FUNDAÇÃO GETULIO VARGAS
ESCOLA DE DIREITO DE SÃO PAULO

DANIELE DE ANDRADE MALTA

A REGULAÇÃO DO OPEN FINANCE E SUA INTERSEÇÃO COM A PROTEÇÃO DE DADOS PESSOAIS

SÃO PAULO
2023

DANIELE DE ANDRADE MALTA

A REGULAÇÃO DO OPEN FINANCE E SUA INTERSEÇÃO COM A PROTEÇÃO DE DADOS PESSOAIS

Dissertação a ser apresentada à Escola de Direito da Fundação Getulio Vargas como requisito para obtenção do título de Mestre em Direito.

Área de concentração: Direito dos negócios

Orientador: Prof. Dr. Emerson Ribeiro Fabiani

SÃO PAULO
2023

Malta, Daniele de Andrade.

A regulação do *open finance* e sua interseção com a proteção de dados pessoais / Daniele de Andrade Malta. - 2023.

f. 107

Orientador: Emerson Ribeiro Fabiani.

Dissertação (mestrado profissional) - Fundação Getulio Vargas, Escola de Direito de São Paulo.

1. Lei Geral de Proteção de Dados Pessoais (LGPD). 2. Indústria de serviços financeiros - Inovações tecnológicas. 3. Compartilhamento. 4. Consentimento (Direito). I. Fabiani, Emerson Ribeiro. II. Dissertação (mestrado profissional) - Escola de Direito de São Paulo. III. Fundação Getulio Vargas. IV. Título.

CDU 342.738

Ficha Catalográfica elaborada por: Isabele Oliveira dos Santos Garcia CRB SP-010191/O
Biblioteca Karl A. Boedecker da Fundação Getulio Vargas - SP

#Pública

DANIELE DE ANDRADE MALTA

A REGULAÇÃO DO OPEN FINANCE E SUA INTERSEÇÃO COM A PROTEÇÃO DE DADOS PESSOAIS

Dissertação a ser apresentada à Escola de Direito da Fundação Getulio Vargas como requisito para obtenção do título de Mestre em Direito.

Área de concentração: Direito dos negócios

Prof. Orientador: Dr. Emerson Ribeiro Fabiani

Data de aprovação ____ / ____ / ____
Banca examinadora:

_____
Prof. Dr. Emerson Ribeiro Fabiani (Orientador)
FGV – Direito SP

_____
Prof. Dr. Alexandre Pacheco da Silva
FGV- Direito SP

_____
Prof. Dra. Tainá Aguiar Junquilho

SÃO PAULO
2023

AGRADECIMENTOS

Ao meu marido, Sérgio Ricardo de Freitas, companheiro de vida e o maior entusiasta dos meus sonhos, por ser o refúgio seguro e fonte de coragem e incentivo nos momentos de desânimo.

Ao meu pai, Aristides Ferreira Malta (*in memorian*), por mesmo ausente do mundo terreno ser minha principal referência intelectual e me impulsionar a honrar e reescrever sua história de vida por meio das minhas conquistas.

A minha mãe, Maria Conceição Garcia de Andrade Malta, aquela que, mesmo sem dominar os conceitos, ensinou-me a importância da luta das mulheres por espaço e respeito. Agradeço pelo exemplo de sempre enfrentar os desafios de cabeça erguida, com a força e retidão que lhe são peculiares. E, por durante todo o período de dedicação ao mestrado, compreender minhas ausências e por me devolver a tranquilidade com a fé depositada em suas orações diárias.

Ao meu orientador, Professor Emerson Ribeiro Fabiani, pelas valiosas contribuições ao presente trabalho, sempre pautadas no aperfeiçoamento, clareza das ideias e rigor acadêmico, e prestadas com especial educação e cordialidade.

Ao Banco do Brasil, pelo compromisso de apoiar o desenvolvimento de seu corpo funcional, traduzido em instrumentos institucionais efetivos de apoio à pesquisa, aos quais tive acesso e foram essenciais para o êxito do presente trabalho.

Ao meu gestor e amigo, José Roberto Chieffo Junior, por apoiar incondicionalmente minha dedicação ao mestrado e por tantos outros exemplos diários de liderança, por todo o conhecimento compartilhado e, sobretudo, pela alegria genuína que vi em seu rosto a cada etapa superada no desenvolvimento do presente trabalho.

Aos meus amigos de jornada no mestrado, turma Direito dos Negócios, ano 2021, cujo contato eminentemente virtual, dada as limitações impostas pela pandemia do Covid-19, não impediu a construção de vínculos sólidos, permeados por parceria, troca de ideias, incentivos mútuos e alegrias compartilhadas.

