III ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

FLAVIA PIVA ALMEIDA LEITE

JOSÉ RENATO GAZIERO CELLA

AIRES JOSE ROVER

D597

Direito, governança e novas tecnologias I [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Aires Jose Rover; Flavia Piva Almeida Leite; José Renato Gaziero Cella – Florianópolis: CONPEDI, 2021.

Inclui bibliografia
ISBN: 978-65-5648-323-8
Modo de acesso: www.conpedi.org.br em publicações
Tema: Saúde: segurança humana para a democracia

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Governança. 3. Novas tecnologias. III Encontro Virtual do CONPEDI (1: 2021 : Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

III ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

Apresentação

No III Encontro Virtual do CONPEDI, realizado de 23 a 26 de junho de 2021, o grupo de trabalho "Direito, Governança e Novas Tecnologias I", que teve lugar na tarde de 23 de junho de 2021, destacou-se no evento não apenas pela qualidade dos trabalhos apresentados, mas pelos autores dos artigos, que são professores pesquisadores acompanhados de seus alunos pós-graduandos e um graduando. Foram apresentados 16 artigos objeto de um intenso debate presidido pelos coordenadores e acompanhado pela participação instigante do público presente na sala virtual.

Esse fato demonstra a inquietude que os temas debatidos despertam na seara jurídica. Cientes desse fato, os programas de pós-graduação em direito empreendem um diálogo que suscita a interdisciplinaridade na pesquisa e se propõe a enfrentar os desafios que as novas tecnologias impõem ao direito. Para apresentar e discutir os trabalhos produzidos sob essa perspectiva, os coordenadores do grupo de trabalho dividiram os artigos em três blocos, quais sejam a) proteção jurídica dos dados pessoais; b) algoritmos e inteligência artificial; e c) governança na sociedade em rede.

A proteção jurídica dos dados pessoais foi objeto do primeiro bloco de trabalhos, com as exposições e debates sobre os seguintes artigos: 1. "A Vulnerabilidade dos Dados Digitais e as Leis que Normatizam a Coleta no Cyber Espaço", de Jackson Lucena Santos e Elaine Késsia de Freitas Lira; 2. "Efetividade dos Mecanismos Jurisdicionais para Concretização de Direitos: o Poder Judiciário como Instrumento de Aplicação da LGPD", de Vinícius Borges Fortes e Vitor Luís Botton; 3. Proteção de Dados Pessoais dos Professores: das Vulnerabilidades do Ensino Remoto à Construção de Programas de Governança de Dados Pessoais nas Instituições de Ensino Superior", de Rosane Leal da Silva; 4. "Tecnologias Vestíveis e Capitalismo de Vigilância: do Compartilhamento de Dados sobre Saúde e a Proteção dos Direitos da Personalidade", de Raissa Arantes Tobbin e Valéria Silva Galdino Cardin; e 5. "A Aplicação da Lei Geral de Proteção de Dados (LGPD) para o Setor Financeiro, Considerando o Open Banking (Sistema Financeiro Aberto) e a 'Nova' Lei do Cadastro Positivo, de Thiales Borges Bonfim, Silvio Bitencourt da Silva.

Os algoritmos e a inteligência artificial foram o pano de fundo do segundo bloco de artigos apresentados, em que os problemas decorrentes de sua implantação foram apresentados e debatidos a partir dos seguintes trabalhos: 1. "Algoritmo, onde foi parar a Liberdade de

Expressão?", de Ícaro Ataia Rossi e Karem Luiza da Costa; 2. "Projeto Victor e MCDA-C: (In)Compatibilidade com a Carta Europeia de Ética sobre o Uso da Inteligência Artificial e com a Resolução 332 do CNJ", de Eduarda Perini da Silva; 3. "Isso é Muito 'Black Mirror': o Uso do 'Soft Law' na Regulação de Discriminações Algorítmicas", de Raphael Ferreira Santana Silva; 4. "Big Data, Softwares de Inteligência Artificial (IA) e a Proteção do Meio Ambiente Marinho", de Camila Cristiane de Carvalho Frade, Daniel Alberico Resende e Henrique de Almeida Santos"; e 5. "A Responsabilidade Civil Frente ao Assédio de Consumo: Publicidade Excessiva e a Perturbação do Sossego", de Stéphany Cindy Costa Baptistelli.

As discussões acerca da governança na sociedade em rede congregaram as apresentações dos seguintes trabalhos: 1. "Plataformas Digitais e Regulação da Neutralidade da Rede: como a Regulação Atende aos Interesses de Companhias com Dominância de Mercado", de Clara Leitão de Almeida; 2. "Da Governança Corporativa como Viabilizador da Sustentabilidade da Empresa ao Longo das Gerações", de Marcos Carsalade Rabello; 3. "A Necessidade de Normatização sobre os Dados Pessoais Disponíveis nos Cartórios de Registros Públicos", de Gelson Oliveira Ferri e Marco Aurélio Rodrigues da Cunha e Cruz; 4. "Multiparentalidade e os seus Efeitos no Direito Notarial: o Papel da Tecnologia em Tempos de Pandemia", de Jorge Alberto dos Santos e José Carlos Francisco dos Santos; 5. "Política em Rede: da Ampliação da Participação Política à Manipulação dos Cidadãos", de Sarah Priscila Feitosa Alexandre e Lucas Gonçalves da Silva; e 6. "Atuação do Estado em Rompimentos de Barragens no Paradigma do Estado Democrático de Direito", de Thiago Loures Machado Moura Monteiro e Antônio Luiz Lima Camargos Filho.

Os artigos que ora são apresentados ao público têm a finalidade de fomentar a pesquisa e fortalecer o diálogo interdisciplinar em torno do tema "Direito, Governança e Novas Tecnologias". Trazem consigo, ainda, a expectativa de contribuir para os avanços do estudo desse tema no âmbito da pós-graduação em direito brasileira, apresentando respostas para uma realidade que se mostra em constante transformação.

Os Coordenadores

Prof. Dr. Aires José Rover

Prof. Dr. José Renato Gaziero Cella

Prof. Dra. Flavia Piva Almeida Leite

A APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) PARA O SETOR FINANCEIRO, CONSIDERANDO O OPEN BANKING (SISTEMA FINANCEIRO ABERTO) E A "NOVA" LEI DO CADASTRO POSITIVO.

THE APPLICATION OF THE GENERAL DATA PROTECTION LAW (LGPD) IN BRAZIL FOR THE FINANCIAL SECTOR, CONSIDERING THE OPEN BANKING (OPEN FINANCIAL SYSTEM) AND THE "NEW" BRAZILIAN POSITIVE REGISTRATION LAW.

Thiales Borges Bonfim
Silvio Bitencourt da Silva

Resumo

Neste artigo, por meio de uma revisão da literatura sobre LGPD a partir da metodologia de pesquisa bibliográfica, além do arcabouço legal aplicável, se explorou a aplicação da Lei Geral de Proteção de Dados (LGPD) para o setor financeiro, considerando o Open Banking (Sistema Financeiro Aberto) e a "nova" Lei do Cadastro Positivo. Ao estar de acordo com as novas normas do Open Banking, a instituição também deve estar pronta para atender a LGPD. A padronização é a chave para um sistema de Open Banking dar certo, para mitigar vulnerabilidades e delimitar responsabilidades dos que operam nesse fluxo de informações.

Palavras-chave: Dados pessoais, Finanças, Instituições financeiras, Open banking, Proteção

Abstract/Resumen/Résumé

In this article, through a literature review on General Data Protection Law (LGPD) in Brazil based on the bibliographic research methodology, in addition to the applicable legal framework, the application of the LGPD for the financial sector was explored, considering Open Banking (Open Financial System) and the "new" Brazilian Positive Registration Law. When complying with the new rules of Open Banking, the institution must also be ready to meet the LGPD. Standardization is the key for an Open Banking system to work, to mitigate vulnerabilities and delimit the responsibilities of those who operate in this flow of information.

