada criptografia[195].

[195] BRASIL. **Decreto nº 8.771, de 11 de maio de 2016.** Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Art. 13: Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança: [...] IV - o uso de soluções de gestão dos

Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Para considerar-se que determinado agente de tratamento possua um nível adequado de proteção de dados pessoais, deve-se observar como todos os seus sistemas estão estruturados e interligados, e também como estes sistemas efetivamente protegem os atributos dos dados pessoais mantidos por aquela determinada organização, como é o caso, por exemplo, dos dados pessoais sensíveis, que devem estar devidamente segregados dos demais dados pessoais, por demandarem uma proteção maior.

registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.

Seção II - Das Boas Práticas e da Governança

Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e

a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

I - implementar programa de governança em privacidade que, no mínimo:

a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

g) conte com planos de resposta a incidentes e remediação; e

h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.

§ 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

1. Governança de proteção de dados pessoais

O art. 50 trata de um claro estímulo para que os agentes de tratamento criem regulações próprias para a proteção de dados pessoais. Neste sentido, em seu *caput* o art. 50 lista uma série de exemplos de atividades internas que poderiam ser concretizados pelos agentes de tratamento na busca pelo enquadramento com a LGPD, enquanto o §2º lista uma série de objetivos a serem almejados minimamente na criação

de um programa de governança da privacidade e dos dados pessoais dos titulares.

Este programa de governança, que visa o *compliance* com a LGPD, deverá ser elaborado de forma sistemática, envolvendo todas as áreas da instituição, e deverá ser implementado de forma contínua, com averiguações periódicas de sua real eficácia. Para que isto seja possível, é recomendável que a organização desenvolva, no mínimo, políticas internas de segurança da informação e de privacidade, além de realizar treinamentos e campanhas recorrentes para que todos os funcionários conheçam as políticas da instituição.

A seguir, são abordados alguns passos-chave para a criação de um programa efetivo de *compliance*, nos termos do que indica este art. 50.

2. Mapeamento de processos e dados

Apesar de não ser mencionado na série de atividades internas, antes de qualquer outra tratativa de adequação com LGPD, o agente de tratamento deverá se preocupar com a realização de um extensivo mapeamento de processos e de dados no âmbito interno da sua organização, a fim de identificar todos os riscos à proteção dos dados pessoais dos titulares e, desta forma, ser capaz de elaborar um plano para aplicar as medidas necessárias.

Este mapeamento pode ser realizado através de entrevistas com os funcionários das mais diversas áreas da empresa, embora também possa ser necessária a realização de auditorias para a confirmação das informações obtidas através destas entrevistas, para que sejam, eventualmente, complementadas com informações faltantes.

De forma resumida, o mapeamento de processos e de dados possuem os seguintes objetivos:

- Identificação dos processos de operação e de suporte da instituição;
- Averiguação de todas as características dos dados pessoais tratados pela organização;
- Apuração das finalidades de tratamento destes dados;
- Verificação das formas de coleta e de eliminação destes dados;
- Identificação dos setores envolvidos no tratamento destes dados;
- Constatação de quaisquer transferências de dados pessoais a terceiros, sejam elas a agentes de tratamento localizados no Brasil ou no exterior;
- Confirmação de quaisquer medidas de segurança já tomadas pela organização.

3. *Risk Assessment*

A partir do mapeamento acima referido, é possível a verificação de todos os riscos à proteção de dados pessoais, que podem dar ensejo a incidentes de segurança da informação. Neste sentido, o *risk assessment* envolve a utilização de uma matriz de riscos para mensurar os pontos principais a serem corrigidos através do projeto de adequação com a LGPD, permitindo assim que seja elaborado um cronograma de implementação do referido projeto.

A título de complementariedade, o Considerando 75 do RGPD lista algumas ameaças comuns que podem se materializar em riscos para a organização, dentre as quais se destacam:

(i) potencial de discriminação;

(ii) roubo de identidade, fraude ou perda financeira;

(iii) danos à reputação;

(iv) perda de confidencialidade de dados protegidos por sigilo profissional;

(v) reversão de processo de anonimização;

(vi) prejuízo econômico ou social;

(vii) privação dos direitos e liberdades do titular;

(viii) envolvimento de dados pessoais sensíveis ou de crianças e adolescentes[196].

4. Medidas de adequação

Primeiramente, insta ressaltar que qualquer programa de governança corporativa que almeje ser efetivo, seja na seara da proteção de dados, seja em outra área, deve ser liderado pela alta direção da empresa, sendo este o significado da expressão "*tone from the top*" (tom da alta direção, em tradução livre).

[196] UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).** Considerando 75. O risco para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, poderá resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, em especial quando o tratamento possa dar origem à discriminação, à usurpação ou roubo da identidade, a perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, à inversão não autorizada da pseudonimização, ou a quaisquer outros prejuízos importantes de natureza económica ou social; quando os titulares dos dados possam ficar privados dos seus direitos e liberdades ou impedidos do exercício do controlo sobre os respetivos dados pessoais; quando forem tratados dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical, bem como dados genéticos ou dados relativos à saúde ou à vida sexual ou a condenações penais e infrações ou medidas de segurança conexas; quando forem avaliados aspetos de natureza pessoal, em particular análises ou previsões de aspetos que digam respeito ao desempenho no trabalho, à situação económica, à saúde, às preferências ou interesses pessoais, à fiabilidade ou comportamento e à localização ou às deslocações das pessoas, a fim de definir ou fazer uso de perfis; quando forem tratados dados relativos a pessoas singulares vulneráveis, em particular crianças; ou quando o tratamento incidir sobre uma grande quantidade de dados pessoais e afetar um grande número de titulares de dados. Disponível em: < https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>. Acesso em 28/01/2021.

Logo, deve haver um compromisso genuíno dos indivíduos da alta direção com a proteção de dados pessoais, a fim de conferir credibilidade ao programa de governança e influenciar, de forma positiva, os demais funcionários da organização.

No que diz respeito às medidas de adequação determinadas após a realização do *risk assessment*, tem-se que elas geralmente envolvem a criação de diversos documentos internos no âmbito da organização, como forma de demonstrar o *compliance* com as determinações legais sobre a proteção de dados pessoais. Estes documentos podem envolver desde regulamentos gerais até procedimentos mais específicos para a execução de determinadas atividades, como *backups*, por exemplo.

É mais comum, entretanto, que sejam elaboradas políticas, que podem ser definidas como normas internas que estabelecem o posicionamento da instituição acerca de determinados temas. Estas políticas geralmente envolvem penalidades para a não observação das disposições nelas contidas.

A título de exemplificação, a seguir são elencadas algumas políticas, expondo suas finalidades dentro das organizações:

- Política de Segurança da Informação: contempla tudo o que diz respeito à segurança da informação, sobretudo as medidas técnicas e organizacionais necessárias para a

proteção da integridade, disponibilidade e confidencialidade da informação;

- Política de privacidade e proteção de dados pessoais: demonstra as circunstâncias e as finalidades de tratamento dos dados pessoais dos titulares pela instituição, em conformidade com os princípios da transparência e da prestação de contas da LGPD;

- Política de *backu*p: contempla a forma e a periodicidade de realização dos procedimentos de *backup* pelo agente de tratamento, com o fim de garantir que as informações estejam sempre disponíveis;

- Política de criptografia: inclui a forma e as condições de aplicação dos procedimentos de criptografia definidos pela organização, com o fim de proteger a integridade e a confidencialidade das informações;

- Política de senhas: aborda a utilização de senhas dentro dos sistemas da instituição, com o fim de proteger o acesso das informações a indivíduos não autorizados;

- Política de retenção de dados pessoais: contempla as formas de retenção e eliminação de dados pessoais pela instituição, em respeito aos princípios da necessidade e adequação e ao disposto nos artigos 15 e 16 da Lei;

- Política de antivírus e *firewall*: contempla procedimentos de instalação, atualização e utilização de softwares de antivírus e *firewall* nos equipamentos informáticos do agente de tratamento, que têm o fito de proteger as informações de acessos não autorizados;

- Política de *LOGs*: aborda as formas e condições com que são feitos os registros nos sistemas da organização, em consonância com o que dita o art. 37 da Lei.

Ainda, durante a implementação do programa de governança, devem ser adequados todos os contratos vigentes no âmbito da organização, tanto com clientes quanto com fornecedores e colaboradores, a fim de mitigar quaisquer riscos jurídicos relativos a incidentes de proteção de dados.

Por fim, é importante também o desenvolvimento de canais seguros e efetivos de comunicação com os titulares de dados para a solicitação de informações e para a realização de requerimentos, adotando-se uma linguagem clara e que contemple todas as informações sobre o tratamento exigidas pela LGPD, mais especificamente aquelas contidas no art. 9º da Lei, a saber:

(i) a finalidade, a forma e a duração específica do tratamento;

(ii) a identificação e informações de contato do controlador;

(iii) as informações sobre o compartilhamento dos dados;

(iv) os direitos do titular e as responsabilidades dos agentes de tratamento.

5. Nomeação de um encarregado de dados

O programa de *compliance* também deverá envolver a nomeação de um encarregado pelo tratamento de dados pessoais, que deverá ser realizado nos termos do artigo 41 da Lei, e deverá possuir autonomia financeira e hierárquica para realizar as suas atividades.

Não é recomendável que o encarregado de dados tenha outras responsabilidades na instituição, não ligadas à proteção de dados pessoais, tendo em vista a possibilidade da existência de conflitos de interesses com outras áreas, como aquela responsável pelo *compliance*, por exemplo, conforme já vem sendo o entendimento de algumas autoridades de dados europeias[197].

[197] Neste sentido, em uma decisão recente da autoridade da Bélgica, uma empresa foi multada em 10 mil euros, por nomear como DPO o responsável pela área de compliance e conformidade. In. CHAVES, Luís Fernando Prado. Bélgica: Empresa é multada por ter nomeado head de compliance, auditoria e riscos como DPO. **UOL**, 2020.Disponível em: <https://migalhas.uol.com.br/depeso/328258/belgica--empresa-e-multada-por-ter-nomeado-head-de-compliance--auditoria-e-riscos-como-dpo>. Acesso em 20/01/2021.

6. Treinamento

Após completadas as fases de mapeamento de processos e de dados, mensuração dos riscos e adequação dos procedimentos internos, a organização terá em mãos uma série de documentos que refletirá, em grande parte, as suas atividades de tratamento de dados pessoais. Todo esse conteúdo, para se tornar efetivo, deve ser transmitido e trabalhado com todos os funcionários da instituição, além de eventuais funcionários terceirizados.

7. Implementação contínua

Por último, deve-se realizar uma revisão periódica do programa de governança implantado na empresa. Esta revisão envolve, sobretudo, o estabelecimento de um sistema de registro de incidentes de segurança da informação que permita o melhoramento contínuo dos procedimentos internos da organização, no que diz respeito à proteção de dados pessoais. Tal sistema também pode ser utilizado para a melhoria do canal dos titulares e para a eventual elaboração de relatórios de impacto à proteção de dados pessoais.