RESUMO

Este estudo pretende tratar da proteção dos dados pessoais dos clientes bancários no *open finance.* Para tanto, adota a metodologia de pesquisa bibliográfica, com preponderância dos estudos desenvolvidos pelo Banco Central do Brasil e literatura especializada, cotejo entre o arcabouço jurídico sobre proteção de dados pessoais e a regulação do open finance bem como imersão na sua sistematização e operacionalização. A partir desse quadro, foram identificados os potenciais riscos, classificando-os em riscos exógenos e endógenos. Pautado na compatibilização entre a proteção de dados pessoais e o seu compartilhamento via *open finance,* bem como no atingimento dos objetivos almejados por tal ecossistema, recomenda-se um conjunto de boas práticas, composto por medidas mitigadoras dos riscos mapeados, a serem adotadas pelas instituições participantes.

Palavras-chave: Proteção de dados pessoais. LGPD. *Open finance*. Compartilhamento de dados. Consentimento.

ABSTRACT

This study intends to address the impacts of personal data security of bank customers in open finance. Therefore, it adopts a bibliographic research methodology, with predominantly studies developed by the Brazilian Central Bank and published articles related to the topic, comparing between legal framework regarding personal data security and regulating this ecosystem, as well as an immersion in its categorization and operationalization.

From this scope, potential menaces have been identified and classified as exogeneous and endogenous risks. Based on the compatibility between personal data security and its classification via open finance, as well as achieving the desired objectives by aforementioned ecosystem, it's recommended that a set of best practices, composed of measures to mitigate the mapped risks, is to be adopted by the participating institutions.

Keywords: Personal data protection. LGPD. Open finance. Data sharing. Consent.

LISTA DE ILUSTRAÇÕES

Figura 1	Escala progressiva da adjetivação do consentimento	35
Figura 2	Fluxo operacional do *open finance*.	41
Figura 3	Jornada do Consentimento	54
Figura 4	Informações do Portal do *open finance*	55
Figura 5	Vantagens do *open finance* (casos de uso)	56

LISTA DE TABELAS

Tabela 1	Vocabulário analítico para a definição do conceito de dados pessoais	23
Tabela 2	Fatores de risco no open finance	75
Tabela 3	Riscos, fatores de riscos e ações mitigadoras dos riscos	76
Tabela 4	Mecanismos de preservação da privacidade do usuário	88

LISTA DE ABREVIATURAS E SIGLAS

ACT - Acordo de Cooperação Técnica

ANPD - Autoridade Nacional de Proteção de Dados

API - *Application Programming Interface*

Bacen - Banco Central do Brasil

BNDES - Banco Nacional do Desenvolvimento

CADE - Conselho Administrativo de Defesa Econômica

CDC - Código de Defesa do Consumidor

CEP - Código de Endereçamento Postal

CIR - *The Center for Investigative Reporting*

CMN - Conselho Monetário Nacional

CPC - Código de Processo Civil

DTN - *Do not Track*

EDPB - *European Data Protection Board*

Febraban - Federação Nacional dos Bancos

ITS - Instituto de Tecnologia e Sociedade

P3P - *Platform for Privacy Preferences*

PETs - *Privacy Enhancing Technologies*

RIPDP - Relatórios de Impacto à Proteção de Dados Pessoais

SCR - Sistema de Informações de Crédito

Senacon - Secretária Nacional do Consumidor

SFN - Sistema Financeiro Nacional

STJ - Superior Tribunal de Justiça

WP29 - *Article 29 Working Party*

SUMÁRIO

1 **INTRODUÇÃO** 10

2 **ESTRUTURA JURÍDICO-NORMATIVA DA PROTEÇÃO DE DADOS PESSOAIS E DO *OPEN FINANCE*** 22

2.1 CONCEITOS DA LEI GERAL DE PROTEÇÃO DOS DADOS PESSOAIS (LGPD) 22

2.1.1 Base legal do consentimento 31

2.1.2 Consentimento no *open finance* 39

3 COMPATIBILIDADE DO OPEN FINANCE À PROTEÇÃO DE DADOS PESSOAIS 44

3.1 POTENCIAIS VIOLAÇÕES À PROTEÇÃO DE DADOS PESSOAIS NO *OPEN FINANCE* 45

3.1.1 Riscos exógenos – segurança da informação 49

3.1.2 Riscos endógenos 52

3.2 TRATAMENTO DOS DADOS PESSOAIS COM FULCRO NO CONSENTIMENTO 57

3.3 TRATAMENTO DE DADOS PESSOAIS COM FULCRO NA PROTEÇÃO DO CRÉDITO 63

3.4 DECISÕES AUTOMATIZADAS E *PROFILING* NO *OPEN FINANCE* 66

4 RECOMENDAÇÕES DE BOAS PRÁTICAS PARA A PROTEÇÃO DOS DADOS PESSOAIS NO OPEN FINANCE 76

4.1 RISCOS EXÓGENOS – SEGURANÇA DA INFORMAÇÃO 77

4.2 RISCOS ENDÓGENOS 82

5 CONCLUSÃO 94

REFERÊNCIAS 98

1 INTRODUÇÃO

O uso exponencial e a monetização dos dados pessoais impulsionaram uma mudança estrutural na economia e forjaram o debate sobre a tutela jurídica a ser conferida à matéria, alçando os dados pessoais à condição de bem jurídico, com relevantes implicações econômicas, por se tratar do "novo petróleo da internet e a nova moeda do mundo digital"[1], assertiva que já se tornou lugar comum quando se fala em dados.