Keywords/Palabras-claves/Mots-clés: Personal data, Finance, Financial institutions, Open banking, Protection

1 INTRODUÇÃO

Na Era da Informação, uma nova etapa da sociedade industrial e da evolução histórica dos direitos humanos, a dignidade da pessoa humana perpassa pela proteção dos dados pessoais[1], em especial pelos dados sensíveis[2], o que propiciou a criação de novos regimes jurídicos para tutelar de modo mais rigoroso e pedagógico a coleta, armazenamento, tratamento, processamento, proteção e o sigilo dos dados (TEIXEIRA, 2021, p. 51-52).

Por conta disso, o setor financeiro acostumado a lidar com sigilo e dados de clientes e usuários é objeto de profunda evolução tecnológica e a tempo investe significativamente em recursos e tecnologia. Não apenas às tecnologias aplicadas, mas à gestão da informação financeira, base para novos avanços e aprimoramento dos serviços financeiros.

Ao longo das últimas décadas, as informações esparsas e mantidas em papel foram substituídas por bases de dados eletrônicos e incluídas em aplicativos, de modo a permitir a perenidade da informação, a facilidade de acesso e o cruzamento de dados, trazendo para esse setor um novo horizonte e imprimindo um novo dinamismo. No entanto, esse tipo de atividade deve andar em paralelo com o direito à privacidade e à proteção de dados pessoais dos usuários desses serviços. O crescimento exponencial no armazenamento de dados pessoais em sistemas informatizados traz, automaticamente, uma maior exposição de tais dados a um incidente de segurança, além de tornar mais fácil a eventual utilização não autorizada de tais informações (PALHARES, et al., 2020, p. 128-129).

Nesta direção, este artigo explora a aplicação da Lei Geral de Proteção de Dados – LGPD para o setor financeiro, considerando o *Open Banking* (Sistema Financeiro Aberto) e a "nova" Lei do Cadastro Positivo, por meio de uma revisão da literatura sobre LGPD a partir da metodologia de pesquisa bibliográfica baseada na análise da literatura já publicada em

[1] Conjunto de regras que visam impedir o tratamento inadequado, injusto ou antiético de dados pessoais. Está relacionado à chamada "privacidade informacional". Enquanto a proteção à privacidade, em sentido mais amplo, está mais voltada à preservação da intimidade, a proteção de dados pessoais se concentra em resguardar, contra abusos e mau usos, os dados ou informações que dizem respeito a cada um de nós. Ao fazê-lo, a proteção de dados visa resguardar direitos de alta significância. Nesse sentido, o regime de proteção de dados pessoais é, em grande parte, baseado na "autodeterminação informativa" (*informationelle Selbstbestimmung*), ou seja, a regulação jurídica da privacidade informacional está fortemente amparada no conceito de que o indivíduo (no caso, o titular dos dados) deve poder controlar livremente as formas de coleta, uso e revelação de seus dados pessoais pela sociedade. Essa é a única maneira pela qual é garantida ao indivíduo a preservação da capacidade de livre desenvolvimento de sua personalidade, entre outros direitos fundamentais.

[2] 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. São assim denominados por terem um tratamento diferenciado na lei, com uma tutela mais rígida, já que envolvem informações de foro mais íntimo.

forma de livros, artigos e literatura cinzenta (teses, dissertações, trabalhos apresentados em congressos, relatórios, etc.), além do arcabouço legal aplicável.

Além desta seção introdutória o artigo contempla o desenvolvimento da pesquisa em que com algumas noções básicas da LGPD e os elementos que a compõem, incluindo seus princípios, os direitos aos titulares de dados, as bases legais de tratamento desses dados, bem como as sanções e multas propostas, o papel do DPO, o entendimento sobre a Autoridade Nacional de Proteção de Dados (ANPD), e também esclarecer pontos referentes ao *Open Banking* (Sistema Financeiro Aberto) e a "nova" Lei do Cadastro Positivo. Na sequência são apresentadas as conclusões e, por fim, as referências adotadas para a revisão da literatura.

2 DESENVOLVIMENTO DA PESQUISA

2.1 Lei Geral de Proteção de Dados – LGPD

O fornecimento de dados pessoais para aquisição de produtos e serviços se tornou uma tarefa comum no mundo conectado (PALHARES, et al., 2020, p. 317). Os bancos de dados[3] que contêm dados pessoais aumentam o número de sujeitos que podem ter acesso a um conjunto sempre mais detalhado e preciso de informações sobre terceiros, o que faz com que o estatuto jurídico desses dados se torne um dos pontos centrais que vão definir a própria autonomia, identidade e liberdade do cidadão contemporâneo (DONEDA, 2011).

Ademais, a proteção dos dados pessoais compõe uma das partes essenciais da tutela da dignidade da pessoa humana, mostrando-se essencial para a garantia das liberdades fundamentais, da igualdade, da solidariedade e da integridade psicofísica. A tutela dos dados relativos à pessoa natural mostra-se hoje vital para que ela se realize integralmente e se relacione na sociedade, representando garantia de maior segurança às informações dos cidadãos e impedindo práticas autoritárias e de vigilância por parte de instituições públicas e privadas (FRAZÃO; TEPENDINO; OLIVA, 2020, p. 282).

Por esse e outros motivos, a proteção dos dados pessoais recebe destaque em sociedade e com a Lei Geral de Proteção de Dados (LGPD), o Brasil inaugura o denominado "sistema protetivo dos dados pessoais" (TEIXEIRA; ARMELIN, 2020, p. 11-12).

A LGPD se aplica a todo tipo de tratamento de dados pessoais, seja por meio biométrico, digital, eletrônico ou físico, por pessoa natural ou por pessoa jurídica de direito

[3] Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico. Com a vigência da lei, muitos bancos de dados terão que ser revistos, pois grande parte deles concentra uma quantidade infindável de dados pessoais, e que, segundo a lei, assim que atinjam sua finalidade deverão ser eliminados, o que na prática poderá ser bem complexo. É de se prever que quanto maior o banco de dados e mais completa a sua gama de informações, maior impacto terá caso algum incidente venha a ocorrer.

público ou privado. Faz-se a ressalva de que a lei não se aplica a tratamento de dados que sejam realizados por pessoa natural para fins particulares e não econômicos, ou fins jornalísticos, artísticos, acadêmicos, de segurança pública, de defesa nacional, de segurança do estado e de atividades de investigação e repressão de infrações penais, entre outras. Ainda assim é recomendado o cuidado com a proteção dos dados para que, independentemente de a lei não cobrir esses casos, continuem mesmo assim sendo preservados os direitos de intimidade e privacidade de terceiros (TEIXEIRA; LOPES; TAKADA, 2020, p. 281-282). Aos dados originados e destinados a outros países, que apenas passam pelo território nacional não será aplicável a lei brasileira, desde que o país de proveniência proporcione grau de proteção de dados semelhante ao da LGPD, o que será avaliado pela Autoridade Nacional de Proteção de Dados (ANPD)[4] (TEIXEIRA; ARMELIN, 2020, p. 41).

Cumpre esclarecer, ainda, que a LGPD estabelece um dever de adoção de medidas de proteção a partir da criação de qualquer nova tecnologia ou produto (*privacy by design*)[5]. Neste caso, vazamentos de dados e incidentes de segurança devem ser notificados à autoridade de proteção de dados e, em alguns casos, aos titulares afetados (PALHARES, et al., 2020, p. 138). Ambos são indispensáveis aos sistemas de tratamento de dados, já que os mesmos deverão ser estruturados visando proporcionar a segurança adequada desde a sua estruturação, chamada de *security by design* (TEIXEIRA; ARMELIN, 2020, p. 134-139).

Além disso, o *compliance* [6], as boas práticas de governança, o gerenciamento de riscos, o plano emergencial para incidente de vazamento de dados e de forma especial o mapeamento de dados, são indispensáveis para a garantia da segurança e a proteção das informações, e são algumas das mais variadas técnicas de adequação à LGPD (TEIXEIRA, 2021, p. 53).