Deste modo, pode-se dizer que o programa de adequação à LGPD trata de um processo contínuo, que deve ser enxergado pelo agente de tratamento como um investimento capaz de influenciar na transformação digital na empresa e trazer vantagens comparativas substanciais sobre a concorrência.

Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.

O art. 51 da Lei possui natureza de complementariedade com o art. 50, dispondo que a ANPD deverá estimular a adoção de padrões técnicos que facilitem o direito de autodeterminação informativa dos titulares.

CAPÍTULO VIII - DA FISCALIZAÇÃO

Seção I - Das Sanções Administrativas

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração;

VII - (VETADO);

VIII - (VETADO);

IX - (VETADO).

X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;

XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

§ 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:

I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;

II - a boa-fé do infrator;

III - a vantagem auferida ou pretendida pelo infrator;

IV - a condição econômica do infrator;

V - a reincidência;

VI - o grau do dano;

VII - a cooperação do infrator;

VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;

IX - a adoção de política de boas práticas e governança;

X - a pronta adoção de medidas corretivas; e

XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990, e em legislação específica.

§ 3º O disposto nos incisos I, IV, V, VI, X, XI e XII do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junho de 1992, e na Lei nº 12.527, de 18 de novembro de 2011.

§ 4º No cálculo do valor da multa de que trata o inciso II do caput deste artigo, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea.

§ 5º O produto da arrecadação das multas aplicadas pela ANPD, inscritas ou não em dívida ativa, será destinado ao Fundo de Defesa de Direitos Difusos de que tratam o art. 13 da Lei nº 7.347, de 24 de julho de 1985, e a Lei nº 9.008, de 21 de março de 1995. (Incluído pela Lei nº 13.853, de 2019)

§ 6º As sanções previstas nos incisos X, XI e XII do caput deste artigo serão aplicadas: (Incluído pela Lei nº 13.853, de 2019)

I - somente após já ter sido imposta ao menos 1 (uma) das sanções de que tratam os incisos II, III, IV, V e VI do caput

deste artigo para o mesmo caso concreto; e (Incluído pela Lei nº 13.853, de 2019)

II - em caso de controladores submetidos a outros órgãos e entidades com competências sancionatórias, ouvidos esses órgãos. (Incluído pela Lei nº 13.853, de 2019)

§ 7º Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo. (Incluído pela Lei nº 13.853, de 2019)

Para melhor compreensão, o art. 52 será comentado em conjunto com o art. 53.

Art. 53. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa.

§ 1º As metodologias a que se refere o caput deste artigo devem ser previamente publicadas, para ciência dos agentes de tratamento, e devem apresentar objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa, que deverão conter fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos nesta Lei.

§ 2º O regulamento de sanções e metodologias correspondentes deve estabelecer as circunstâncias e as condições para a adoção de multa simples ou diária.

1. *Enforcement* da LGPD

Primeiramente, conforme visto no Capítulo anterior, cumpre frisar que a LGPD busca acompanhar uma tendência legislativa internacional de corregulação e *accountability*[198]. Entretanto, a Lei não

[198] O Working Party do Article 29 definiu que "o termo 'accountability' deriva do mundo anglo-saxão, onde tem uso comum e há uma compreensão amplamente compartilhada sobre o seu significado – muito embora seja complexo definir o que, exatamente, 'accountability' significa na prática. Em termos gerais, entretanto, a ênfase está em demonstrar como a responsabilidade é exercida e em tornar tal fato demonstrável. Responsabilidade e 'accountability' são dois lados da mesma moeda e

deixa de prever as medidas tradicionais para o seu *enforcement* (cumprimento, em tradução livre) efetivo, tais como as sanções admoestativas, pecuniárias e restritivas de direitos, além da introdução de uma "sanção reputacional" no ordenamento, com o condão de danificar a imagem do agente de tratamento infrator perante a sociedade.

Outra condição necessária para o *enforcement* efetivo da LGPD perpassa pela criação de mecanismos de cooperação internacional para a proteção de dados pessoais, a fim de serem estabelecidos padrões comuns de interoperabilidade entre diferentes ordenamentos jurídicos. Tais padrões certamente impediriam a interrupção do fluxo de bens e serviços entre países como, por exemplo, os bloqueios judiciais determinados ao aplicativo de mensagens *Whatsapp* nos anos de 2015 e 2016, por ausência de cooperação[199].

---

ambos constituem elementos essenciais de boa governança. Somente quando se pode demonstrar na prática o exercício da responsabilidade é que a confiança pode se desenvolver. Na maior parte dos outros idiomas europeus, devido principalmente a diferenças em sistemas jurídicos, o termo 'accountability' não é facilmente traduzido. Como consequência, o risco de interpretações divergentes do termo e, consequentemente, de falta de harmonização, é substantivo. Outras expressões que têm sido sugeridas para capturar o significado de 'accountability' são 'reinforced responsibility', 'assurance', 'reliability', 'trustworthiness' e, em francês, 'obligation de rendre comptes' etc. Pode-se também sugerir que 'accountability' se refere à 'implementação de princípios de proteção de dados". Apud. WIMMER, Miriam. Os desafios do enforcement na LGPD: fiscalização, aplicação de sanções administrativas e coordenação intergovernamental. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz (orgs). **Tratado de Proteção de Dados Pessoais**. 1º ed. Rio de Janeiro: Forense, 2021. pp. 377-379.

[199] Ibidem. p. 380.

2. Sanções Administrativas

As competências de aplicação das sanções pela ANPD são definidas pelo inciso IV do art. 55-J da Lei, e também pelos §§7º e 8º do art. 2º do Anexo I do Decreto nº 10.474/20[200], enquanto as sanções em si estão elencadas nos incisos do artigo 52 da LGPD. Estas sanções possuem uma natureza jurídica primordialmente repressiva [201], implicando, pois, em uma manifestação do poder de polícia do Estado, que visa coibir a prática de atividades que possam resultar em um ilícito administrativo[202].

O *caput* do artigo 52 não determina o escopo da infração que poderá dar ensejo a aplicação de determinada sanção, bastando, em tese, a ocorrência de qualquer infração à Lei para seja aberto um procedimento administrativo de apuração pela autoridade nacional, respeitados os princípios do contraditório e da ampla defesa, bem como demais ressalvas previstas no §1º do artigo 52.

---

[200] BRASIL. **Decreto nº 10.474, de 26 de agosto de 2020.** Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança. Art. 2º: Compete à ANPD: [...] § 7º A aplicação das sanções previstas na Lei nº 13.709, de 2018, compete exclusivamente à ANPD e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública. § 8º A ANPD articulará sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais e será o órgão central de interpretação da Lei nº 13.709, de 2018, e do estabelecimento de normas e diretrizes para a sua implementação.

[201] MELLO, Rafael Munhoz de. **Princípios constitucionais de direito administrativo sancionador**: As sanções administrativas à luz da Constituição Federal de 1988. São Paulo: Malheiros, 2007. p. 134.

[202] OSÓRIO, Fábio Medina. **Direito Administrativo Sancionador**. São Paulo: Revista dos Tribunais, 2010. p. 87.

Ademais, em decorrência do princípio do *ne bis in idem*, a ANPD não poderá aplicar mais de uma sanção administrativa pelo mesmo fato concreto [203]. Todavia, nada impede que a autoridade nacional realize uma fiscalização posterior para averiguar se o agente de tratamento continua a infringir a Lei, ocasião em que poderá aplicar outra sanção com base na reincidência, que constitui, inclusive, um dos parâmetros de aplicação das sanções administrativas, previsto no §1º, inciso V do art. 52.

Insta salientar que a ocorrência de um incidente de segurança não impedirá a aplicação das disposições contidas no CDC, em normas de setores econômicos específicos ou mesmo das normas atinentes à esfera penal ou à esfera cível, conforme dispõe o §2º do artigo 52.

3. Composição prévia

O §7º do artigo 52 prevê que, nos casos de "vazamentos individuais ou os acessos não-autorizados de que trata o art. 46", há a possibilidade de realização de uma conciliação entre o titular e o controlador, previamente ao procedimento sancionatório pela ANPD.

[203] A expressão em latim *bis in idem* significa "duas vezes o mesmo". A ideia do termo indica a repetição de algo ou de alguma atividade. A expressão *ne bis in idem*, por sua vez, "em sua própria acepção semântica já impõe de imediato que se esclareça o que (idem) não deve ser repetido (ne bis). Nessa linha provisoriamente pode-se antecipar que sua utilização jurídica, por via de regra, é associada à proibição de que um Estado imponha a um indivíduo uma dupla sanção ou um duplo processo (ne bis) em razão de uma mesma conduta (idem)". In. FONSECA, Carlos Rodolfo. **O princípio do *ne bis in idem* e a Constituição Brasileira de 1988**. Boletim Jurídico. Direito, Estado e Sociedade, 2018. p. 27.

A intenção do legislador parece ser, através deste dispositivo legal, permitir uma espécie de acordo direto entre o titular de dados e o controlador, afastando a incidência das penalidades previstas no artigo 52. Entretanto, ainda que exista esta possibilidade de composição, a ANPD deverá investigar aqueles incidentes de grandes proporções, como nos casos de vazamento de bases de dados inteiras, hipóteses estas em que deverá lançar mão do seu poder de polícia contra os agentes de tratamento infratores.

4. Dosimetria das sanções

Ao aplicar as sanções, a ANPD deverá observar os parâmetros contidos no §1º do artigo 52, a fim de agravar ou atenuar a severidade da sanção, conforme disposto na Lei de Introdução às Normas do Direito Brasileiro[204]. Estes parâmetros envolvem:

(i) a gravidade e a natureza das infrações e dos direitos pessoais afetados;

(ii) a boa-fé do infrator;

[204] BRASIL. **Decreto-lei nº 4.657, de 4 de setembro de 1942**. Lei de Introdução às normas do Direito Brasileiro. Art. 22: Na interpretação de normas sobre gestão pública, serão considerados os obstáculos e as dificuldades reais do gestor e as exigências das políticas públicas a seu cargo, sem prejuízo dos direitos dos administrados.
§ 2º Na aplicação de sanções, serão consideradas a natureza e a gravidade da infração cometida, os danos que dela provierem para a administração pública, as circunstâncias agravantes ou atenuantes e os antecedentes do agente.

(iii) a vantagem auferida ou pretendida pelo infrator;

(iv) a condição econômica do infrator;

(v) a reincidência da conduta;

(vi) o grau do dano;

(vii) a cooperação do infrator;

(viii) a adoção de mecanismos e procedimentos internos capazes de minimizar o dano;

(ix) a adoção de política de boas práticas e governança;

(x) a pronta adoção de medidas corretivas; e

(xi) a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

No entanto, até que haja alguma cominação de sanção ou regulamentação pela ANPD, não é possível indicar exatamente como será feita esta dosimetria das sanções administrativas.