À medida em que os dados pessoais ganharam destaque no direcionamento das atividades econômicas, o tratamento desses dados tornou-se potencial vantagem competitiva, capaz de impactar toda a cadeia produtiva mediante alteração da dinâmica concorrencial e da experiência do titular desses dados.

Os novos modelos de negócios e inovações tecnológicas advindas do uso massivo de dados despertam inúmeros desafios na seara de sua proteção jurídica, resultando em importantes marcos legislativos, a exemplo do Regulamento Geral de Proteção de Dados da União Europeia (GDPR*)*, no espectro internacional, e a Lei nº 13.709/18 – Lei Geral de Proteção de Dados Pessoais (LGPD), em âmbito nacional, além da Emenda Constitucional nº 115/2020[2], que incluiu a proteção de dados pessoais no rol dos direitos fundamentais.Os direitos da personalidade nascem no espectro do direito público como resposta ao absolutismo do Estado e da consequente busca pela valorização do cidadão[3]. Com a evolução social, tais direitos tornam-se mais abrangentes, de modo a integrar também as relações pautadas pelo direito privado[4].

A visão dos direitos da personalidade como direitos subjetivos privados ampara o elenco de suas características descritas no artigo 11 do Código Civil, quais sejam, instransmissibilidade, indisponibilidade e irrenunciabilidade. Nesse espectro, os direitos da personalidade ainda engendrados como direitos subjetivos de forte viés patrimonial, pautados no binômio lesão-sanção, tornam-se incapazes de tutelar todas as atuais facetas da personalidade[5].

No intento de conferir uma tutela adequada à sociedade contemporânea, o subjetivismo é superado e adota-se o valor máximo da pessoa humana como diretriz interpretativa dos direitos

---

[1] KUNEVA. Meglena. Discurso proferido na mesa redonda sobre coleta de dados, direcionamento e perfilação. Bruxelas. 31 de março de 2009.

[2] Artigo 5º, LXXIX da Constituição Federal: É assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. (Incluído pela Emenda Constitucional nº 115 de 2020)

[3] Seus marcos históricos são a Revolução Norte-americana, em 1776, e a Revolução Francesa, em 1789 e seus signos normativos são a Declaração Americana (1776), a Declaração Francesa (1789) e a Declaração Universal da ONU (1946).

[4] A teoria dos direitos subjetivos é construída pela doutrina alemã, cujo principal expoente é Otto Von Gierke, responsável por cunhar a terminologia *"direitos da personalidade."*

[5] TARTUCE. Flávio. Lei de Introdução e Parte Geral. v.1. 13ª ed. Rio de Janeiro. Forense. 2017. p. 144-145

da personalidade, mediante a adoção cláusula geral de tutela da personalidade, cujo fundamento central é o princípio da dignidade da pessoa humana, extraído do artigo 1º, III, da CF[6].

A partir da colocação da dignidade da pessoa humana como cerne interpretativo, a positivação dos direitos da personalidade em determinados artigos constitucionais e legais não mais restringe sua classificação, pois irrefutável o caráter não exauriente de tais dispositivos, de tal sorte que toda a hermenêutica jurídica passa a ser balizada pela cláusula geral de tutela da personalidade e os princípios a ela inerentes, de modo a assegurar proteção jurídica à todas as irradiações da personalidade ante as mudanças sociais cada vez mais dinâmicas.[7]

Dentre as diversas matizes dos direitos da personalidade, o direito à privacidade, cuja consolidação como direito fundamental está atrelada a própria evolução dos direitos da personalidade, emerge como potencial fundamento hábil a adaptar-se a tutela requerida pelos dias hodiernos[8].

Não obstante a relevância do "*direito de estar só*", enquanto embrião do direito à privacidade, indelével a essencialidade das interações sociais para a existência do indivíduo, razão pela qual o caráter relacional ganha destaque[9].

Assim, a superação do paradigma individualista e patrimonialista, no qual pautava a origem do direito à privacidade, converge para a evolução dos direitos da personalidade, no sentido da colocação do homem como centro do ordenamento jurídico e na tutela do livre desenvolvimento de sua personalidade, ao qual o convívio social é fundamental[10].

Dada essa arquitetura, a interpretação do direito à privacidade, à luz do princípio da dignidade humana, adquire contornos mais nítidos, de modo que a *"privacidade torna-se uma grande preocupação, pois a partir da sua violação, com efeito cascata, serão lesionados direitos fundamentais*"[11].