Assim, muitas instituições já adotaram tecnologias de segurança para as informações coletadas de seus usuários, sendo que com a vigência da LGPD deverão providenciar que essa segurança seja capaz de proteger os dados pessoais de qualquer pessoa, mesmo após o

[4] Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional

[5] O termo *privacy by design* refere-se à metodologia que visa proteger a privacidade do usuário desde a concepção de quaisquer sistemas de tecnologia da informação ou de práticas de negócio que sejam concernentes ao ser humano. Logo, a proteção de privacidade seria o ponto de partida para o desenvolvimento de qualquer projeto, sendo incorporada à própria arquitetura técnica dos produtos ou serviços.

[6] A expressão “compliance” tem origem na língua inglesa, a partir do verbo “to comply” que expressa a ideia de cumprir, satisfazer, executar. A ideia central é, portanto, cumprir ou satisfazer as determinações jurídicas impostas pelo ordenamento, assim como as normas internas daquela organização. O objetivo do compliance é assegurar que a corporação esteja aderente às normas vigentes, fazendo com que riscos sejam afastados ou mitigados. Acredita-se que uma empresa comprometida com a cultura do compliance estará menos exposta a riscos e assim terá um ambiente corporativo impróprio para o surgimento de condutas irregulares ou ilícitas.

término de seu tratamento. Agora, caso ocorra algum 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 terceiro não autorizado acessá-los (TEIXEIRA; ARMELIN, 2020, p.136).

Cabe destacar, também, que a LGPD não detém a exclusividade no tratamento do tema da proteção de dados pessoais, sendo o mesmo igualmente inserido em outros diplomas legais. O que singulariza a regulação presente na lei é a sua abrangência, com a anuência de princípios, direitos, responsabilidades e demais aplicações decorrentes do tratamento de dados pessoais[7] (FRAZÃO; TEPENDINO; OLIVA, 2020, p.416).

Pois bem, a LGPD (Lei nº 13.709/2018) entrou em vigor no dia 18 de setembro de 2020, com o envolvimento de diversos atores e setores da sociedade civil, criando novos desafios a serem enfrentados para cumprir com os requisitos previstos na lei, na concepção e na oferta de produtos e serviços ao consumidor, incluindo, por exemplo, a análise e concessão de crédito (PALHARES, et al., 2020, p. 133). No entanto, suas sanções (multas e penalidades por descumprimento) somente serão aplicadas a partir de agosto de 2021 (KREMER, 2020).

Isto posto, no conceito de dado pessoal, se incluem até aquelas informações que não se prestam a identificar a pessoa quando usadas isoladamente (IP, faixa etária, altura, etc.), mas que poderão fazê-lo se conjugadas com outros dados, são, portanto, identificáveis (FRAZÃO; TEPENDINO; OLIVA, 2020, p. 159). Além disso, todo o dado pessoal é privativo. Assim, para que se torne público seria necessário que o dado fosse publicamente tratado.

Como se vê, a LGPD tem como objetivo regular os "dados pessoais". Ficam fora do escopo dessa lei, portanto, os dados relacionados a pessoas jurídicas. Qualquer informação que possa ser relacionada a um indivíduo, já identificado ou passível de identificação, pode ser considerada como um dado pessoal. Assim, informações de cadastro, perfil comportamental, econômico e/ou social se enquadram no conceito de dado pessoal. Por outro lado, as informações que não permitem a identificação (imediata ou posterior) de um único indivíduo, podem se enquadrar no conceito de "dado anonimizado"[8]. Trata-se, por exemplo,

[7] 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. Em suma, resume toda e qualquer operação com dados pessoais, não se limitando aos exemplos pontuados pela lei, qualquer atividade que for realizada com dados pessoais será alcançada pelas determinações legais.

[8] Dado relativo à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Frise-se que dados anônimos não são dados pessoais e, portanto, não são tutelados pela lei. São aqueles que a sua reidentificação é impossível por qualquer parte e por quaisquer meios razoavelmente possíveis. De outra sorte, esses dados são aqueles que através de técnicas, como a criptografia, não possam ser levados a identificar uma pessoa. Insta frisar que se o dado, mesmo criptografado,

de informação sobre dados estatísticos e cujo processo de anonimização[9] seja irreversível revelam apenas uma informação de caráter coletivo e, por isso, não estão sujeitos ao regime de proteção de dados da LGPD, sendo seu uso livre.

A LGPD não foi criada para limitar a atuação das empresas gestoras de dados e sim para promover a inovação, bem como a expansão segura dessas atividades, tendo por missão a proteção e promoção dos direitos fundamentais, essenciais para efetiva tutela dos dados privados de seus cidadãos, de suas instituições e corporações privadas (TEIXEIRA, 2021, p. 53). Assim, o Brasil passa a integrar o grupo de mais de 120 países que têm uma legislação de proteção de dados semelhante ao modelo europeu (GDPR) (CIAB FEBRABAN, 2020).

2.1.1 Princípios

Os princípios, também conhecidos como *Fair Information Privacy Principles* – FIPPs que, da perspectiva da OCDE e, como consequência, de várias legislações voltadas à proteção de dados pessoais, se propõe a preservar o adequado tratamento de dados pessoais. Compreendê-los, equivale a compreender os fundamentos de um regime geral de proteção de dados pessoais (CARVALHO; ALVIM, et al., 2019, p. 504-505). É indispensável a aplicação de princípios, que norteiam a aplicação da lei, pois serão capazes de atingir eventos futuros, como novas tecnologias e distintas realidades (TEIXEIRA; ARMELIN, 2020, p. 49).

Dito isso, verifica-se, que os princípios estabelecidos pela LGPD, elencados em seu artigo 6, estabelecem um dever de transparência. Entre outras hipóteses, o tratamento de dados pessoais é autorizado com o consentimento do titular dos dados, para fins de cumprimento de obrigação legal ou regulatória, quando necessário para execução de contrato, para atender interesses legítimos do controlador dos dados ou terceiros e para fins de proteção ao crédito (PALHARES, et al., 2020, p.134-135).

Além disso, os princípios da segurança, da prevenção e da responsabilidade, ou prestação de contas, também são bastante próximos. O primeiro visa evitar situações ilícitas, e o segundo pretende evitar o dano à pessoa por causa do tratamento inadequado dos dados pessoais. Não obstante, o ilícito e o dano são conceitos clássicos da responsabilidade civil.

---

por exemplo, for identificado através de meios razoáveis e disponíveis à época do tratamento, possibilitando-se a sua reidentificação, ele estará sobre a tutela da lei, é o que se chama de pseudonimização do dado.

[9] 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. A anonimização deve levar em conta as técnicas razoáveis e disponíveis adotadas no momento do tratamento, ou seja, por mais que surjam técnicas melhores posteriormente, será considerada aquela à época do tratamento, posto que a tecnologia avança exponencialmente com o tempo, não sendo possível prever o que será razoável futuramente.

Com efeito, não é espantoso que a concretização desses princípios na lei ocorra, muitas vezes, por um mesmo dispositivo (FRAZÃO; TEPENDINO; OLIVA, 2020, p. 76).

Os princípios da LGPD são princípios do sistema brasileiro de proteção de dados e que a nova lei não supera às anteriores. Ao contrário, se inspira e, portanto, se integra às predecessoras, de proteção de dados no Brasil (FRAZÃO; TEPENDINO; OLIVA, 2020, p.81). Por sua vez, a violação desses princípios, notadamente o da finalidade, há de ser aferida diante do valor da privacidade, a qual, a seu turno, encontra-se naturalmente funcionalizada à dignidade da pessoa humana (FRAZÃO; TEPENDINO; OLIVA, 2020, p.260).