Ademais, a Administração Pública deverá se pautar pelos princípios da proporcionalidade e da razoabilidade na aplicação das sanções, sempre atenta às circunstâncias do caso concreto e aos impactos sociais e econômicos que podem ser resultantes da sanção uma vez aplicada. Estes procedimentos de fiscalização em si deverão

ser mais bem detalhados através de regulamento próprio da ANPD, seguindo as diretrizes constantes do artigo 53.

Por fim, a ANPD poderá se inspirar na Agência Europeia para Segurança de Redes e da Informação (ENISA), que possui uma metodologia própria para a avaliação da severidade de incidentes de segurança, levando em consideração três critérios principais, cada um com um coeficiente distinto[205]: o contexto em que os dados eram tratados (DPC), a facilidade com que os dados são identificados (EI) e o aspecto circunstancial do incidente (CB). O grau de severidade do incidente, portanto, poderia ser definido como baixo, médio, alto e muito alto, a depender do resultado da fórmula: SE = DPC x EI + CB.

5. Advertência

Partindo para as sanções em espécie, tem-se que o inciso I do artigo 52 prevê a sanção de advertência, que nada mais é do que uma admoestação escrita dirigida ao agente de tratamento após a ocorrência de uma infração à LGPD, com caráter puramente pedagógico.

Nesta advertência deve ser estabelecido um prazo para que o agente de tratamento adote as medidas necessárias para a correção da referida infração. Decorrido este prazo, a autoridade nacional poderá

[205] O processo de avaliação realizado pela agência é complexo, e cada um dos critérios possui níveis de pontuações predefinidas. cf. EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY. Recommendations for a methodology of the assessment of severity of personal data breaches. **Working Document**, v. 1, Dec. 2013. Disponível em: <https://www.enisa.europa.eu/publications/dbn-severity>. Acesso em 21/12/2020.

realizar outra fiscalização, a qual poderá importar na aplicação de uma outra sanção mais grave, no caso em que o agente de tratamento continuar infringindo os ditames da LGPD.

6. Multas

Já os incisos II e III preveem duas formas de aplicação de sanções pecuniárias: uma delas se refere ao valor total da sanção, enquanto a outra se refere a um valor diário a ser pago pelo agente de tratamento. Os valores destas multas, por infração à Lei, serão limitados a 2% do faturamento da pessoa jurídica no último exercício financeiro, excluídos os tributos, não podendo ultrapassar o valor máximo de R$50.000.000,00 (cinquenta milhões de reais).

É interessante notar o comportamento silente do legislador, não mencionando a multa simples e diária, dispostas nos incisos II e III deste artigo, às pessoas físicas. Todavia, vale ressaltar que, por não haver qualquer menção nos demais incisos, todas as demais sanções poderão lhes ser aplicadas.

Embora sejam valores altos, espera-se que a ANPD limite o aspecto de confisco das multas aplicadas, para que elas não se tornem excessivamente onerosas aos agentes de tratamento, o que certamente poderia causar impactos sociais e econômicos piores dos que os causados pela infração que se estaria tentando reprimir.

Por fim, segundo o §5º do artigo 52, os valores arrecadados com estas sanções pecuniárias deverão ser destinados ao Fundo de Defesa dos Direitos Difusos, criado pela Lei nº 9.008/95, ou seja, certamente serão utilizados para o fortalecimento de iniciativas e políticas públicas de proteção de dados pessoais dos cidadãos.

7. Publicização da infração

O inciso IV do artigo 52 prevê uma espécie de sanção "reputacional", como já mencionado, dizendo respeito à publicização da ocorrência da infração pelo próprio agente de tratamento, após devidamente apurada e confirmada a sua existência.

8. Bloqueio e eliminação

Os incisos V e VI do art. 52 tratam de sanções restritivas de direito dos agentes de tratamento, dizendo respeito ao bloqueio e a eliminação dos dados pessoais, conforme conceituado no art. 5º, incisos XIII e XIV da própria LGPD. Em suma, enquanto no bloqueio os dados pessoais ficam temporariamente indisponíveis ao agente de tratamento, na eliminação os dados pessoais devem ser excluídos.

9. Suspensão e proibição

Os incisos X (suspensão parcial do funcionamento do banco de dados), XI (suspensão do tratamento de dados pessoais) e XII (proibição parcial ou total das atividades relacionadas a tratamento de dados), também constituem sanções restritivas de direitos dos agentes de tratamento.

Diferentemente daquelas sanções de bloqueio e suspensão, estas sanções previstas nos incisos X, XI e XII do art. 52 têm o condão de impactar de maneira mais profunda as atividades dos agentes de tratamento, pois impediriam a própria atividade de tratamento de dados pelo agente infrator.

Desta forma, a sua aplicação deve ser limitada apenas às hipóteses previstas no §6º do art. 52, ou seja, quando já tiver sido imposta alguma das outras sanções que não a de advertência, ou caso o agente de tratamento integre um setor regulado da economia, ocasiões em que as agências reguladoras deverão ser ouvidas em momento anterior à tomada de decisão pela ANPD.

10. Sanções à Administração Pública

As pessoas jurídicas de direito público, nos termos do §3º do art. 52, também estarão submetidas às sanções previstas no Capítulo VIII da Lei. Entretanto, quando o legislador utiliza o verbo “poder” na disposição do referido parágrafo, acaba por abrir espaço para uma

interpretação de que seriam incluídas também as sanções pecuniárias aos órgãos públicos, sendo este, portanto, mais um erro de redação legislativa que tem causado algumas divergências doutrinárias.

Fabrício da Mota Alves[206] entende que a interpretação do referido parágrafo possibilita esta forma de sanção ao dispor que ela:

> reside no fato de que o verbo 'poderá' não se associa a nenhum advérbio que lhe pudesse delimitar o sentido, como, por exemplo, 'somente ou 'exclusivamente'. Por certo que, juridicamente, 'poderá' não possui suficiente semântica de restrição de disposição legal, pelo contrário, expande para compreender permissividade, adição, complementação. (...) Daí ser possível entender-se viável a aplicação de penalidade de multa contra entes públicos, se o escopo maior for o de ampliar a proteção de dados pessoais na sociedade.

Entretanto, Márcio Cots e Ricardo Oliveira[207] entendem de maneira contrária, alegando que:

> por princípio lógico, algumas sanções administrativas não poderão ser aplicadas à administração pública, quais sejam, multa simples, multa diária e publicização. Isso porque, nos dois primeiros casos, a atividade dos referidos órgãos não se dedica ao lucro, sendo que a imposição de penalidade pecuniária somente oneraria o orçamento público, precarizando ainda mais os serviços prestados (...).

Observando-se que houve uma omissão expressa do legislador em incluir as sanções de multa e de multa diária na redação do §3º, entende-se que a segunda posição seria mais adequada em um primeiro momento, a fim de se evitar um excesso de litigiosidade na aplicação

---

[206] ALVES. Fabrício da Mota Alves. Capítulo VIII – Da Fiscalização. In. MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). **LGPD** – Lei Geral de Proteção de Dados – Comentada. 2ª ed. São Paulo: Revista dos Tribunais, 2019. p. 390.

[207] COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais** – Comentada. 3º ed. São Paulo, Revista dos Tribunais, 2019. p. 215.

da LGPD, a qual já possui inúmeras falhas legislativas que deverão ser sanadas através de uma construção jurisprudencial. Portanto, as sanções de multa e de multa diária não poderiam ser incluídas no rol de sanções administrativas possíveis aos órgãos do Poder Público.

Cumpre frisar também que, embora alguns autores defendam não ser a sanção de publicização aplicável ao Poder Público, esta sanção é perfeitamente cabível e até recomendável, por seu aspecto pedagógico e em acordo com o princípio da transparência elencado no inciso VI do art. 6º da Lei.

Já nos casos das sanções previstas nos incisos X, XI e XII, a aplicação deverá ser ainda mais ponderada pela ANPD, tendo em vista que a interrupção de tratamento por órgãos do Poder Público poderá impactar diretamente na prestação de serviços públicos à população. Logo, deve-se entender que apenas naquelas circunstâncias extremas, em que a própria Administração Pública estivesse agindo em flagrante descumprimento aos dispositivos da LGPD, seria razoável que a ANPD agisse para suspender ou proibir as operações de tratamento consideradas ilegais.

Art. 54. O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional.

Parágrafo único. A intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento.

O artigo 54 também dispõe sobre a aplicação da multa, assim como o fazem alguns dos dispositivos imediatamente anteriores, havendo aqui uma clara fragmentação normativa relativa à matéria.

Passadas estas considerações, o referido dispositivo legal busca deixar expresso que a ANPD deverá observar o princípio da proporcionalidade na aplicação de quaisquer sanções pecuniárias. Também dispõe que o documento de intimação da multa diária deverá conter, ao menos, a descrição da obrigação, que poderá ser de fazer ou de não-fazer, o prazo razoável estipulado para o seu cumprimento e o valor diário da multa no caso de descumprimento da ordem.

CAPÍTULO IX - DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE

Seção I - Da Autoridade Nacional de Proteção de Dados (ANPD)

Art. 55. (VETADO).

Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República.

§ 1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República.

§ 2º A avaliação quanto à transformação de que dispõe o § 1º deste artigo deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD.

§ 3º O provimento dos cargos e das funções necessários à criação e à atuação da ANPD está condicionado à expressa

autorização física e financeira na lei orçamentária anual e à permissão na lei de diretrizes orçamentárias.

Art. 55-B. É assegurada autonomia técnica e decisória à ANPD. (Incluído pela Lei nº 13.853, de 2019)

1. Autoridade Nacional de Proteção de Dados

A criação da Autoridade Nacional de Proteção de Dados teve um processo legislativo conturbado, considerando que o art. 55, que originalmente criava a estrutura da autoridade nacional, foi completamente vetado pela Presidência da República quando da promulgação da Lei, sob a justificativa de que o Poder Legislativo teria invadido competência privativa do Poder Executivo, o que possivelmente geraria imensa insegurança jurídica sobre a existência da própria autoridade nacional.

Para corrigir este vício de iniciativa legislativa, foi editada, em 27 de dezembro de 2018, a MP nº 869/2018, posteriormente convertida na Lei nº 13.853/19, a qual, além de realizar alguns ajustes na Lei, criou a Autoridade Nacional de Proteção de Dados – ANPD.

2. Estrutura da ANPD

A princípio, tendo em vista o momento de grave crise fiscal do país e a necessidade de observação da EC nº 95/16, também conhecida como Emenda Constitucional do Teto dos Gastos Públicos, a ANPD foi

criada nos moldes da redação do art. 55-A da Lei, não oferecendo aumento nas despesas.