A remodelação conceitual do direito à privacidade e, notadamente, a mencionada preocupação que sua violação provoca é ampliada ao confrontar-se com a nova arquitetura informacional, fruto do dinamismo tecnológico e de sua consequente majoração do fluxo qualitativo e quantitativo de informações.

---

[6] MORAES. Maria Celina Bodin. Ampliando os direitos da personalidade. In: José Ribas Vieira (org.), 20 anos da Constituição cidadã de 1988: efetivação ou impasse institucional?. Rio de Janeiro. Forense. 2008. p.5

[7] JABUR. Gilberto Haddad. Liberdade de pensamento e direito à vida privada. São Paulo. Revista dos Tribunais. 2000. p. 28

[8] DONEDA. Danilo. Da privacidade à proteção de dados. Rio de Janeiro. Renovar. 2006. p. 14

[9] MORAES. Maria Celina Bodin. Op.cit. p. 14

[10] DONEDA. Danilo. Op. cit. p. 90

[11] FERREIRA. Rafael Freire. Desafios em sede de tutela da Personalidade: a autodeterminação informativa e a privacidade na sociedade da informação. Dissertação (Mestrado em Ciências Jurídicas) – Universidade Autónoma de Lisboa Luís de Camões, Lisboa.2016. p. 62

A origem do direito à privacidade contrapõe-se a proteção dos dados pessoais almejada nos dias hodiernos, dado o paradoxo entre o direito de ficar só e a tutela da privacidade numa sociedade de elevada exposição digital, sob um viés de coletividade.

Essa mudança de paradigma impôs ao direito à privacidade ocupar-se também de seu viés informacional, com vistas a proteção de dados pessoais, dando ensejo aos preceitos da autodeterminação informativa.

No entanto, a evolução legislativa em matéria de proteção de dados e as mudanças tecnológicas e sociais dos últimos tempos despertaram a insuficiência da hermenêutica do direito à proteção de dados pessoais como corolário do direito à privacidade, ainda que este mostre-se aperfeiçoado pelos ditames informacionais.

A abordagem da proteção de dados como um direito autônomo não é nova e remonta as gerações legislativas anteriores, com forte caráter individualista e exclusivista. A categorização como direito fundamental, por sua vez, é fruto do atual estágio da evolução jurídica da proteção de dados, inserta na quarta fase geracional de leis sobre a matéria.

Aliás, os contornos iniciais da "autodeterminação informacional", compreendida como a autonomia do indivíduo sobre as informações disponíveis sobre sua própria vida e tão cara à proteção de dados, surge apenas na terceira fase geracional, ainda com fortes traços individualistas, e tem como o signo a decisão da Corte Constitucional alemã pela inconstitucionalidade parcial da Lei do Censo de 1983.[12]

Apenas a quarta geração transpôs a barreira individualista da proteção de dados pessoais, consolidando a própria evolução do direito da privacidade, ambos no sentido da tutela coletiva.[13]

No arcabouço jurídico brasileiro, defendeu-se que a intelecção da proteção de dados como um direito fundamental poderia ser extraída dos direitos da personalidade e da privacidade, sob a ótica interpretativa do princípio da dignidade humana, conforme evolução interpretativa desses direitos, a exemplo da decisão do Supremo Tribunal Federal, nos autos do ADI 6387/DF, ao tratar da suspensão da eficácia da MP 954/20, no qual a Corte Superior conferiu aos dados pessoais a proteção constitucional assecuratória com base nos direitos positivados, entendendo que tal proteção alcança todas as manifestações da personalidade. Por outro lado, para manter tal entendimento seria forçoso sepultar a interpretação literal do sigilo previsto no artigo 5º, XII

[12] BIONI. Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro. Forense. 2019. p. 103.

[13] DONEDA. Danilo. Privacidade e transparência no acesso à informação pública. Zaragoza. Prensas Universitárias de Zaragoza. 2010. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/lefis11-09.pdf. Acesso em: 16 de novembro de 2022. p. 203.

da CF, no sentido de que a proteção de informações pessoais, entendida como dados, estaria adstrita à sua comunicação.

O direito é um fenômeno social, fruto de um processo histórico, e como tal, varia no tempo e no espaço.[14] Assim, conquanto possível a recondução interpretativa dos direitos fundamentais já consagrados, o debate sobre o direito à proteção aos dados pessoais foi, por fim, superado com a intervenção do constituinte derivado, mediante sua positivação no texto constitucional, ainda que sua interpretação esteja, especialmente sobre o viés histórico, atrelada aos direitos da personalidade e da privacidade.