2.1.2 Bases legais de tratamento

De início, cabe mencionar que a Lei geral de Proteção de Dados apresenta, em seu artigo 7, um rol com dez hipóteses para o tratamento de dados pessoais. Todavia, esse trabalho não apresenta base legal segura e apta a embasar o tratamento de dados pessoais e dados pessoais sensíveis existentes em processos judiciais, sejam eles físicos ou digitais, pelo Poder Judiciário, de modo que a sua taxatividade deve ser flexibilizada para que se encontre, dentro da própria lei, alicerce legal, como aquele identificado no caput do art. 23[10]. Dessa forma, o caput do artigo 23 da LGPD deve ser considerado uma base legal autônoma àquelas descritas no artigo 7º da LGPD, e apta a embasar o tratamento de dados pessoais e dados sensíveis contidos nos processos judiciais (PALHARES, et al., 2020, p.317).

Ainda, assim, o tratamento de dados corresponde a "toda operação realizada com dados, 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" (art. 5º, inciso X). Além disso, o modelo de tratamento de dados instituídos pela LGPD se ampara nas seguintes características básicas: a ampliação do conceito de dado pessoal; o respeito à base legal; e o legitimo interesse como hipótese autorizativa e a necessidade de realização de um teste de balanceamento de interesses. E, segundo a LGPD, todo e qualquer tratamento de dados deve respeitar a base legal definida no art. 7º (FRAZÃO; TEPENDINO; OLIVA, 2020, p.158-159).

Por isso, antes de qualquer coisa, a realização do tratamento de dados deve ocorrer para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de

[10] 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.

tratamento posterior de forma incompatível com essas finalidades; de forma compatível ou adequada com as finalidades informadas ao titular, de acordo com o contexto do tratamento; e ainda no limite do 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. Utiliza-se do princípio da proporcionalidade, ou seja, o tratamento dos dados é protegido na medida em que o meio é adequado e necessário para o fim almejado (FRAZÃO; TEPENDINO; OLIVA, 2020, p.220).

Contudo, o consentimento[11] é trazido por muitos como a hipótese principal para tratamento de dados, entretanto não há qualquer grau de hierarquia entre as dez hipóteses legais estabelecidas pela LGPD. Entretanto, continua a ter certa preferência sobre os demais, pois geralmente facilita a obrigação do agente de tratamento em demonstrar que o tratamento foi feito dentro de uma hipótese legal, ante o princípio da *accountability*[12] (prestação de contas ou responsabilidade demonstrável).

Insta, ainda, ressaltar que o consentimento autoriza tão somente o agente que o obteve, não se estendendo a outras pessoas para quem possa compartilhar os dados, devendo, para esse caso, obter o consentimento especifico do titular (TEIXEIRA; ARMELIN, 2020, p.55-56). Faz parte do processo de consentimento dar, também, a indicação a respeito das circunstâncias e para quais finalidades o processamento se dará. Destaque-se que a observância ao princípio da finalidade (*purpose limitation*) é fulcral para efetividade do consentimento. Como regra geral, cada consentimento deve corresponder a uma finalidade específica (CARVALHO; ALVIM, et al., 2019, p.506).

[11] Para os fins da LGPD, considera-se consentimento a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (LGPD, art. 5º, inciso XII). Significa dizer que o consentimento desvinculado da finalidade ou tempo para o qual foi dado não é consentimento e, portanto, não merece proteção. Vale pontuar que o consentimento do titular para tratamento de seus dados pessoais sensíveis além de ser livre, inequívoco e informado, também deverá ser específico e de forma destacada, diferindo-se do consentimento de dados pessoais que não são sensíveis.

[12] A exigência de que as empresas e o governo (quando no papel de controlador de dados pessoais) assumam papel central e maiores responsabilidades no processo de tratamento de dados pessoais. Trata-se de mais um meio de legitimação, pelo qual se presume e exige que as instituições que pretendam controlar dados pessoais se responsabilizem, de forma demonstrável (ao regulador), pela utilização e processamento adequados, justos e éticos dos dados pessoais. Logo, não retira do indivíduo o direito de fazer valer seu direito ao controle dos dados que a ele digam respeito. O que o *accountability* propõe é tirar do indivíduo a responsabilidade primária pela proteção de seus dados pessoais e repassá-la à organização que coleta e faz uso dos dados em seu próprio benefício. Pelo conceito de *accountability*, uma organização responsável transparece comprometimento com sua responsabilidade, implementa políticas de privacidade de dados ligadas a critérios externos reconhecidos e estabelece mecanismos de desempenho para garantir tomadas de decisões responsáveis sobre o gerenciamento de dados que estejam de acordo com as políticas da organização.

Não se deve perder de vista, portanto, que o cumprimento de obrigação legal ou regulatória consiste no controlador[13] poder tratar dados pessoais, mesmo sem o consentimento do titular, quando tiver que cumprir alguma determinação legal ou regulamentação. Por outro lado, o inciso III, do artigo 7º, possibilita que a "Administração Pública trate dados, mas delimita esse tratamento a utilização do mesmo para consecução de políticas públicas previstas em lei ou regulamentos" (TEIXEIRA; ARMELIN, 2020, p.56-57).

Outra questão diz respeito ao tratamento de fatos pretéritos que envolvem o indivíduo e na possibilidade de não serem objeto de eterna divulgação pública quando não há interesse legítimo para tal permanência.

A eliminação dos dados pessoais, por manifestação de vontade do titular, independe de qualquer motivação, eis que a revogação do consentimento retira a legitimidade do tratamento dos dados. Além disso, uma vez que o término do tratamento de dados não é seguido da sua eliminação[14], há de se verificar a repercussão na seara da responsabilidade civil (FRAZÃO; TEPENDINO; OLIVA, 2020, p.229-234).

2.1.3 Direitos dos titulares de dados

O conceito de titularidade exprime não apenas a ideia de poder de controle sobre um bem jurídico, mas, também e consequentemente, o sentido de atribuição do mesmo, com regras claras disponíveis acerca de seus modos de utilização e disposição. Logo, a opção legislativa, manifestada no *caput* art. 17 da LGPD, de tratar a pessoa física a quem os dados se vinculam como seu titular, implica que o exercício do direito ali descrito se dará de modo direto e imediato sobre o bem jurídico em questão, inexistindo intervenção de qualquer outra pessoa sobre o vínculo (FRAZÃO; TEPENDINO; OLIVA, 2020, p.145-149).

Vale esclarecer que a LGPD, embora tenha essa nomenclatura, visa proteger o titular dos dados e não os dados pessoais *per se.* Isso pois, mesmo que os dados pessoais de qualquer indivíduo possam estar espalhados em milhares de bancos de dados pelo mundo, qualquer tratamento deverá obedecer às normas legais, sendo que o seu titular possui direito sobre seus dados inerentes à sua personalidade. Contudo, a ordem prática de todos esses direitos demandará tempo e investimento por parte dos controladores, já que engloba o fornecimento

[13] Controlador pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
[14] Exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

dos dados que são tratados, como também quem tratou, a possibilidade de corrigi-los, eliminá-los, bloqueá-los e a sua portabilidade (TEIXEIRA; ARMELIN, 2020, p.85-88).

Cabe destacar, ainda, que o controlador deverá, em atendimento ao inciso VII, do artigo 18, possuir lista atualizada de quem são as entidades públicas e privadas com os quais compartilha os dados pessoais do titular, por ser seu direito solicitá-la a qualquer tempo (TEIXEIRA; ARMELIN, 2020, p.89-90).

Há também que se falar que os dados pessoais informados pelo titular em um boletim de ocorrência ou processo judicial, por exemplo, não podem ser utilizados para prejudica-lo, uma vez que os mesmos foram informados ou se tornaram públicos visando exercício regular de um direito, como o de ação ou de defesa. No mais, é importante esclarecer que a lei possibilita ao titular dos dados que sua tutela em juízo seja individual, seja coletiva, quando sentirem que seus direitos estão sob ameaça (TEIXEIRA; ARMELIN, 2020, p.94-95).