Ainda que esta medida possa ser vista como benéfica às finanças públicas, tem-se também que ela pode se mostrar insuficiente frente o escopo de trabalho necessário para uma fiscalização efetiva da Lei, a qual deverá requerer um investimento substancial em pessoal e tecnologia.

O §1º do art. 55-A também afirma a natureza transitória da ANPD, que se encontrará, de início, vinculada diretamente à Presidência da República, com autonomia administrativa reduzida. Já pelo §2º do artigo 55-A, a avaliação de transformação da ANPD em uma autarquia deverá ser realizada em até dois anos da data de vigência da sua estrutura regimental prevista no Anexo I do Decreto nº 10.474/20, ou seja, até a data de 27 de agosto de 2022.

Esta transformação da ANPD em autarquia submetida a regime especial certamente traria diversos benefícios, permitindo uma maior autonomia funcional, decisória, administrativa e financeira da autoridade, incluindo a autoridade sob a tutela da Lei nº 13.848/19 assim como as demais agências reguladoras setoriais[208]. Nas atuais

[208] BRASIL. **Lei nº 13.848, de 25 de junho de 2019**. Dispõe sobre a gestão, a organização, o processo decisório e o controle social das agências reguladoras, altera a Lei nº 9.427, de 26 de dezembro de 1996, a Lei nº 9.472, de 16 de julho de 1997, a Lei nº 9.478, de 6 de agosto de 1997, a Lei nº 9.782, de 26 de janeiro de 1999, a Lei nº 9.961, de 28 de janeiro de 2000, a Lei nº 9.984, de 17 de julho de 2000, a Lei nº 9.986, de 18 de julho de 2000, a Lei nº 10.233, de 5 de junho de 2001, a Medida Provisória nº 2.228-1, de 6 de setembro de 2001, a Lei nº 11.182, de 27 de setembro de 2005, e a Lei nº 10.180, de 6 de fevereiro de 2001. Art. 3º: A natureza especial

circunstâncias, segundo o art. 55-B, a ANPD deverá possuir apenas autonomia técnica e decisória.

A LGPD não prevê, contudo, o que acontecerá na hipótese de o Poder Executivo não transformar a ANPD em um órgão da administração indireta neste prazo de dois anos, havendo, portanto, a possibilidade de impetração de remédios constitucionais em caso de inércia, dentre os quais o mandato de injunção, que forcem o Executivo a cumprir esta disposição normativa, o que seria danoso à segurança jurídica do país.

conferida à agência reguladora é caracterizada pela ausência de tutela ou de subordinação hierárquica, pela autonomia funcional, decisória, administrativa e financeira e pela investidura a termo de seus dirigentes e estabilidade durante os mandatos, bem como pelas demais disposições constantes desta Lei ou de leis específicas voltadas à sua implementação.:

Art. 55-C. A ANPD é composta de:

I - Conselho Diretor, órgão máximo de direção;

II - Conselho Nacional de Proteção de Dados Pessoais e da Privacidade;

III – Corregedoria;

IV - Ouvidoria;

V - órgão de assessoramento jurídico próprio; e

VI - unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei.

Art. 55-D. O Conselho Diretor da ANPD será composto de 5 (cinco) diretores, incluído o Diretor-Presidente. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Os membros do Conselho Diretor da ANPD serão escolhidos pelo Presidente da República e por ele nomeados, após aprovação pelo Senado Federal, nos termos da alínea 'f' do inciso III do art. 52 da Constituição Federal, e ocuparão cargo em comissão do Grupo-Direção e Assessoramento Superiores - DAS, no mínimo, de nível 5. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Os membros do Conselho Diretor serão escolhidos dentre brasileiros que tenham reputação ilibada, nível

superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados. (Incluído pela Lei nº 13.853, de 2019)

§ 3º O mandato dos membros do Conselho Diretor será de 4 (quatro) anos. (Incluído pela Lei nº 13.853, de 2019)

§ 4º Os mandatos dos primeiros membros do Conselho Diretor nomeados serão de 2 (dois), de 3 (três), de 4 (quatro), de 5 (cinco) e de 6 (seis) anos, conforme estabelecido no ato de nomeação. (Incluído pela Lei nº 13.853, de 2019)

§ 5º Na hipótese de vacância do cargo no curso do mandato de membro do Conselho Diretor, o prazo remanescente será completado pelo sucessor. (Incluído pela Lei nº 13.853, de 2019)

1. Composição da ANPD

O art. 55-C define os órgãos que deverão, necessariamente, compor a estrutura da ANPD. O Anexo I do Decreto nº 10.474/20, que criou a estrutura regimental da ANPD, detalhou a estrutura e as competências de cada órgão da autoridade nacional, conforme abaixo disposto:

> Art. 3º A ANPD é constituída pelos seguintes órgãos: I - Conselho Diretor; II - órgão consultivo: Conselho Nacional de Proteção de Dados Pessoais e da

> privacidade; III - órgãos de assistência direta e imediata ao Conselho Diretor: a) Secretaria-Geral; b) Coordenação-Geral de Administração; e c) Coordenação-Geral de Relações Institucionais e Internacionais; IV - órgãos seccionais: a) Corregedoria; b) Ouvidoria; e c) Assessoria Jurídica; e V - órgãos específicos singulares: a) Coordenação-Geral de Normatização; b) Coordenação-Geral de Fiscalização; e c) Coordenação-Geral de Tecnologia e Pesquisa.

2. Conselho Diretor da ANPD

O Conselho Diretor da autoridade será composto de cinco membros, sendo um deles designado o Diretor-Presidente, que deverá realizar a gestão e a representação institucional da ANPD, e outros quatro diretores, escolhidos e nomeados pelo Presidente da República após aprovação pelo Senado Federal, o que ocorreu no dia 20 de outubro de 2020.

Os diretores deverão exercer os mandatos de forma escalonada, e deverão ser remunerados de acordo com o cargo comissionado do Grupo-Direção e Assessoramento Superiores – DAS de nível 5.

Art. 55-E. Os membros do Conselho Diretor somente perderão seus cargos em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar.

§ 1º Nos termos do caput deste artigo, cabe ao Ministro de Estado Chefe da Casa Civil da Presidência da República instaurar o processo administrativo disciplinar, que será conduzido por comissão especial constituída por servidores públicos federais estáveis.

§ 2º Compete ao Presidente da República determinar o afastamento preventivo, somente quando assim recomendado pela comissão especial de que trata o § 1º deste artigo, e proferir o julgamento.

O art. 55-E estabelece as competências e o procedimento para a aferição de ilícitos cometidos pelos membros do Conselho Diretor da ANPD. Embora a Constituição Federal disponha que os cargos em comissão não devam gozar de qualquer estabilidade funcional[209], por serem de livre nomeação e exoneração, os membros do Conselho

[209] BRASIL. **Constituição da República Federativa do Brasil**, 1988. Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte: [...] II - a investidura em cargo ou emprego público depende de aprovação prévia em concurso público de provas ou de provas e títulos, de acordo com a natureza e a complexidade do cargo ou emprego, na forma prevista em lei, ressalvadas as nomeações para cargo em comissão declarado em lei de livre nomeação e exoneração.

Diretor somente perderão os seus cargos em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar, tendo em vista a natureza especial da ANPD e o risco de interferências políticas indevidas no órgão[210].

[210] BRASIL. **Lei nº 8.112, de 11 de dezembro de 1990.** Dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais. Art. 22. O servidor estável só perderá o cargo em virtude de sentença judicial transitada em julgado ou de processo administrativo disciplinar no qual lhe seja assegurada ampla defesa.

Art. 55-F. Aplica-se aos membros do Conselho Diretor, após o exercício do cargo, o disposto no art. 6º da Lei nº 12.813, de 16 de maio de 2013.

Parágrafo único. A infração ao disposto no caput deste artigo caracteriza ato de improbidade administrativa.

O membro do Conselho Diretor, sob pena de incorrer em ato de improbidade administrativa, não poderá divulgar ou fazer uso de quaisquer informações privilegiadas ou confidenciais obtidas em razão da sua função na ANPD, e também sofrerá limitações em suas atividades profissionais pelo período de 06 meses após o afastamento do cargo, conforme o disposto no artigo 6º da Lei nº 12.813/13[211].

[211] BRASIL. **Lei nº 12.813, de 16 de maio de 2013**. Dispõe sobre o conflito de interesses no exercício de cargo ou emprego do Poder Executivo federal e impedimentos posteriores ao exercício do cargo ou emprego; e revoga dispositivos da Lei nº 9.986, de 18 de julho de 2000, e das Medidas Provisórias nº 2.216-37, de 31 de agosto de 2001, e 2.225-45, de 4 de setembro de 2001. Art. 6º Configura conflito de interesses após o exercício de cargo ou emprego no âmbito do Poder Executivo federal: I - a qualquer tempo, divulgar ou fazer uso de informação privilegiada obtida em razão das atividades exercidas; e II - no período de 6 (seis) meses, contado da data da dispensa, exoneração, destituição, demissão ou aposentadoria, salvo quando expressamente autorizado, conforme o caso, pela Comissão de Ética Pública ou pela Controladoria-Geral da União: a) prestar, direta ou indiretamente, qualquer tipo de serviço a pessoa física ou jurídica com quem tenha estabelecido relacionamento relevante em razão do exercício do cargo ou emprego; b) aceitar cargo de administrador ou conselheiro ou estabelecer vínculo profissional com pessoa física ou jurídica que desempenhe atividade relacionada à área de competência do cargo ou emprego ocupado; c) celebrar com órgãos ou entidades do Poder Executivo federal contratos de serviço, consultoria, assessoramento ou atividades similares, vinculados, ainda que indiretamente, ao órgão ou entidade em que tenha ocupado o cargo ou emprego; ou d) intervir, direta ou indiretamente, em favor de interesse privado perante órgão ou entidade em que haja ocupado cargo ou emprego ou com o qual tenha estabelecido relacionamento relevante em razão do exercício do cargo ou emprego.

Algumas vedações aos membros do Conselho Diretor durante a ocupação do cargo são definidas no artigo 11 do Anexo I do Decreto nº 10.474/20, dentre as quais:

(i) o recebimento de honorários ou percentagens;

(ii) o exercício de profissão liberal, exceto as constitucionalmente permitidas;

(iii) a participação, na forma de controlador, diretor, administrador, gerente, preposto ou mandatário, de sociedade civil, comercial ou empresas;

(iv) a emissão de parecer sobre matéria de sua especialização, ainda que em tese, ou a atuação como consultor de empresa;

(v) a manifestação, por qualquer meio de comunicação, opinião sobre processo pendente de julgamento ou juízo depreciativo sobre despachos, votos ou sentenças de órgãos judiciais, ressalvada a crítica nos autos, em obras técnicas ou no exercício do magistério; e

(vi) o exercício de atividade político-partidária.

Art. 55-G. Ato do Presidente da República disporá sobre a estrutura regimental da ANPD.