Nesse prisma, a crescente necessidade de tutela dos dados pessoais e sua positivação como direito fundamental não infirmam os preceitos do direito da privacidade, sendo, ao reverso, o ponto de convergência das mudanças de paradigmas dos direitos fundamentais forjadas pela relevância dos dados pessoais no contexto da sociedade da informação. Assim, *"transpassou incontroverso também, que a proteção de dados pessoais, é hoje (ou continua sendo) um elemento primordial para a autopreservação do seu titular, sendo uma questão de "sobrevivência" do direito à privacidade"*[15].

Todo o desenvolvimento tecnológico promoveu (e ainda promove) substanciais alterações macrossociais, abarcando as mais variadas atividades econômicas[16], ante as quais o direito foi instado a adequar-se, na forma supra relatada.

O mercado financeiro, da mesma forma, não ficou indene à intensificação das inovações tecnológicas e aos novos modelos de negócios[17], fortemente calcados no tratamento de dados pessoais, conforme pontuado pela Comissão Europeia:

> "Embora a inovação no setor financeiro não seja nova, o investimento em tecnologia e o ritmo da inovação aumentaram consideravelmente. Soluções FinTech usando identificação digital, aplicativos móveis, computação em nuvem, análise de big data, inteligência artificial e blockchain estão sendo lançadas. As novas tecnologias estão mudando a indústria financeira e a forma como os consumidores e as empresas acessam os serviços, criando oportunidades para as soluções baseadas na FinTech proporcionarem um melhor acesso ao financiamento e melhorarem a inclusão financeira dos cidadãos digitalmente conectados. Coloca os clientes no papel do condutor,

[14] JUNIOR. Ivo Gico. Introdução ao Direito e Economia. In. Direito e economia no Brasil. Organizador Luciano Benetti Timm. 2ª ed. São Paulo. Atlas. 2018. p. 4.

[15] FERREIRA. Rafael Freire. Op. cit. p. 55

[16] MALDONADO. Viviane Nóbrega; GUTIERREZ, Andriei. A estratégia brasileira para a transformação digital e as questões que dela emergem no que se refere à proteção de dados pessoais. Revista dos Tribunais. v. 993. 2018. p.295

[17] ARNER. Douglas. BARBERIS. Janos Nathan. BUCKELY. Ross. Fintech, Regtech, and the Reconceptualization of Financial Regulation. Northwestern Journal of International Law & Business. v.37. n. 3. 2017.

> apoia a eficiência operacional e aumenta ainda mais a competitividade da economia da União Europeia".[18]

Em resposta a tal contexto social e com o escopo de fomentar tais inovações, e, ao mesmo tempo, resguardar o *enforcement* à regulação do setor, o Banco Central (BC) adotou um papel de protagonista, por meio da AgendaBC#, direcionando o desenvolvimento de importantes ações, em alinhamento com o Plano Estratégico Institucional (PEI-BCB) para o período de 2020 a 2023.

A agendaBC# consubstancia parte do planejamento estratégico do Banco Central voltado ao incentivo à inovação tecnológica e é norteado por cinco pilares: inclusão, competitividade, transparência, educação e sustentabilidade.

Dentre os projetos desenvolvidos sob a ótica da agenda BC#, destacam-se o PIX, o *open finance*, inicialmente denominado *open banking*, e o Sandbox regulatório.

A construção de um ambiente regulatório pró-inovação e competitividade demonstra que o ineditismo não se restringe à intensificação das inovações e de novos modelos de negócios no segmento financeiro, mas também na mudança da atuação do próprio órgão regulador, anteriormente centrada na política monetária e estabilidade do Sistema Financeiro Nacional[19], sem esquecer que a superação da hiperinflação e as medidas estruturantes do setor contribuem, sobremaneira, para viabilizar o direcionamento dos esforços em novas frentes.[20]

O posicionamento do órgão regulador de adotar instrumentos para o fomento da competitividade representa uma mudança de sua atuação, historicamente pautada pelas suas funções de zelar pelo poder de compra da moeda como assegurar um sistema financeiro sólido e eficiente[21], distante da adoção de uma política concorrencial, tendo em vista o papel exercido pelos Bancos para a estabilidade do setor e os riscos para a economia advindos de externalidades que envolvam a quebra de tais Instituições[22].

---

[18] Fintech Action Plan: For a more competitive and innvotive European financial sector. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0109. Acesso em 25 de janeiro de 2023.

[19] Destacam-se a estabilidade monetária com o Plano Real (1994), o saneamento do sistema bancário a partir de 1995, a flutuação do câmbio em 1999, o Sistema de Metas para a Inflação (Decreto nº 3.088/99), a reforma de Sistema de Pagamentos Brasileiro (SPB), no final de 1999 e consolidado na Lei nº 10.214/01), a reforma cambial introduzida pela Lei nº 11.371/06 e as medidas prudenciais advindas dos Acordos de Basiléia.