Dessa forma, esse assunto é de vital importância, pois revela ao indivíduo a titularidade de seus dados pessoais que integram sua personalidade, que deverão estar sob o "manto" da liberdade, privacidade e intimidade (TEIXEIRA; ARMELIN, 2020, p.86).

2.1.4 Sanções e multas propostas

A violação das exigências impostas pela LGPD pode ter um custo alto, tanto monetário como na reputação das instituições, o que para muitas pode ser irrecuperável. Assim, em caso de descumprimento da lei, as penalidades incluem advertência, obrigação de divulgação do incidente, eliminação ou bloqueio de dados pessoais, multa de até 2% (dois por cento) do faturamento anual da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil, no seu último exercício, excluídos os tributos, limitada, no total, de R$ 50.0000.000,00 (cinquenta milhões de reais) por infração cometida, e suspensão ou proibição das atividades de tratamento ou funcionamento do banco de dados (PALHARES, et al., 2020, p.137).

Dessa forma, poderá ser imposto ao controlador o bloqueio ou até mesmo a eliminação do banco de dados do infrator dos dados pessoais relativos à infração, o que a depender do tipo de atividade da instituição poderá levá-la ao encerramento de suas atividades.

Os órgãos públicos, não estarão sujeitos às multas estipuladas, entretanto sujeitar-se-ão às demais penalidades, sem prejuízo das demais leis pertinentes (servidor público, acesso à informação e improbidade administrativa) (TEIXEIRA; ARMELIN, 2020, p.146-147)

Portanto, enquanto entidades responsáveis por determinar como os dados pessoais são utilizados, passarão a ter obrigações adicionais relativas ao tratamento desses dados, como a necessidade de indicar um *Data Protection Officer* (DPO), pessoa encarregada de atuar na

comunicação entre a organização e os titulares dos dados e a ANPD (PALHARES, et al., 2020, p.136. Ainda, assim, precisam investir bastante na capacitação de seus profissionais, juntamente com soluções tecnológicas e a revisão de seus contratos (PINHEIRO, 2020a).

2.1.5 Quem é o DPO e qual o seu papel?

Embora o legislador nacional tenha copiado do GDPR a figura do *Data Protection Officer* (DPO; em português, Oficial de Proteção de Dados), optou por denominá-lo simplesmente de "encarregado", previsto nos artigos 5º e 41, da Lei. Isso pode ser objeto de regulamentação pela ANPD, que fará essa análise de quais instituições deverão ter necessariamente um DPO/encarregado (BLUM, 2020), mas – até o presente momento – a legislação não limitou a sua obrigatoriedade a qualquer tipo de responsável pelo tratamento de dados, atribuindo – de acordo com a lei – a toda e qualquer pessoa física ou jurídica, que trate dados pessoais, a obrigatoriedade de se indicar um encarregado pelo tratamento desses dados (TEIXEIRA; ARMELIN, 2020, p.123).

Pois bem, o DPO, é a 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), nos termos do art. 5º, inciso VIII, da LGPD.

Além disso, para o cargo de DPO, é importante que haja a observância ao princípio de *accountability* (prestação de contas), responsabilização e prestação de contas, previsto no artigo 6º, inciso X da LGPD, correspondendo à obrigatoriedade de demonstração de medidas eficazes e cumprimento das normas de proteção de dados, como geração de evidências em forma de relatórios de impacto[15], geração de indicadores de incidentes, treinamento dos colaboradores, e outros sobre a conformidade com a LGPD (BLUM, 2020), já que a lei é inteiramente baseada no respeito aos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Cabe ainda ao DPO garantir a implementação das políticas internas criadas e a sua adaptação aos novos produtos e necessidades que forem surgindo com o decorrer do tempo. A conformidade com a legislação de proteção de dados não é estática, e a instituição deve estar atenta para já prever a adequação de novos produtos, áreas ou negócios (BLUM, 2020).

[15] 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. Logo, é uma obrigação que todo o controlador deverá cumprir. Esse relatório é a prestação de contas. Não basta o controlador cumprir a lei, ele deverá gerar a todo tempo evidências de que está cumprindo a lei. Neste relatório o controlador deverá demonstrar todo o tratamento da dados feitos, bem como os riscos a ele inerentes e medidas, salvaguardas e mitigações de risco.

Há que se esclarecer, também, que a responsabilização do encarregado por eventuais desconformidades da instituição não deverá ocorrer. Salvo em casos pontuais em que fique demonstrado o dolo na sua atuação. Nos demais, a responsabilização caberá ao controlador e ao operador dos dados pessoais (BLUM, 2020).

2.1.6 Autoridade Nacional de Proteção de Dados (ANPD)

Logo depois de o Senado aprovar o Projeto de Lei de Conversão (PLV) 34/20, o presidente da república assinou o decreto que cria a Autoridade Nacional de Proteção de Dados (ANPD). Assim, vale destacar que a ANPD, por definição, é o órgão da administração pública responsável por zelar e implementar a lei de proteção de dados em todo o território nacional, garantindo o cumprimento e o melhor proveito da regulamentação, seja por meio de normas complementares, pareceres técnicos e procedimentos de inspeção. Portanto, a ANPD, tem o objetivo de proteger os direitos fundamentais de liberdade e privacidade, orientar, promover e fiscalizar o cumprimento da LGPD, além de aplicar sanções administrativas em casos de violação no tratamento de dados (PINHEIRO, 2020a).

Cumpre esclarecer, ainda, que a ANPD, após muito debate, foi criada como sendo uma autoridade de natureza jurídica transitória, ou seja, em um primeiro momento ela será um órgão da administração pública federal, submetida a um regime autárquico especial e vinculada à Presidência da República. O principal questionamento que foi trazido à tona durante o trâmite da MP nº 869/2018, que originou a lei nº 13.853/2019[16], foi sobre a indispensável autonomia da autoridade, sendo mister sua desvinculação com outros órgãos a fim de garantir a adequada segurança jurídica de suas decisões (TEIXEIRA; ARMELIN, 2020, p.150-151). Justamente por isso o ideal seria ter um órgão independente, com meios de alcançar eficiência e sustentabilidade (PINHEIRO, 2020a).

Desse modo, infelizmente, não há como escapar do clichê de necessidade de uma regulamentação especifica pela ANPD sobre assuntos que necessitam de uma atenção especial sem que se trave o avanço tecnológico e a inovação, de forma a não prejudicar o mercado, mas a definir formas de se continuar desenvolvendo tecnologias e, ao mesmo tempo, respeitando os direitos fundamentais dos titulares (PALHARES, et al., 2020, p.94).

Assim sendo, uma vez criada a autoridade nacional será a responsável por zelar para que o tratamento de dados realizados pelo poder Público esteja em conformidade com a lei e, caso entenda necessário, estipular outros requisitos ou adequações para que esse tratamento

[16] Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências.

esteja dentro dos parâmetros legais. Daí a importância de a autoridade nacional ser um órgão independente, autônomo e altamente especializado, visto que a lei afeta todos os setores do país, tanto público quanto privado e considerando a sua importância na fiscalização do próprio poder Público (TEIXEIRA; ARMELIN, 2020, p.105).

2.1.7 *Open Banking* (Sistema Financeiro Aberto) e a "nova" Lei do Cadastro Positivo

O *Open Banking* (Sistema Financeiro Aberto) e a "nova" Lei do Cadastro Positivo, aos poucos, estão revolucionando o Sistema Financeiro Nacional, ampliando as possibilidades de acesso aos dados pessoais, mas com cautela e sustentabilidade, atendendo princípios de segurança e privacidade de dados cada vez mais cobrados e exigidos pela sociedade.