§ 1º Até a data de entrada em vigor de sua estrutura regimental, a ANPD receberá o apoio técnico e administrativo da Casa Civil da Presidência da República para o exercício de suas atividades.

§ 2º O Conselho Diretor disporá sobre o regimento interno da ANPD.

Art. 55-H. Os cargos em comissão e as funções de confiança da ANPD serão remanejados de outros órgãos e entidades do Poder Executivo federal. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-I. Os ocupantes dos cargos em comissão e das funções de confiança da ANPD serão indicados pelo Conselho Diretor e nomeados ou designados pelo Diretor-Presidente. (Incluído pela Lei nº 13.853, de 2019)

O ato mencionado no *caput* do art. 55-G já foi realizado, e se refere ao Decreto nº 10.474, de 26 de agosto de 2020, que aprovou a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da ANPD, e também remanejou e transformou cargos em comissão e funções de confiança de outros

órgãos da Administração Pública para a ANPD. Deste modo, segundo consta no Anexo II do referido Decreto nº 10.724/20, a autoridade contará, inicialmente, com 36 membros, remanejados de outras funções do Poder Executivo Federal[212].

[212] Até a data da publicação deste livro, o regimento interno ainda se encontrava em elaboração, com previsão para o 1º semestre de 2021, de acordo com a agenda regulatória da ANPD, tornada pública pela Portaria nº 11, de 27 de janeiro de 2021, da Presidência da República. Disponível em: < https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313>. Acesso em: 29/01/2021.

Art. 55-J. Compete à ANPD:

I - zelar pela proteção dos dados pessoais, nos termos da legislação;

II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei;

III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;

IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;

V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação;

VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;

VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;

VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis;

IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;

X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial;

XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei;

XII - elaborar relatórios de gestão anuais acerca de suas atividades;

XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei;

XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento;

XV - arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas;

XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público;

XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942;

XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei;

XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso);

XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos;

XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento;

XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal;

XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e

XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei.

§ 1º Ao impor condicionantes administrativas ao tratamento de dados pessoais por agente de tratamento privado, sejam eles limites, encargos ou sujeições, a ANPD deve observar a exigência de mínima intervenção, assegurados os fundamentos, os princípios e os direitos dos titulares previstos no art. 170 da Constituição Federal e nesta Lei.

§ 2º Os regulamentos e as normas editados pela ANPD devem ser precedidos de consulta e audiência públicas, bem como de análises de impacto regulatório.

§ 3º A ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados, conforme legislação específica, e o tratamento de dados pessoais, na forma desta Lei.

§ 4º A ANPD manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e

entidades da administração pública responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar as competências regulatória, fiscalizatória e punitiva da ANPD.

§ 5º No exercício das competências de que trata o caput deste artigo, a autoridade competente deverá zelar pela preservação do segredo empresarial e do sigilo das informações, nos termos da lei.

§ 6º As reclamações colhidas conforme o disposto no inciso V do caput deste artigo poderão ser analisadas de forma agregada, e as eventuais providências delas decorrentes poderão ser adotadas de forma padronizada.

Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública. (Incluído pela Lei nº 13.853, de 2019)

Parágrafo único. A ANPD articulará sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais e será o órgão central de interpretação

desta Lei e do estabelecimento de normas e diretrizes para a sua implementação. (Incluído pela Lei nº 13.853, de 2019)

1. Dos poderes da Administração

As competências da ANPD, previstas no art. 55-J, vinculam a atuação do órgão ao cumprimento e fiscalização da Lei Geral de Proteção de Dados. Estas competências envolvem, sobretudo, a utilização dos chamados "poderes da Administração Pública", os quais são inerentes a todas as entidades estatais[213].

No âmbito das competências da ANPD, dois tipos de poderes se destacam, quais sejam, o poder de polícia e o poder regulamentar. Enquanto o poder de polícia é a faculdade de que dispõe a Administração Pública para condicionar e restringir o uso e gozo de bens, atividades e direitos individuais, em benefício da coletividade ou do próprio Estado [214], o poder regulamentar busca conferir à

[213] Nesse sentido, a doutrina classifica estes poderes da seguinte forma: (i) poder vinculado; (ii) poder discricionário; (iii) poder hierárquico; (iv) poder disciplinar; (v) poder regulamentar e (vi) poder de polícia. Cf. MEIRELLES, Hely Lopes. **Direito Administrativo Brasileiro**.42ª ed. São Paulo: Malheiros, 2016. p. 152.

[214] O conceito de poder de polícia também se encontra positivado no artigo 78 do Código Tributário Nacional: "Considera-se poder de polícia atividade da administração pública que, limitando ou disciplinando direito, interesse ou liberdade, regula a prática de ato ou abstenção de fato, em razão de interesse público concernente à segurança, à higiene, à ordem, aos costumes, à disciplina da produção e do mercado, ao exercício de atividades econômicas dependentes de concessão ou autorização do Poder Público, à tranqüilidade pública ou ao respeito à propriedade e aos direitos individuais ou coletivos". BRASIL. **Lei nº 5.172, de 25 de outubro de 1966**. Denominado Código Tributário Nacional. Dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios.

Administração a competência de regulamentar a Lei e suprir, com normas próprias, eventuais omissões do Poder Legislativo.

Diante da imprevisibilidade e rápida mutação das atividades de tratamento de dados pessoais, este poder regulamentar deverá ser especialmente útil, uma vez que possibilita à ANPD editar atos normativos de forma mais célere que o Poder Legislativo, regulamentando, deste modo, tanto o que está disposto na própria Lei, quanto aquelas situações inéditas e imprevistas relacionadas ao tratamento de dados pessoais que deverão surgir nos próximos anos[215].

2. A atuação conjunta com outros órgãos governamentais

Nos termos do inciso XXIII do art. 55-J e do art. 55-K da LGPD, e também do art. 2º, § 8º do Anexo I do Decreto nº 10.474/20, a ANPD deverá articular com outros órgãos e entidades de setores regulados da economia para harmonizar as normativas atinentes à proteção de dados pessoais, de acordo com as disposições da LGPD. Na mesma linha, seguem as disposições do §4º do art. 55-J, que prevê a criação de um fórum permanente entre os órgãos reguladores e a ANPD para a cooperação acerca das questões que envolvem a proteção de dados pessoais.

[215] Estas regulamentações deverão ser editadas, em sua maioria, até o ano de 2023, de acordo com a agenda regulatória da ANPD, tornada pública pela Portaria nº 11, de 27 de janeiro de 2021, da Presidência da República. Disponível em: < https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313>. Acesso em: 29/01/2021.

Um exemplo mais concreto dessa necessidade de harmonização regulamentar entre os diversos órgãos da Administração Pública se dá na esfera de aplicação do Código de Defesa do Consumidor. Tendo em vista que a Portaria nº 1.840/12, do Ministério da Justiça, delegou ao Departamento de Proteção e Defesa do Consumidor (DPDC), órgão que integra a Senacon (Secretaria Nacional do Consumidor), as competências de fiscalizar demandas que envolvam relevante interesse nacional e aplicar sanções administrativas por violações a normas de direito do consumidor, poderia haver, em tese, decisões contraditórias na seara da proteção de dados e do consumidor.

As mesmas disposições são válidas quando da necessidade de efetivação das sanções contra entes da própria Administração, ocasiões em que deverá haver uma comunicação efetiva com os órgãos de controle interno, como a Controladoria Geral da União (CGU), o Tribunal de Contas da União (TCU) e o Conselho Nacional de Justiça (CNJ), conforme o disposto no inciso XXII do art. 55-J da Lei.

3. Política Nacional de Proteção de Dados Pessoais

Chama atenção também a competência da ANPD presente no inciso III do art. 55-J, pela qual ela deverá elaborar as diretrizes de uma "Política Nacional de Proteção de Dados", sem maiores explicações sobre qual seria o objeto desta norma futura. Entretanto, o termo "política nacional" abrange uma gama de diversos instrumentos

normativos e regulatórios que centralizam e organizam, em âmbito nacional, determinadas atividades afeitas ao Estado.

Neste sentido, pode-se inferir que essa "Política Nacional de Proteção de Dados" deverá ser constituída com o intuito de centralizar e organizar a implementação de políticas públicas relacionadas à proteção de dados e à privacidade dos titulares, através de uma legislação complementar à LGPD.

Art. 55-L. Constituem receitas da ANPD: (Incluído pela Lei nº 13.853, de 2019)

I - as dotações, consignadas no orçamento geral da União, os créditos especiais, os créditos adicionais, as transferências e os repasses que lhe forem conferidos; (Incluído pela Lei nº 13.853, de 2019)

II - as doações, os legados, as subvenções e outros recursos que lhe forem destinados; (Incluído pela Lei nº 13.853, de 2019)

III - os valores apurados na venda ou aluguel de bens móveis e imóveis de sua propriedade; (Incluído pela Lei nº 13.853, de 2019)

IV - os valores apurados em aplicações no mercado financeiro das receitas previstas neste artigo; (Incluído pela Lei nº 13.853, de 2019)

V - (VETADO); (Incluído pela Lei nº 13.853, de 2019)

VI - os recursos provenientes de acordos, convênios ou contratos celebrados com entidades, organismos ou empresas, públicos ou privados, nacionais ou internacionais; (Incluído pela Lei nº 13.853, de 2019)

VII - o produto da venda de publicações, material técnico, dados e informações, inclusive para fins de licitação pública. (Incluído pela Lei nº 13.853, de 2019)

Quando do processo legislativo, as discussões acerca das receitas da ANPD giravam em torno da exclusão ou inclusão das verbas recebidas a título de aplicação das sanções pecuniárias.

Acertadamente, optou o legislador pela subvenção direta da autoridade pela União, considerando que a disposição em contrário poderia acabar por incentivar a aplicação de sanções de valor mais elevado por parte da autoridade. Esta subvenção direta não impede, entretanto, que a ANPD se financie também através de acordos, convênios ou contratos, ou mesmo através de doações e aplicações de capital próprio da agência.

Art. 56. (VETADO).

Art. 57. (VETADO).

Seção II - Do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

Art. 58. (VETADO).