[20] SANTOS. Marcel Mascarenhas dos. Revolução Regulatória no Sistema Financeiro Nacional. In: Banking 4.0: Desafios jurídicos e regulatórios do novo paradigma bancário e de pagamentos. Coord. Bruzzi, Eduardo; Feigelson. Bruno. 1ª ed. Thomson Reuters. São Paulo. 2020. p.65.

[21] ESTRELA. Márcio Antonio. Moeda, Sistema Financeiro e Banco Central – Uma abordagem teórica e prática sobre o funcionamento de uma autoridade monetária no mundo e no Brasil. Rio de Janeiro: Fundação Cesgranrio, 2011. p. 179.

[22] CARLETTI. Elena. SMOLENSKA, Agnieska. 10 years on from the financial crisis: co-operaion between competition agencies and regulators in the financial sector. OECD, 2017. Disponível em: https://one.oecd.org/document/DAF/COMP/WP2(2017)8/en.pdf. Acesso em 07 de janeiro de 2024.

Reconhecida a importância de todas as preditas ações impulsionadas pelo Banco Central do Brasil com o escopo de fomentar a inovação no setor, o presente trabalho debruça-se, especificamente, sobre o *open finance.*

O *open finance* ou sistema financeiro aberto é uma plataforma, estruturada em interface de programação de aplicativos abertos (*Application Programming Interface - API's)*, na qual é possível o compartilhamento de dados pessoais e informações sobre produtos e serviços do cliente bancário entre as instituições participantes. Em síntese, o *open finance* permite a portabilidade de dados bancários e financeiros entre instituições financeiras e/ou instituições de pagamento, por meio de uma plataforma única para sua operacionalização. Nesse sentido:

> "O modelo de Open Banking pode ser compreendido como um meio para compartilhamento de dados pelos clientes do Sistema Financeiro Nacional. Se o outrora as informações sobre a vida financeira dos clientes bancários eram armazenadas exclusivamente nas instituições detentoras de suas contas, o modelo do Open Banking vem alterar essa estrutura, viabilizando o trânsito livre de informações financeiras entre instituições financeiras"[23].

A estruturação do open finance traz consigo, portanto, a promessa de "*mudar a forma como as pessoas se relacionam com o mercado financeiro, impactando diretamente bancos e outros negócios relacionados, por permitir a ampliação de produtos e serviços financeiros oferecidos e por tornar mais fácil o processo de comparação desses produtos, bem como a migração de uma instituição financeiro para outra*"[24].

Sua origem remonta, no cenário nacional, ao Comunicado nº 33.455/19[25], que apresentou as definições e propostas para o *open finance.* Sua implementação deu-se pela Resolução Conjunta do CMN e BCB nº 1/2020[26], que consolidou as diretrizes da regulação do *open finance, e pela* Circular nº 4.015/2020, que fixou o escopo mínimo de dados e os serviços englobados.

Os objetivos do *open finance* são incentivar a inovação, promover a concorrência, aumentar a eficiência do Sistema Financeiro Nacional e do Sistema de Pagamentos Brasileiro, bem como promover a cidadania financeira, conforme artigo 3º da Resolução Conjunta nº 01/2020.[27]

---

[23] GOETTENAUER. Carlos. Open Banking e proteção de dados pessoais: convergências e divergências entre a LGPD e a regulação. In: Direito Público e Tecnologia. Coord. CRAVO. Daniela Copetti. JOBIM. Eduardo. JUNIOR. José Luiz de Moura Faleiros. Indaiatuba. Editora Foco. 2022. p. 81.

[24] ANAQUIM. Ludmilla. LIMA. Marcello.Open Banking e portabilidade de dados – uma análise supranacional. In: Banking 4.0: Desafios jurídicos e regulatórios do novo paradigma bancário e de pagamentos. Coord. Bruzzi, Eduardo; Feigelson. Bruno. 1ª ed. Thomson Reuters. São Paulo. 2020. p.195-196.

[25] BANCO CENTRAL DO BRASIL. 2019.

[26] BANCO CENTRAL DO BRASIL. Conselho Monetário Nacional. 2020.

[27] BANCO CENTRAL DO BRASIL. Conselho Monetário Nacional. 2020.

Tendo em vista a complexidade envolvida, a implementação do ecossistema deu-se de forma faseada, cujo cronograma suportou pontuais atrasos[28], sendo certo que atualmente encontra-se em operação, sujeitando-se a aprimoramentos e desenvolvimento de novos modelos de negócios nele lastreados.

Por tal razão, inclusive, é que o ecossistema foi inicialmente denominado como *open banking*, seguindo o padrão adotado em outros países, e, quando da ampliação do escopo de dados, com o compartilhamento de dados de seguro, investimentos e previdência privada, sua nomenclatura foi adequada para *open finance*.

Ainda que a conceituação jurídica de *open finance* esteja em construção, a regulação permite afirmar que se trata de um sistema aberto e integrado de compartilhamento de dados e serviços bancários entre as Instituições Financeiras, Instituições de Pagamentos e demais Instituições autorizadas a funcionar pelo Banco Central, mediante o consentimento do titular dos dados.