Primeiramente, o Open Banking pode ser definido como um modelo colaborativo no qual os dados bancários são compartilhados por meio de interface de programação de aplicativo (API), um conduíte inteligente que permite o fluxo de dados entre sistemas de maneira controlada, mas contínua, entre duas ou mais partes não afiliadas para fornecer recursos aprimorados ao mercado. As APIs têm sido usadas há décadas, mas estão recebendo atenção renovada como um meio de aprimorar a entrega de serviços financeiros. Até agora, entretanto, essas conexões têm sido usadas principalmente para compartilhar informações, em vez de transferir saldos monetários (BRODSKY; OAKES, 2017).

Recentemente, o Banco Central do Brasil publicou a Circular nº 4.015 e, em conjunto com o CMN, a resolução nº 1, ambas de 4 de maio de 2020 ("Resolução Conjunta"), que regulamentam como será implementado o Open Banking no Brasil. A Circular nº 4.015, ainda, regulamenta e padroniza quais dados estão sujeitos aos sistemas e quais devem ser disponibilizados para compartilhamento. A Resolução Conjunta estabelece que os dados pessoais de clientes somente poderão ser compartilhados com terceiros mediante o consentimento do cliente, como a manifestação livre, informada, prévia e inequívoca de vontade, feita por meio eletrônico, pela qual o cliente concorda com o compartilhamento de dados ou serviços para finalidades determinadas. Assim diferentemente do que dispõe a LGPD, autorizando o tratamento (e, portanto, o compartilhamento) de dados pessoais em outras bases legais com o consentimento do titular, a portabilidade ou compartilhamento de dados dentro do sistema *Open Banking* dependerá sempre do consentimento do titular dos dados. Ainda, de acordo com a Resolução, o consentimento, os registros de acesso e revogação do consentimento devem ser armazenados pelo prazo mínimo de 5 (cinco) anos (art. 49 da Resolução Conjunta). Além do consentimento, antes de concluir o compartilhamento de dados, as instituições deverão observar as etapas de autenticação (do

titular ou da instituição solicitante dos dados, conforme aplicável) e confirmar a operação. De modo similar a LGPD e a resolução CMN 4.658/2018, a Resolução Conjunta também determina a obrigatoriedade das instituições participantes de nomear um Diretor Responsável pelo compartilhamento (art. 32 da Resolução), responsável por produzir semestralmente relatório de compartilhamento (nas datas-bases de 30 de junho e 31 de dezembro). Tal relatório deve ser submetido ao conselho de administração ou, na sua inexistência, à diretoria da instituição até noventa dias após a respectiva data-base. Por fim, a Resolução Conjunta permitirá o compartilhamento de dados entre instituições financeiras e seus parceiros de negócio não regulados (artigo 36 da resolução), desde que obtido o consentimento do titular, adotadas medidas organizacionais e condições contratuais específicas, conforme estabelecido na Resolução (PALHARES, et al., 2020, p.145-150).

No entanto, existe um direito à privacidade para o pagador/beneficiário correspondente? Nesse caso, o processo de consentimento torna-se mais complexo – particularmente quanto as partes do banco de transações com instituições diferentes e não há um repositório central de permissões concedidas (BRODSKY; OAKES, 2017).

Outra questão, ainda, refere-se à base legal de "proteção ao crédito", não é certa qual a sua amplitude, isto é, em quais hipóteses a base legal de tratamento para fins de proteção ao crédito poderá ser utilizada, mas esta certamente será de grande valia para as instituições do setor financeiro, especialmente nos casos em que o consentimento não puder ser obtido e outra base legal não puder ser utilizada. Tal base legal também deveria permitir operações de tratamento de dados para fins de realizar a cobrança e negativação de inadimplentes, ainda que em caráter extrajudicial ou anterior à fase litigiosa (PALHARES, et al., 2020, p.135).

Vale saber, contudo, que a proteção ao crédito também autoriza o tratamento de dados garantindo-se o crescimento da economia como um todo e a preservação da sociedade, precedendo o interesse individual do titular, que está inadimplente ou que é um mau pagador. Essa hipótese engloba ainda o tratamento de dados pessoais para compor o *score* (pontuação) do indivíduo e para preservação antifraude a ser adotada pelo agente de tratamento. Assim sendo, não poderá, por exemplo, o titular solicitar a exclusão de seus dados pessoais dos cadastros de restrição ao crédito ou mesmo se negar a fornecer dados pessoais para pleitear financiamento em uma instituição financeira. É de se lembrar que a proteção ao crédito também é vislumbrada na Lei do Cadastro Positivo (Lei 12.414/2011), que disciplina a formação e consulta a banco de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito, conforme abordaremos mais adiante (TEIXEIRA; ARMELIN, 2020, p.59-60).

Quanto a portabilidade, direito relevante no sistema bancário aberto (*Open Banking*), que tem como um de seus objetivos permitir a portabilidade de informações entre diversos *stakeholders* do mercado financeiro (PALHARES, et al., 2020, p.136).

Por outro lado, diferentes categorias de dados garantem diferentes níveis de segurança, e o consentimento informado requer a compreensão das implicações do compartilhamento antes da aprovação – uma proeza nada pequena quando o clique reflexivo de "Concordo" em um conjunto de termos e condições não lido é padrão (BRODSKY; OAKES, 2017).

Assim sendo, as instituições financeiras devem fornecer ao titular dos dados, as suas respectivas políticas de privacidade (PALHARES, et al., 2020, p.135-136).

Por fim, algumas premissas basilares do *Open Banking*: (1) dados têm valor, principalmente na sociedade contemporânea; (2) em linha com a LGPD, o consumidor é titular de seus próprios dados e, por isso, detém o poder de decisão quanto ao que ocorre com eles; (3) dados referentes a operações financeiras de consumidores são privados e sigilosos, nos termos da Lei do Sigilo Bancário; (4) possuir dados sigilosos significa, além de responsabilidade, uma enorme oportunidade de entender o perfil dos consumidores e poder ofertar produtos e serviços com base em padrões identificados; e (5) o setor financeiro sempre foi severamente regulado e restrito, o que determinou a concentração desse mercado por poucas e grandes instituições financeiras que por muito tempo foram as únicas a terem acesso aos dados bancários dos consumidores (HORTA, 2019).

Cabe mencionar, também, o cadastro positivo, que visa beneficiar aqueles que possuem histórico de "bom pagador" (EROLES, 2019, p.207). Originalmente criado no Brasil em 2011, com a Lei do Cadastro Positivo (Lei 12.414/2011), a inclusão de indivíduos nesse banco de dados exigia o consentimento do consumidor. A necessidade de obtenção do consentimento implicou baixa taxa de adesão por parte dos consumidores. Com as alterações recentes, a inclusão de consumidores no cadastro passa a ser automática e tais indivíduos serão notificados por prazo de 30 dias a partir da criação de seu perfil, ampliando a relevância dessa base de dados para o Sistema Financeiro Nacional e o *Open Banking* (Circular nº 4.015 de 04/05/2020 do BACEN, em conjunto com CMN, Resolução Conjunta nº 1/2020), que tem como fundamento central a facilitação do compartilhamento e acesso aos dados pessoais. Dessa forma, se verifica uma evolução significativa nas normas que visam regulamentar o uso e proteger informações e dados pessoais contra divulgação não autorizada, de usuários de serviços financeiros, no Brasil (PALHARES, et al., 2020, p. 129).

Porém, apesar do registro automático, o indivíduo terá o direito de optar por não participar do cadastro, a qualquer momento, por meio eletrônico. Ainda, assim, a nova Lei do

Cadastro Positivo[17] proíbe o uso de informações consideradas excessivas (ou seja, aquelas que não estão vinculadas à análise de risco de crédito do consumidor) ou o tratamento de dados sensíveis (ou seja, informações que revelem origem étnica e social, saúde, informações genéticas, orientação sexual e crenças políticas, religiosas e filosóficas) para formar o histórico e/ou o *score* de crédito (*credit score*), nota de pontuação de crédito que indica o comportamento financeiro do consumidor, principalmente se as bases não foram construídas atendendo à LGPD. Por isso, se faz necessário atualizar a redação da ficha cadastral da oferta do crédito (aviso prévio sobre tratamento), bem como inserir aviso na própria CCB (Cédula de Crédito Bancário)[18], chamados de "*privacy notices*" (BXBLUE, 2020; PINHEIRO, 2020a).