Art. 58-A. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto de 23 (vinte e três) representantes, titulares e suplentes, dos seguintes órgãos: (Incluído pela Lei nº 13.853, de 2019)

I - 5 (cinco) do Poder Executivo federal; (Incluído pela Lei nº 13.853, de 2019)

II - 1 (um) do Senado Federal; (Incluído pela Lei nº 13.853, de 2019)

III - 1 (um) da Câmara dos Deputados; (Incluído pela Lei nº 13.853, de 2019)

IV - 1 (um) do Conselho Nacional de Justiça; (Incluído pela Lei nº 13.853, de 2019)

V - 1 (um) do Conselho Nacional do Ministério Público; (Incluído pela Lei nº 13.853, de 2019)

VI - 1 (um) do Comitê Gestor da *Internet* no Brasil; (Incluído pela Lei nº 13.853, de 2019;

VII - 3 (três) de entidades da sociedade civil com atuação relacionada a proteção de dados pessoais; (Incluído pela Lei nº 13.853, de 2019)

VIII - 3 (três) de instituições científicas, tecnológicas e de inovação; (Incluído pela Lei nº 13.853, de 2019)

IX - 3 (três) de confederações sindicais representativas das categorias econômicas do setor produtivo; (Incluído pela Lei nº 13.853, de 2019)

X - 2 (dois) de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais; e (Incluído pela Lei nº 13.853, de 2019)

XI - 2 (dois) de entidades representativas do setor laboral. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Os representantes serão designados por ato do Presidente da República, permitida a delegação. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Os representantes de que tratam os incisos I, II, III, IV, V e VI do caput deste artigo e seus suplentes serão indicados pelos titulares dos respectivos órgãos e entidades da administração pública. (Incluído pela Lei nº 13.853, de 2019)

§ 3º Os representantes de que tratam os incisos VII, VIII, IX, X e XI do caput deste artigo e seus suplentes: (Incluído pela Lei nº 13.853, de 2019)

I - serão indicados na forma de regulamento; (Incluído pela Lei nº 13.853, de 2019)

II - não poderão ser membros do Comitê Gestor da *Internet* no Brasil; (Incluído pela Lei nº 13.853, de 2019)

III - terão mandato de 2 (dois) anos, permitida 1 (uma) recondução. (Incluído pela Lei nº 13.853, de 2019)

§ 4º A participação no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será considerada prestação de serviço público relevante, não remunerada. (Incluído pela Lei nº 13.853, de 2019)

O Conselho Nacional de Proteção de Dados Pessoais, nos termos do Anexo I do Decreto nº 10.474/20, é um órgão consultivo e multidisciplinar da ANPD, que busca integrar os diferentes *stakeholders* interessados nas questões de proteção de dados.

A composição do CNPD, até a publicação do presente livro, não havia sido definida, mas deverá contar com 13 representantes do governo, 02 representantes do setor produtivo, 02 representantes do

setor laboral, 03 representantes da academia e 03 representantes da sociedade civil.

O Anexo I do Decreto nº 10.474/20 também regulamenta, em seu art. 15, que os membros do CNPD serão indicados pelos respectivos órgãos, ao Ministro de Estado Chefe da Casa Civil, para posterior nomeação pelo Presidente da República.

Art. 58-B. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade: (Incluído pela Lei nº 13.853, de 2019)

I - propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD; (Incluído pela Lei nº 13.853, de 2019)

II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)

III - sugerir ações a serem realizadas pela ANPD; (Incluído pela Lei nº 13.853, de 2019)

IV - elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e (Incluído pela Lei nº 13.853, de 2019

V - disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população. (Incluído pela Lei nº 13.853, de 2019)

Art. 59. (VETADO).

O art. 58-B reforça o caráter consultivo do CNPD para a execução das atividades da ANPD, o que deverá se dar através da

proposição de diretrizes estratégicas e de subsídios para a elaboração da “Política Nacional de Proteção de Dados Pessoais e da Privacidade”, além de elaborar relatórios anuais de avaliação da execução da mencionada Política.

CAPÍTULO X - DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 60. A Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da *Internet*), passa a vigorar com as seguintes alterações:

"Art. 7º .....

.....

X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de *internet*, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais;

....." (NR)

"Art. 16. .....

.....

II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a proteção de dados pessoais." (NR)

O art. 60 evidencia o esforço do legislador em harmonizar as duas principais legislações que regem a utilização da *internet* no Brasil: a Lei Geral de Proteção de dados e o Marco Civil da *Internet*.

Assim, quando o usuário de *internet* solicitar a exclusão de seus dados, deverão ser observadas as disposições tanto do MCI quanto da LGPD. Da mesma forma, a retenção de dados por provedores de aplicações da *internet* deverá estar adequada a alguma das bases legais de tratamento previstas na LGPD.

Art. 61. A empresa estrangeira será notificada e intimada de todos os atos processuais previstos nesta Lei, independentemente de procuração ou de disposição contratual ou estatutária, na pessoa do agente ou representante ou pessoa responsável por sua filial, agência, sucursal, estabelecimento ou escritório instalado no Brasil.

Tendo em vista que a LGPD pode se aplicar, inclusive, a agentes de tratamento que não estejam sediados no Brasil, conforme dispõe o art. 3º da Lei, houve a ampliação das possibilidades de notificação e intimação para além daquelas consideradas no Código de Processo Civil[216], adicionando a possibilidade de escritórios ou pessoas físicas de representantes também receberem quaisquer notificações e intimações de atos processuais.

[216] [216] BRASIL. **Lei nº 13.105, de 16 de março de 2015**. Código de Processo Civil. Art. 75. Serão representados em juízo, ativa e passivamente: [...] X - a pessoa jurídica estrangeira, pelo gerente, representante ou administrador de sua filial, agência ou sucursal aberta ou instalada no Brasil; [...]§ 3º O gerente de filial ou agência presume-se autorizado pela pessoa jurídica estrangeira a receber citação para qualquer processo.

Art. 62. A autoridade nacional e o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep), no âmbito de suas competências, editarão regulamentos específicos para o acesso a dados tratados pela União para o cumprimento do disposto no § 2º do art. 9º da Lei nº 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional), e aos referentes ao Sistema Nacional de Avaliação da Educação Superior (Sinaes), de que trata a Lei nº 10.861, de 14 de abril de 2004.

Cabe a interpretação deste artigo em conjunto com as disposições do art. 55-J e art. 55-K, que dispõem sobre a atuação conjunta da ANPD com outros órgãos do governo.

Art. 63. A autoridade nacional estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados.

Até o momento de escrita do presente texto, a ANPD ainda não havia se pronunciado acerca desta regulamentação descrita no art. 63 da Lei. Mesmo que a redação deste artigo não esclareça o que deva ser feito até que haja tal, nada impede que o agente de tratamento adote as medidas técnicas e organizacionais necessárias para a proteção destes bancos de dados, como de ameaças de um acesso não autorizado, por exemplo.

Ademais, caso haja o tratamento de quaisquer dados coletados em momento anterior à vigência da LGPD, o agente de tratamento deverá se atentar à efetivação de todas as medidas de segurança que possibilitem a demonstração da sua boa-fé, perante a ANPD, em uma eventual fiscalização, que podem incluir, dentre outras medidas, a segregação dos dados coletados antes da vigência da Lei e a eliminação de dados desatualizados com os dados a partir de 18/09/2020, a título de exemplificação.

Art. 64. Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

A afirmativa de que direitos e princípios, expressos na LGPD, não devem excluir outros direitos previstos no ordenamento jurídico pátrio relacionados à matéria de proteção de dados pessoais coloca novamente em pauta a necessidade de harmonização entre as diversas normativas existentes sobre o assunto, incluindo os direitos previstos em tratados internacionais dos quais o Brasil seja parte.

Art. 65. Esta Lei entra em vigor: (Redação dada pela Lei nº 13.853, de 2019)

I - dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e (Incluído pela Lei nº 13.853, de 2019)

I-A – dia 1º de agosto de 2021, quanto aos arts. 52, 53 e 54; (Incluído pela Lei nº 14.010, de 2020)

II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos. (Incluído pela Lei nº 13.853, de 2019)

Quanto ao período de *vacatio legis* da LGPD, o legislador optou por fazê-lo de forma escalonada. Em uma primeira fase, no dia 28 de dezembro de 2018, entraram em vigor as normas relativas à ANPD e ao CNPD, certamente para que estes órgãos fossem devidamente estabelecidos antes da entrada em vigor da legislação.

Já em uma segunda fase, no dia 18 de setembro de 2020, entraram em vigor todos os demais Capítulos da Lei, excluindo-se o Capítulo VIII, que trata das fiscalizações e deverá entrar em vigor no dia 1º de agosto de 2021, conforme dispõe o inciso I-A do artigo em comento.

CONSIDERAÇÕES FINAIS

A aprovação da LGPD no Brasil se deu em um contexto muito diferente do europeu, vez que a aprovação do RGPD resultou de discussões sobre a proteção de dados pessoais que existem há décadas. Deste modo, tendo em vista que este tema possui ares de novidade no território nacional, tanto aos agentes públicos quanto aos agentes privados, a presente obra teve como objetivo sanar algumas dúvidas que podem surgir, eventualmente, entre a teoria e a prática na proteção de dados pessoais.

Apesar de a aprovação da LGPD constituir um quadro normativo há muito aguardado e necessário para o atingimento dos objetivos propostos pela Constituição Federal, a referida Lei não é isenta de algumas falhas e omissões substanciais, o que acaba por demonstrar a grande diferença, um verdadeiro abismo, entre a teoria e a prática no esforço de proteção desses dados.

Desta forma, para um melhor entendimento do tema, buscou-se ilustrar algumas dessas aplicações práticas da nova Lei Geral de Proteção de Dados, através de estudos de caso envolvendo alguns setores econômicos que estão sendo direta e profundamente afetados pela Lei, tais como o setor da saúde, da construção civil, de seguros e de condomínios. Tratam-se de casos verídicos, em que teriam ocorrido divulgações não-autorizadas de dados pessoais das mais diversas

formas, utilizando-se, entretanto, nomes fictícios para proteger a real identidade dos envolvidos.

Embora estes casos tenham ocorrido previamente à vigência da LGPD, será realizada uma discussão sobre quais seriam os possíveis impactos sobre os agentes de tratamento, caso ocorressem nos tempos atuais, em que a Lei se encontra vigente.

1. Corretoras de Seguros

No primeiro caso será feita uma análise dos impactos da LGPD em uma corretora de seguros.

Um indivíduo, chamado "João", comprou um carro através de um leilão, com o intuito de presentear sua esposa. Entretanto, João não revela a origem do carro, que consideraria degradante a ela.

Com o intuito de contratar uma apólice de seguro para o veículo, se dirige à corretora de seguros "Angra dos Reis", local em que é atendido por "Maria", lhe informando alguns de seus dados pessoais para a contratação do seguro, incluindo o seu endereço.

De posse destas informações, Maria identifica que João residia em seu condomínio, ou seja, no condomínio "Campos Verdes", e ao chegar a sua casa, revela a "José", seu marido, a informação – de que o vizinho teria comprado carro de leilão –

Dias depois, por um determinado motivo, ocorreu uma discussão acalorada entre João e José, em um grupo de WhatsApp do condomínio, na qual José, com o intuito de humilhá-lo publicamente, afirma que ao menos não havia comprado carro de leilão para sua esposa.

Assim, a esposa de João toma ciência da procedência do veículo que recebera de presente, o que resultou em diversos atritos entre ela e João, seu esposo.