Os dados bancários, antes sujeitos, exclusivamente, a um rígido regramento de sigilo bancário (o qual, obviamente permanece vigente) transpassa para uma interoperabilidade entre instituições, mediante o prévio e expresso consentimento do titular dos dados.

O *open finance,* ao atribuir ao titular dos dados a possibilidade de direcionar o tratamento de seus próprios dados, incorpora, à primeira vista, os atuais preceitos de proteção de dados pessoais, em especial o princípio da autodeterminação informativa, colocando o titular dos dados pessoais no papel de protagonista.

A alteração das regras sobre o compartilhamento de dados e a possibilidade de integração de diferentes sistemas evidenciam a potencialidade de mudanças advindas do *open finance*, especialmente no fomento da competitividade do setor bancário nacional, caracterizada por sua elevada concentração, sobretudo a partir da estabilização monetária advinda com o

[28] Sobre os atrasos, vide: https://www.cnnbrasil.com.br/business/bc-atrasa-primeira-fase-do-open-banking-para-1-de-fevereiro-de-2021/. Acesso em 26 de janeiro de 2023. https://1bilhao.com.br/economia/open-banking-banco-central-adia-para-setembro-de-2022-funcionamento-completo/. Acesso em 26 de janeiro de 2023.

Plano Real[29]. A título ilustrativo desta concentração, os cinco maiores bancos do Brasil[30] respondem por 77,6% do volume de crédito e concentram 74,7% dos depósitos bancários, conforme Relatório de Economia Bancária do Banco Central, referente ao ano de 2022[31].

A atuação do órgão regulador afasta-se, pois, das históricas preocupações referentes à higidez do sistema e direciona-se à competitividade do setor[32].

O tratamento de dados, já disseminado nos mercados digitais, enseja ganhos de eficiência pela individualização das necessidades de cada titular, resultando em vantagem competitiva às empresas mediante diversificação de sua carteira de produtos.[33]

Por outro lado, a assimetria informacional decorrente dessa concentração dos dados enseja implicações concorrências relevantes, notadamente pela caracterização de uma barreira à entrada no mercado, em virtude da dificuldade de os novos entrantes atingirem o mesmo grau de eficiência e conhecimento dos vieses comportamentais, notadamente na seara creditícia, de seus potenciais clientes.

Ainda que não se trate de um remédio concorrencial, acredita-se que o compartilhamento desses dados contribua para modificar esse cenário, gerando efeitos concorrenciais positivos, pois propicia um instrumento para mitigar a assimetria informacional, além de reduzir os custos de transação do titular dos dados migrar seus produtos e/ou serviços entre as diferentes Instituições Financeiras, antes sedimentado na dinâmica de mercado *single homing*.

---

[29] "Com a implementação do Plano Real, em julho de 1994, ocorreu o maior processo de mudanças estruturais no sistema financeiro brasileiro, que pode ser dividido em três fases: i. Na primeira, ocorreu o uso dos mecanismos oficiais de intervenção e de liquidação, que teve como conseqüência a redução do número de bancos. ii. A segunda fase se caracterizou pela implementação do Programa de Estímulo à Reestruturação e ao Fortalecimento do Sistema Financeiro Nacional (Proer), em novembro de 1995, e do Programa de Incentivo à Redução do Setor Público Estadual na Atividade Bancária (Proes). iii. A terceira fase foi marcada pela entrada de bancos estrangeiros que compraram instituições financeiras, inclusive por meio do programa de privatização (Meridional, Banerj, Banespa). Assim, em função da estabilização monetária, o número de instituições financeiras e de suas dependências diminuiu, em conseqüência sobretudo da diminuição nos ganhos provocados pelo imposto inflacionário". (ESTRELA. Márcio Antonio. Moeda, Sistema Financeiro e Banco Central – Uma abordagem teórica e prática sobre o funcionamento de uma autoridade monetária no mundo e no Brasil. Rio de Janeiro: Fundação Cesgranrio, 2011. p. 232-233)

[30] Banco do Brasil, Bradesco, Caixa Econômica Federal, Itaú e Santander.

[31] GARCIA. Larissa. Quatro bancos concentraram 59% do mercado de crédito em 2022, com operações pressionadas pela Selic. Valor Investe. 06 de junho de 2023. Disponível em: https://valorinveste.globo.com/produtos/credito/noticia/2023/06/06/quatro-bancos-concetraram-59percent-do-mercado-de-credito-em-2022-com-operacoes-pressionadas-pela-selic.ghtml. Acesso em 07 de janeiro de 2024.

[32] DOLABELLA. Gabriel. RAGAZZO. Carlos. Open Banking ao redor do mundo: EUA, UE e Austrália – Panorama Econômico #18. Realização Instituto Propague. 2020. Disponível em: https://www.youtube.com/watch?v=NeWNkamyXL8. Acesso em 20 de abril de 2023.