Além disso, as informações tratadas no cadastro positivo devem ser consideradas confidenciais entre os gestores do banco de dados e a divulgação não autorizada implicará violação do sigilo bancário. Por fim, além das regras especificas do cadastro positivo, os princípios e obrigações estabelecidas na LGPD também devem ser observados na utilização de dados pessoais advindos dessa base de dados (PALHARES, et al., 2020, p.142-144).

No que tange ao setor financeiro, as regras de tratamento de dados pessoais, tem como principais marcos regulatórios: Lei de Sigilo Bancário (Lei Complementar nº 105/2001); Resolução 2.025/1993 (contas de depósitos); Circular 3.461/2009 (combate à lavagem de dinheiro); Resolução 4.539/2016 (relacionamento com clientes e usuários de produtos e serviços financeiros); Resolução 4.557/2017 (gerenciamento contínuo de riscos); Resolução 4.658/2018 (segurança cibernética e *cloud computing*) (LEONARDI, 2019, p.48), além da Circular nº 3.909/2018 (trouxe a obrigação de implementação de uma política de segurança cibernética por parte das instituições de pagamento).

É necessário buscar um equilíbrio entre o direito à privacidade e o desenvolvimento de produtos e serviços, que ganha enorme propulsão com a digitalização dos serviços bancários, alinhado com a crescente capacidade de processamento de dados pelas *fintechs,* instituições financeiras e outros *players* do mercado financeiro (PALHARES, et al., 2020, p. 134-150).

Assim sendo, o STJ passou a examinar questões atinentes ao cadastro positivo de crédito, visto que, além do direito de acesso e do direito à correção da informação, já previstos no CDC, incluiu, expressamente, entre os direitos do cadastrado: (i) o direito de obter o

[17] A Lei Complementar nº 166, com início de vigência de julho de 2019, regulamentada pelo Decreto nº 9.936/2019, altera substancialmente a Lei 12.414/11, conhecida como Lei do Cadastro Positivo. Mais da metade da norma foi modificada: é possível falar, assim, na existência de uma Nova Lei do Cadastro Positivo.

[18] Título de crédito emitido de forma escrita por pessoa física ou jurídica, em favor de uma instituição financeira. Foi criada através da MP 1.925/99 e incluída na Lei nº 10.931/04. Representa uma promessa de pagamento, em dinheiro, que é decorrente de uma operação de crédito. Assim, toda vez que alguém contrata um empréstimo (independente da modalidade) com uma instituição financeira deve assinar a CCB, declarando ciência do crédito e do pagamento. O documento tem, portanto, a mesma validade de um contrato.

cancelamento do cadastro; (ii) o direito de conhecer os principais elementos e critérios considerados para a análise de risco; (iii) o direito de ser informado previamente sobre o armazenamento, a identidade do gestor do banco de dados, o objetivo do tratamento dos dados pessoais e os destinatários dos dados em caso de compartilhamento; (iv) o direito de solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados; (v) o direito de ter os seus dados pessoais utilizados de acordo com a finalidade para qual foram coletados (FRAZÃO; TEPENDINO; OLIVA, 2020, p.87).

A rigor, o novo cadastro tende a tornar o acesso ao crédito mais fácil e com juros menores para consumidores e empresas que honram seus compromissos financeiros. O bom pagador terá um *score* (nota de pontuação de crédito que indica o comportamento financeiro do consumidor) mais alto e essa pontuação poderá ser considerada pelas instituições financeiras em eventuais concessões de crédito, conforme o Banco Central. A expectativa é que outros segmentos comecem a fornecer informações de pagamentos dos clientes.

Em síntese, o governo elaborou o Projeto de Lei Complementar 441/2017, que deu origem à Lei Complementar 166/2019, que altera a Lei 12.414/11. O Projeto alterou o modelo de inclusão dos consumidores no sistema de cadastro positivo, com o intuito de ampliar a base de dados de "bons pagadores". Para que as alterações feitas na LCP fossem levadas a cabo, o Poder Executivo editou novo Decreto regulamentador (Decreto nº 9.936, 24 de julho de 2019), estabelecendo diretrizes para a constituição dos gestores de banco de dados, a disponibilização de histórico de crédito, as hipóteses de vazamentos de dados, etc. Ademais, o BACEN, em 29 de julho de 2019, editou a Resolução nº 4.737/19 e a Circular nº 3.955/19 para impor normas de registro dos gestores de banco de dados junto ao BACEN para o recebimento de informações de adimplemento das instituições financeiras, bem como da forma de fornecimento destas informações. Por exemplo, há previsão de que não constitui quebra do dever de sigilo bancário o compartilhamento, por parte de instituições financeiras e demais autorizadas pelo Banco Central do Brasil ("BACEN"), de dados de adimplemento aos gestores de bancos de dados cadastrados junto ao BACEN (MORIBE; SILVA, 2020).

3 CONCLUSÕES

Percebe-se, que ao estar de acordo com as novas normas do Open Banking, a instituição também, tem que estar pronta para atender a LGPD. Como a resolução do

Bacen estabelece que o compartilhamento é legitimado pelo consentimento[19], deve haver a harmonização com a LGPD, aplicando-se os demais direitos do titular previstos em lei. Assim, a instituição doadora dos dados permanece na posição de controladora e responsável pela proteção dos dados pessoais dos seus clientes sob as diretrizes da LGPD.

De fato, o Open Banking se baseia em uma premissa básica: os dados de transações, histórico financeiro e informações gerais de um indivíduo são de propriedade dele e não da instituição financeira. O cliente tem o poder de escolha em relação ao que deseja fazer com esses dados, podendo, por exemplo, compartilhá-los com provedores de serviços financeiros de sua escolha. Esse terceiro, provedor de serviços financeiros, poderia utilizar os dados desse cliente para ofertar novos produtos e serviços financeiros inovadores e adaptados às necessidades do mesmo. Contudo, é necessário desenvolver padrões para o compartilhamento de dados bancários de forma fácil e segura entre as instituições participantes do mercado financeiro. Essa conexão e troca de informações se daria através de interfaces de programação de aplicações (APIs), conforme visto anteriormente. As "APIs abertas" permitiriam que terceiros, desde que autorizados pelos clientes, acessassem informações importantes sobre produtos bancários, sendo elas taxas de juros, termos, condições de operações e dados de contas de clientes, como histórico de transações e saldos de contas.

Por isso, a padronização é a chave para um sistema de Open Banking dar certo. Isso porque o tráfego de dados por APIs traz consigo uma série de novos riscos, e demanda uma política de privacidade e segurança bem estabelecida, para mitigar vulnerabilidades e delimitar responsabilidades dos *players* que operam dentro desse fluxo de informações. Destaque para algumas questões: (i) como limitar a responsabilidade, principalmente considerando um ambiente maior de interoperabilidade via APIs. Com especial atenção a situações em que não seja possível alcançar via contratos, principalmente devido a possíveis intepretações da Súmula 479 do Superior Tribunal de Justiça, emitida em junho de 2012, e que esclarece que "as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias"; (ii) o Art. 1.016 do Código Civil, que determina: "os administradores respondem solidariamente perante a sociedade e os terceiros prejudicados, por culpa no desempenho de suas funções". Diante do risco intersistêmico, como limitar a responsabilidade das instituições participantes? Em caso de vazamento, haverá responsabilização solidária?

[19] Deve ser solicitado de maneira clara, objetiva e adequada. Deve, ainda, especificar a finalidade do compartilhamento e o prazo de validade de acordo com a finalidade solicitada (máximo 12 meses). Ademais deve indicar quais dados serão compartilhados, mediante identificação do cliente.