A partir do caso narrado acima, podem ser verificados diversos pontos de infração à LGPD, a seguir mencionados:

i. A divulgação das informações pessoais sobre a origem dos bens de João constitui um incidente de segurança da informação, que teria o condão de causar inúmeros prejuízos reputacionais e econômicos à corretora de seguros, além de processos civis por parte do titular, no caso, João, sem prejuízo de eventuais sanções pela ANPD.

ii. Maria, por sua vez, poderia ser condenada a indenizar a corretora através de uma ação de regresso, com fulcro no art. 932, inciso III do Código Civil e também com previsão no art. 42, §4º da LGPD.

iii. Maria também poderia ser processada criminalmente e denunciada no crime de violação de sigilo profissional, previsto no art. 154 do Código Penal. Seu marido, José, poderia ser processado pelo crime de injúria, constante do art. 140 do Código Penal.

iv. Embora não seja o foco deste primeiro estudo de caso, tem-se que o condomínio não poderia ter criado um grupo de WhatsApp em formato aberto, pelo seu potencial de gerar discussões desnecessárias entre os condôminos e por expor indevidamente alguns de seus dados pessoais, como os seus nomes e números de telefone. O ideal seria, pois, a criação de uma lista de transmissão direta para a comunicação da administração com os condôminos.

2. Condomínios residenciais

No segundo caso, assim como no primeiro, será analisada uma situação que também envolve uma divulgação não-autorizada de dados pessoais no âmbito de condomínios residenciais.

Um indivíduo, chamado "Guilherme", chega de carro com a amante ao condomínio residencial "Vivendas da Prata", local onde ela residia. Um dos porteiros do condomínio, chamado "Manoel", reconhece Guilherme através do sistema de câmeras, vez que eram da mesma igreja e sabia, inclusive, que ele era casado com outra pessoa.

Então, Manoel fotografou o monitor do sistema de câmeras do condomínio, no momento exato em que Guilherme estava beijando sua amante. Horas depois, esta fotografia chega até a esposa de Guilherme, o que posteriormente resulta em um divórcio.

O caso narrado acima demonstra a importância que políticas de segurança da informação bem aplicadas têm para os condomínios.

Isto porque, embora tivesse o condomínio instalado diversas câmeras de vigilância, com o fim de combater ameaças externas, não se atentou em utilizar o mesmo sistema para coibir a ocorrência de ameaças internas, ou seja, não instalou câmeras também na portaria, que poderiam se mostrar cruciais para ao menos coibir condutas como a do porteiro do caso narrado.

Ainda, em uma eventual ação judicial movida por Guilherme contra o referido condomínio, este poderia provar a culpa de Manoel, o que certamente o faria através de ação de regresso, prevista no art. 42, §4º da LGPD. No entanto, sem as provas contra o porteiro, obtidas pelo sistema de vigilância, esta ação de regresso restaria prejudicada.

Na esteira do que foi mencionado nos dois últimos casos, é possível vislumbrar algumas outras práticas comuns que não poderão mais ser realizadas em condomínios que almejem agir em respeito à proteção de dados pessoais dos condôminos, a saber:

i. Listas de devedores do condomínio devem possuir o acesso restrito apenas aos funcionários que necessariamente necessitem acessar estas informações, sendo recomendável que o Condomínio procure contratar, para a realização de cobranças extrajudiciais, agências que estiverem devidamente em *compliance* com a LGPD;

ii. Os dados biométricos são considerados sensíveis, e devem estar em bases de dados segregadas e com acesso restrito;

iii. Listas de convidados também devem ter o seu acesso restrito, sendo recomendável que o Condomínio colete apenas os dados necessários dos convidados para o provimento de segurança aos demais condôminos. Também deve se atentar ao tratamento de dados pessoais sensíveis, que podem ser coletados apenas para determinadas finalidades, estritamente definidas na LGPD.

3. Incorporadoras e Imobiliárias

No terceiro caso, será realizada a análise de incorporadoras e imobiliárias, que tratam uma grande quantidade de dados pessoais no exercício de suas operações, em um cenário hipotético.

Uma incorporadora denominada "Campos Elíseos", a fim de vender apartamentos na planta, realizou parcerias com diversas corretoras de imóveis. Entretanto, um dos funcionários destas imobiliárias divulgou, de má-fé, os dados pessoais dos compradores dos imóveis em uma base de dados de acesso público, na *internet*.

Diante desta divulgação não-autorizada, alguns titulares resolveram ingressar na justiça contra a incorporadora Campos Elíseos, alegando que ela teria descumprido a LGPD, em uma identificação correta de que este agente de tratamento teria muito mais condições de pagar uma indenização do que a corretora de imóveis.

Analisado o incidente, tem-se então que a incorporadora, neste caso, certamente seria condenada se não estivesse em conformidade

com os ditames da LGPD, pois não teria como demonstrar o seu efetivo *compliance* com a Lei, ou mesmo se valer de qualquer das excludentes prevista no art. 43 da Lei.

Pode-se considerar, ainda, uma ocasião em que algum indivíduo mal-intencionado cruze os dados provenientes da incorporadora com outros dados de acesso público, como aqueles presentes em redes sociais, afirmando serem todos eles provenientes da construtora, o que certamente majoraria o valor da indenização por poder configurar, em tese, uma afronta ao princípio da necessidade e da adequação.

Na verdade, em um julgado recente contra uma renomada construtora, houve a primeira aplicação da LGPD, com a condenação fundamentada na teoria da responsabilidade objetiva do CDC, aventada pelo art. 45 da LGPD, como demonstra o excerto do julgado abaixo colacionado:

Tampouco desnecessário aferir se outras pessoas físicas ou jurídicas participaram da ilicitude (como no caso de corretores de imóveis), porquanto todos que participam da cadeia produtiva respondem de forma solidária pelos danos causados (arts. 7º, parágrafo único, e 25, I, CDC). A própria testemunha da ré, Sr. C.E.C.P., afirmou que não seria impossível que corretores compartilhassem dados dos clientes, bem como teria trabalhado como corretor em alguns empreendimentos da ré e que esta não teria treinamento que abordasse sigilo de dados (fls. 798/801).

Entretanto, mesmo sendo condenada, a construtora poderia se valer de uma ação de regresso contra os agentes de tratamento que teriam realizado o tratamento de dados pessoais fora das finalidades previstas, o que poderia ser facilitado caso já houvesse o enquadramento da incorporadora na LGPD.

Tendo em vista as práticas recorrentes de mercado, é de se esperar que os controladores de maior porte já tenham realizado a devida adequação à LGPD, enquanto os menores, em sua grande maioria, desconhecem a Lei ou simplesmente a ignoram.

Especialmente nos ramos que envolvem a corretagem (seguros, saúde suplementar, imobiliárias), que trata de um intermediário na relação entre o consumidor e o fornecedor, deverão existir muitos conflitos relacionados com a proteção de dados pessoais e com as responsabilidades de cada agente de tratamento, como pode se observar da decisão paradigmática acima descrita.

Nestes casos em que existe mais de uma controladora dos dados pessoais, há de se averiguar se ambos os agentes de tratamento estariam em *compliance* e, também, quais teriam sido as medidas de adequação à LGPD, efetivamente realizadas por cada um deles.

4. Hospitais e setor da saúde

A área de saúde trata diretamente dados pessoais sensíveis dos titulares, e já conta com agência reguladora própria, no caso, a Agência Nacional de Saúde Suplementar – ANS.

No incidente aqui em questão, um determinado indivíduo, chamado "Paulo", começou a frequentar um determinado hospital para realização de tratamentos médico. Uma determinada enfermeira identificou que ele seria o pastor da sua igreja e percebeu que ele estava muito magro. Curiosa, esta enfermeira acessou um computador que o médico havia deixado logado e descobriu que o pastor havia desenvolvido AIDS.

Espantada com esta informação, ela começou a investigar de maneira mais aprofundada a vida do pastor, e acabou por descobrir que ele tinha em uma relação extraconjugal homoafetiva. De posse desta descoberta, esta enfermeira divulgou estas informações na igreja que frequentava, e Paulo acabou por ser destituído de sua função pela instituição religiosa e, consequentemente, se divorciando de sua esposa.

Neste caso, existem inúmeras violações à proteção de dados sensíveis de Paulo, que não poderiam ter sido divulgadas sem o seu consentimento expresso, o que pode dar ensejo a possíveis indenizações ao titular e fiscalizações por parte da ANPD.

Deste modo, o hospital poderia ter adotado algumas políticas internas que teriam inibido toda esta situação com o titular. A título de

exemplo, poderia ter criado um sistema de *logoff* automático dos médicos após alguns minutos sem uso, como medida técnica, ou também uma política de mesa limpa, como medida organizacional.

Já a enfermeira poderia, nesta situação, ser denunciada pelo crime tipificado no inciso V do art. 1º da 12.984/14, além de poder ser condenada a indenizar o titular em conjunto com o hospital.

O médico também agiu de maneira displicente, pois deveria ter tomado os cuidados em se "deslogar" do sistema quando deixou a sua sala. Ele também poderia ser responsabilizado civilmente em ação de regresso do hospital, pois teria realizado ato culposo, ou seja, descumprido com o seu dever de proteção dos dados pessoais de seus pacientes.

5. Outros casos sobre dados sensíveis sobre saúde

Ainda tratando-se de dados sensíveis sobre a saúde dos titulares, mas com consequências em outros setores, pode-se citar o caso que se refere a um indivíduo que teria pego um atestado para fazer uma cirurgia de hemorroida.

No entanto, uma pessoa que trabalhava no RH da empresa identificou a doença pelo CID informado, sendo o indivíduo posteriormente apelidado como "hemorroida" dentro da empresa, o que rendeu à empresa uma condenação alta em uma ação trabalhista.

Nesse sentido, cumpre destacar o cuidado que colaboradores, de maneira geral, deverão ter em deixar documentos sigilosos soltos na mesa.

Há também um caso parecido em que um indivíduo, chamado "Kleber", funcionário de uma agência bancária, telefonou para o seu supervisor avisando-o de que não teria como ir trabalhar, por estar doente. O supervisor apenas pediu que Kleber apresentasse o atestado no dia seguinte, o que foi obedecido por ele.

Entretanto, o supervisor percebeu que o atestado entregue pelo funcionário era de um hospital localizado em um bairro afastado de sua residência, momento em que entrou em contato com o referido hospital e descobriu que não havia qualquer entrada de Kleber nos sistemas do hospital, e que, inclusive, naquela data o médico que o teria atendido sequer estava trabalhando.

O supervisor então pediu que o funcionário esclarecesse o fato, e Kleber confessou que sua mãe, "Joana", trabalhava no hospital e havia subtraído o atestado da mesa do médico, em uma pilha de atestados em branco, já assinados e carimbados.

Este caso, sob o ponto de vista da LGPD, tem algumas implicações interessantes:

(i) O hospital, por possuir um sistema de segurança da informação falho e que permitia a qualquer funcionário o livre acesso a atestados já assinados, poderia ter toda a sorte de problemas com a

utilização fraudulenta destes documentos. Uma medida para a prevenção destes tipos de fraudes se dá pela utilização de atestados impressos através de sistemas próprios, com controle de acesso lógico. Sugere-se também utilizar um *QR Code* em que o empregador pudesse consultar a autenticidade do atestado, podendo inclusive suprimir o CID, evitando-se problema semelhante com o do RH, narrado anteriormente. Pode-se citar também a criação de certificados (através de *logs*) para o acesso a estes sistemas, permitindo ao hospital saber exatamente quem realizou determinada ação.

(ii) O funcionário e a sua mãe poderiam sofrer consequências na esfera cível, trabalhista e criminal. Assim, além de poderem ser demitidos por justa causa, poderiam ser indiciados pelo crime de falsidade ideológica. Ademais, podem ser obrigados a indenizar o empregador diretamente pelo cometimento de ato ilícito. Eventuais condenações na esfera cível e criminal também podem ter consequências no acesos de ambos ao mercado de trabalho, ou seja, se em ações trabalhistas não é possível identificar o titular de dados nos buscadores como o Google, nas ações cíveis e criminais isso é perfeitamente possível.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002**. Tecnologia da Informação. Código de Prática para Gestão da Segurança da Informação. Rio de Janeiro, 2013.

BASTOS, Celso Ribeiro. **Curso de direito constitucional**. São Paulo: Saraiva, 2021.

BEAL, Adriana. **Segurança da informação**: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo:Atlas, 2005.

BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado**. Revista do Advogado**. São Paulo, n. 144, nov. 2019.

_____. De 2010 a 2018: a discussão brasileira sobre uma lei geral de proteção de dados. **Jota**, 2018. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378. Acesso em: 30/12/2020.

_____. **Proteção de Dados Pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2020.

BRASIL**. Constituição da República Federativa do Brasil de 1988**.

_____. **Decreto nº 10.474, de 26 de agosto de 2020**. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança.

_____. **Decreto nº 8.771, de 11 de maio de 2016**. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.

_____. **Decreto nº 9.094, de 17 de julho de 2017**. Regulamenta dispositivos da Lei nº 13.460, de 26 de junho de 2017.

_____. **Decreto-lei nº 2.848, de 7 de dezembro de 1940**. Código Penal.

_____. **Decreto-lei nº 4.657, de 4 de setembro de 1942**. Lei de Introdução às normas do Direito Brasileiro.

_____. **Decreto-lei nº 5.452, de 1º de maio de 1943**. Aprova a Consolidação das Leis do Trabalho.

_____. **Lei nº 5.172, de 25 de outubro de 1966**. Denominado Código Tributário Nacional. Dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios.

_____. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências.

_____. **Lei nº 8.112, de 11 de dezembro de 1990**. Dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais.

_____. **Lei nº 8.212, de 24 de julho de 1991**. Dispõe sobre a organização da Seguridade Social, institui Plano de Custeio, e dá outras providências.

_____. **Lei nº 8.846, de 21 de janeiro de 1994**. Dispõe sobre a emissão de documentos fiscais e o arbitramento da receita mínima para efeitos tributários, e dá outras providências.

_____. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil.

_____. **Lei nº 12.813, de 16 de maio de 2013**. Dispõe sobre o conflito de interesses no exercício de cargo ou emprego do Poder Executivo federal e impedimentos posteriores ao exercício do cargo ou emprego; e revoga dispositivos da Lei nº 9.986, de 18 de julho de 2000,

e das Medidas Provisórias nº 2.216-37, de 31 de agosto de 2001, e 2.225-45, de 4 de setembro de 2001.

_____. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

_____. **Lei nº 13.105, de 16 de março de 2015**. Código de Processo Civil.

_____. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais.

_____. **Lei nº 13.848, de 25 de junho de 2019**. Dispõe sobre a gestão, a organização, o processo decisório e o controle social das agências reguladoras, altera a Lei nº 9.427, de 26 de dezembro de 1996, a Lei nº 9.472, de 16 de julho de 1997, a Lei nº 9.478, de 6 de agosto de 1997, a Lei nº 9.782, de 26 de janeiro de 1999, a Lei nº 9.961, de 28 de janeiro de 2000, a Lei nº 9.984, de 17 de julho de 2000, a Lei nº 9.986, de 18 de julho de 2000, a Lei nº 10.233, de 5 de junho de 2001, a Medida Provisória nº 2.228-1, de 6 de setembro de 2001, a Lei nº 11.182, de 27 de setembro de 2005, e a Lei nº 10.180, de 6 de fevereiro de 2001.

_____. **Medida provisória nº 954, de 17 de abril de 2020**. (Vigência encerrada). Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção

estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020.

_____. **Resolução BCB nº 4.658/18**. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

CAVOUKIAN, Ann. **Privacy by Design**: The 7 Foundational Principles - Implementation and Mapping of Fair Information Practices. Disponível em: https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implement-7found-principles.pdf. Acesso em: 21.12.2020.

CHEUNG, Anne S. Y.; WEBER, Rolf H. (orgs). **Privacy and Legal Issues in Cloud Computing**. Cheltenham: Edward Elgar Publishing, 2016.

COMPARATO, Fábio Konder. **Rumo à justiça**. São Paulo: Saraiva, 2010.

CONSELHO DA EUROPA. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal** Data. Disponível em [https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37]. Acesso em 16/11/2020.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais** – Comentada. 3º ed. São Paulo, Revista dos Tribunais, 2019.

DONEDA, Danilo. **Da privacidade à proteção de dados**. Rio de Janeiro: Renovar, 2005.

HARARI, Yuval Noah. **Homo Deus**. São Paulo: Companhia das Letras, 2016.

_____. Yuval Noah. **21 lições para o século 21**. São Paulo: Companhia das Letras. 2018.

HEILWEIL. Rebecca. **Why algorithms can be racist and sexist**. VOX, 2020. Disponível em: <https://www.vox.com/recode/2020/2/18/21121286/algorithms-bias-discrimination-facial-recognition-transparency>.

IDC's Global DataSphere Forecast Shows Continued Steady Growth in the Creation and Consumption of Data. **IDC**, 2020. Disponível em: https://www.idc.com/getdoc.jsp?containerId=prUS46286020. Acesso em 13/11/2020.

KANELLOS, Michael. 152,000 Smart Devices Every Minute In 2025: IDC Outlines The Future of Smart Things. **Forbes**, 2016. Disponível em https://www.forbes.com/sites/michaelkanellos/2016/03/03/152000-

smart-devices-every-minute-in-2025-idc-outlines-the-future-of-smart-things/?sh=281bb41d4b63. Acesso em 13/11/2020.

KOBIE, Nicole. The complicated truth about China's social credit system. **Wired**, 2019. Disponível em: <https://www.wired.co.uk/article/china-social-credit-system-explained>.

LAGO JR., Antônio. **Responsabilidade civil por atos ilícitos na Internet**. São Paulo: Ed. LTr, 2001.

LIMA, Cíntia Rosa Pereira de Lima. Consentimento inequívoco versus expresso: o que muda com a LGPD? **Revista do Advogado**. São Paulo, n. 144, nov. 2019

LISBOA, Roberto Senise. **Manual de Direito Civil**. V.3. Contratos. 7. E. São Paulo: Saraiva, 2012.

MACIEL, Kátia Regina Ferreira Lobo Andrade (Coord.). **Curso de direito da criança e do adolescente** – aspectos teóricos e práticos. 7ª ed. São Paulo: Saraiva, 2014.

MALDONADO, Viviane Nóbrega (Coord.); BLUM, Renato Opice (Coord.). **LGPD** – Lei Geral de Proteção de Dados – Comentada. 2ª ed. São Paulo: Revista dos Tribunais, 2019.

MCDONALD, Aleecia M.; CRANOR, Lorrie Faith. The Cost of Reading Privacy Policies. **Journal of Law and Policy for information Society**, 2008 v.4.

MEIRELLES, Hely Lopes. **Direito Administrativo Brasileiro**. 43º ed. São Paulo: Malheiros, 2018.

MELLO, Rafael Munhoz de. **Princípios constitucionais de direito administrativo sancionador**: As sanções administrativas à luz da Constituição Federal de 1988. São Paulo: Malheiros, 2007.

MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia. **Direito, inovação e tecnologia**. São Paulo: Saraiva, 2015. v. 1.

MENDES, Laura Schertel (Coord.); DONEDA, Danilo (Coord); SARLET, Ingo Wolfgang (Coord.) et al. **Tratado de Proteção de Dados Pessoais**. 1º ed. Rio de Janeiro: Forense, 2021.

MOREIRA, Rodrigo Pereira; MEDEIROS, Jaqueline Souza. Direito ao Esquecimento: Entre a Sociedade da Informação e a Civilização do Espetáculo. In: **Revista de Direito Privado**, vol. 70, ano 17. São Paulo: RT, 2016.

MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. **Revista do Advogado**. São Paulo, n. 144, nov. 2019.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. Myths and Fallacies of "Personally Identifiable Information". **Communications of the ACM**. Association for Computing Machinery, jun/2010, v. 53, n. 06.

Disponível em: www.cs.utexas.edu/~shmat/shmat_cacm10.pdf>. Acesso em 07.12.2020.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Declaração Universal dos Direitos Humanos**, 1949.

_____. **Human Right Council**. Thirty-second session. Disponível em: <http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/32/L.20>. Acesso em 16.11.2020.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS (OEA). **Corte Interamericana de Direitos Humanos**. Caso de Fontevecchia and D'amico v. Argentina, julgado em 29.11.2011. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_238_por.pdf. Acesso em: 27/01/2020.

OSÓRIO, Fábio Medina. **Direito Administrativo Sancionador**. São Paulo: Revista dos Tribunais, 2010.

SILVA, Jennifer Gomes da. Direito ao esquecimento: a bola agora está com o Supremo Tribunal Federal. **Conjur**, 2020. Disponível em: <https://www.conjur.com.br/2020-set-30/jeniffer-gomes-direito-esquecimento-pauta>. Acesso em 29/01/2021.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados

pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: < https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>. Acesso em 28/01/2021.

VILLAS BÔAS CUEVA, Ricardo, DONEDA, Danilo, MENDES, Laura Schertel (Org.). **Lei Geral de Proteção de Dados** (Lei nº 13.709/2018) - A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters, 2020.

VIOLA, Maria. **Transferência de dados entre Europa e Brasil**: Análise da Adequação da Legislação Brasileira. Rio de Janeiro: ITS Rio, 2019. Disponível em: <https://itsrio.org/wp-content/uploads/2019/12/Relatorio_UK_Azul_INTERACTIVE_Justificado.pdf>. Acesso em: 16.12.2020.

WONG, Julia Carrie. The Cambridge Analytica scandal changed the world – but it didn't change Facebook. **The Guardian**, 2019. Disponível em: <https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook>. Acesso em: 28/01/2021.