Assim, a ausência de limitação de responsabilidade poderá prejudicar instituições que não incorrem no evento danoso (ex.: adoção de rito sumaríssimo nos Juizados Especiais Cíveis, não há dilação probatória).

4. REFERÊNCIAS

BANCO CENTRAL DO BRASIL. **Circular nº 3.909,** de 16 de agosto de 2018. Disponível em: < https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50645/Circ_3909_v1_O.pdf>. Acesso em: 15 out. 2020.

BANCO CENTRAL DO BRASIL. **Circular nº 3.955,** de 29 de julho de 2019. Disponível em: < https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50809/Circ_3955_v1_O.pdf>. Acesso em: 15 out. 2020.

BANCO CENTRAL DO BRASIL. **Circular nº 4.015,** de 04 de maio de 2020. Disponível em: < https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/51025/Circ_4015_v1_O.pdf>. Acesso em: 15 out. 2020.

BANCO CENTRAL DO BRASIL. **Resolução Conjunta nº 1,** de 04 de maio de 2020. Disponível em: < https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/51028/Res_Conj_0001_v1_O.pdf>. Acesso em: 15 out. 2020.

BANCO CENTRAL DO BRASIL. **Resolução nº 4.658,** de 26 de abril de 2018. Disponível em: < https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50581/Res_4658_v1_O.pdf>. Acesso em: 15 out. 2020.

BANCO CENTRAL DO BRASIL. **Resolução nº 4.737,** de 29 de julho de 2019. Disponível em: < https://www.pwc.com.br/pt/estudos/guia-demonstracoes-financeiras/2019/bacen-19-20.pdf>. Acesso em: 15 out. 2020.

BESSA, Leonardo Roscoe. **Nova Lei do Cadastro positivo** [livro eletrônico]: comentários à lei 12.414, com as alterações da lei complementar n. 166/2019 e de acordo com a LGPD. São Paulo: Thomson Reuters Brasil, 2019.

BLUM, Renato Opice. Data protection officer – quem é o nosso encarregado. **Revista CIAB - FEBRABAN.** 2020. Disponível em: < https://noomis.febraban.org.br/especialista/renato-opice-blum/data-protection-officer-quem-e-o-nosso-encarregado>. Acesso em: 19 out. 2020.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 05 mar. 2020.

BRASIL. **Decreto nº 9.936,** de 24 de julho de 2019. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9936.htm>. Acesso em: 15 out. 2020.

_____. **Lei Complementar Nº 105,** de 10 de janeiro de 2001. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm>. Acesso em: 07 jul. 2020.

_____. **Lei Complementar Nº 166,** de 08 de abril de 2019. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/lcp/Lcp166.htm>. Acesso em: 07 jul. 2020.

_____. **Lei 13.709/18,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 05 mar. 2020.

_____. **Lei Nº 13.853,** de 08 de julho de 2019. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm>. Acesso em: 07 jul. 2020.

_____. **Lei Nº 12.414,** de 9 de junho de 2011. Lei do Cadastro Positivo. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>. Acesso em: 07 jul. 2020.

_____. **Lei Nº 14.010,** de 10 de junho de 2020. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Lei/L14010.htm>. Acesso em: 07 jul. 2020.

BRODSKY, Laura; OAKES, Liz. Data sharing and open banking. **McKinsey & Company.** Disponível em: < https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking>. Acesso em: 19 out. 2020.

BXBLUE. **O que é Cédula de Crédito Bancário (CCB)?** Disponível em: < https://bxblue.com.br/aprenda/cedula-de-credito-bancario-ccb-consignado/>. Acesso em: 24 out. 2020.

CARVALHO, André Castro; ALVIM, Tiago Cripa et al. **Manual de *Compliance.*** Rio de janeiro: Forense, 2019. ISBN 978-85-309-8315-4.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law (EJJL**). Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: < https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315/658>. Acesso em: 19 out. 2020.

EROLES, Pedro. ***Fintechs*, Bancos Digitais e Meios de Pagamento:** aspectos regulatórios das novas tecnologias financeiras. São Paulo: Quartier Latin, 2019.

FRAZÃO, Ana; TEPENDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** 2.ed. São Paulo: Thomson Reuters Brasil, 2020.

HORTA, Luciana Simões Rebello. et al. **O que é Open Banking?** Disponível em: < https://baptistaluz.com.br/wp-content/uploads/2019/04/o-que-%C3%A9-open-banking-vers%C3%A3o-final.pdf>. Acesso em: 19 out. 2020.

KREMER, Bianca. **LGPD em vigor:** por que racializar a proteção de dados é tão importante? Disponível em: < https://www.jota.info/opiniao-e-analise/artigos/lgpd-em-vigor-protecao-dados-importante-01102020>. Acesso em: 19 out. 2020.

LEONARDI, Marcel. Bases legais de tratamento de dados pessoais e o mercado financeiro. CANTARINO BRASILEIRO. Anuário Brasileiro de Bancos (ABB) 2019. **Relatório Bancário**, 14 ed. São Paulo, 2019. Disponível em: < https://cantarinobrasileiro.com.br/publicacoes/anuariodebancos19/download/>. Acesso em: 26 ago. 2020.

MORIBE, Gabriela Tiemi; SILVA, Gustavo Henrique Luz. **O que ainda não te contaram sobre a "nova" Lei do Cadastro Positivo?** 2020. Disponível em: < https://baptistaluz.com.br/wp-content/uploads/2020/01/lei_cadastro_positivo_VF.pdf>. Acesso em: 19 out. 2020.

PALHARES, Felipe. et al. **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020.

PINHEIRO, Patrícia Peck. **Direito Digital**. 5 ed. São Paulo: Editora Saraiva, 2013. Livro eletrônico, não paginado.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais:** comentários à Lei nº 13.709/2018 (LGPD). 2º ed. São Paulo: Saraiva Educação, 2020**.**

PINHEIRO, Patrícia Peck. LGPD em vigor: como a nova lei afeta as instituições financeiras. **Revista CIAB - FEBRABAN.** 2020a. Disponível em: < https://noomis.febraban.org.br/especialista/patricia-peck-pinheiro/lgpd-em-vigor-como-a-nova-lei-afeta-as-instituicoes-financeiras?pesquisa=nova-lei-do-cadastro-positivo>. Acesso em: 19 out. 2020.

PINHEIRO, Patrícia Peck. Open banking: ciberseguranca e gestão de dados no sistema financeiro aberto. **Revista CIAB-FEBRABAN.** 2020b. Disponível em: < https://noomis.febraban.org.br/especialista/patricia-peck-pinheiro/open-banking-ciberseguranca-e-gestao-de-dados-no-sistema-financeiro-aberto>. Acesso em: 19 out. 2020.

Revista CIAB - FEBRABAN. 2020. **Como as financeiras devem se preparar para 2020:** o ano da LGPD. Disponível em: < https://noomis.febraban.org.br/especialista/patricia-peck-pinheiro/como-as-financeiras-devem-se-preparar-para-2020-o-ano-da-lgpd?pesquisa=nova-lei-do-cadastro-positivo>. Acesso em: 19 out. 2020.

Revista CIAB - FEBRABAN. 2020. **Lei de proteção de dados ganha confiança de consumidor, mas enfrenta despreparo das empresas.** Disponível em: < https://noomis.febraban.org.br/noomisblog/lei-de-protecao-de-dados-ganha-confianca-de-consumidor-mas-enfrenta-despreparo-das-empresas>. Acesso em: 19 out. 2020.

TEIXEIRA, Tarcísio. **Empresas e a implementação da Lei Geral de Proteção de Dados.** 1.ed. Salvador: Editora JusPodivm, 2021.

TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei geral de proteção de dados pessoais:** comentado artigo por artigo. 2.ed. ver., atual e ampl. Salvador: Editora JusPodivm, 2020.

TEIXEIRA, Tarcísio; LOPES, Alan Moreira; TAKADA, Thalles. **Manual jurídico da inovação e das startups.** 2.ed. Salvador: Editora JusPodivm, 2020.