[33] BOUVIER. Pascal. EZRACHI. Ariel. MORTON. Fiona Scott; et al. Committee for the study of digital platforms: Market structure and antitruste subcommittee report. Chicago. Stigler Center for the study of the Economy and the State. University of Chicago Booth School of Business. 2019.

O compartilhamento propiciado pelo *open finance* tende a gerar vantagem competitiva, na medida em que tais dados permitem o desenvolvimento de modelos de negócios mais eficientes e adequados às demandas individualizadas, agregando valor à experiência do cliente, conforme pontuado por Roberto Campos Neto, Presidente do Banco Central, no workshop sobre *Open Banking*: "A integração de plataformas e o compartilhamento de dados criarão incentivos para oferta de novos produtos e serviços à conveniência do cliente, e novas formas de distribuição dos serviços financeiros".[34]

Além da possibilidade de soluções que atendam às necessidades dos clientes, acredita-se, ainda, que a interface comum torne mais fácil a comparação entre os produtos financeiros oferecidos pelos diversos agentes, bem como viabilize o gerenciamento financeiro de forma centralizada, reduzindo os custos de transação suportados pelo cliente quando diversifica seus produtos e serviços entre diferentes agentes.Note-se, por fim, que o impacto concorrencial do tratamento de dados pessoais é corroborado, inclusive, pela incorporação nas análises concorrenciais feitas pelo CADE de aspectos como transparência de algoritmos, níveis de compartilhamento de dados entre empresas, modelos comerciais integradores de mercados distintos e novas estratégias de negócios digitais.[35]

Outrossim, não se pode perder de vista os riscos na seara de cibersegurança e proteção de dados pessoais, com fraudes crescentes e cada vez mais elaboradas e diversificadas, o que torna o *open finance* potencialmente um novo canal de exposição dos clientes bancários a tais riscos.

A tutela jurídica dos dados pessoais também tem evoluído para além dos aspectos de cibersegurança. Nesse cenário, o *open finance*, por mais relevantes que sejam seus objetivos, sobretudo quanto ao fomento à competitividade, precisa adequar-se ao arcabouço jurídico dos dados pessoais, hoje já alçado a condição de direito fundamental e com bases legais para tratamento dos dados já definidas.

Veja-se que o próprio sucesso do open finance parece condicionado a superação de tais entraves, que enseja a resistência de parte dos clientes bancários em compartilhar dados tão íntimos como os dados bancários, o que tem suscitado, inclusive, propostas de alteração de sua

---

[34]Disponível em: https://www.bcb.gov.br/conteudo/home-ptbr/TextosApresentacoes/Apontamentos%20do%20Presidente_Open%20Banking%20v1.pdf. Acesso em 15 de dezembro de 2022.

[35] BISELLI. Esther Collet Janny Teixeira. Inovação e abertura no setor bancário: desafios concorrenciais. In: Revista do Instituto Brasileiro de Estudos Concorrenciais, Consumo e Comércio Internacional. Volume 24. 2018. Disponível em: https://ibrac.org.br/UPLOADS/PDF/RevistadoIBRAC/Revista_do_IBRAC_24_N._2-2018.pdf. Acesso em 26 de janeiro de 2022.

denominação para "*better banking*", como forma de alterar a perspectiva de abertura para uma perspectiva de aperfeiçoamento e melhoria[36].

Nesse sentido, apesar do reconhecimento do incremento à competitividade pela quebra do domínio informacional propiciado pelo *open finance*, estudo publicado pela McKinsey[37] aponta que a confiança nos grandes bancos ainda é uma vantagem competitiva, o que, atrelado ao maior potencial de investimento em tecnologia desse grupo (que lhes permite desenvolver ou replicar, rapidamente, os modelos de negócios inovadores, bem como associar-se aos entrantes, mediante parceria ou aquisição), pode ensejar uma mitigação dos efeitos concorrenciais almejados pelo *open finance*, em virtude dos vieses cognitivos dos clientes bancários e da captura dos entrantes pelos grandes bancos.

Nesse sentido, relatório da World FinTech Report identificou que 75% das fintechs ao redor do mundo objetivam firmar parcerias com bancos e instituições tradicionais.

No cenário nacional, a Pesquisa de Tecnologia Bancária[38], elaborada pela Delloite, sob encomenda da Febraban, já apresenta a intensificação das parceiras, com movimento de distribuição dos produtos bancários nos canais dos parceiros e dos produtos parceiros nos canais dos bancos, valendo-se os bancos tradicionais da imagem de agente financeiro confiável para agregar valor e segurança aos novos modelos de negócios[39].

Portanto, pode-se asseverar que o engajamento dos usuários no *open finance* e seu consequente aumento da competitividade no setor dependem da confiança e credibilidade no ecossistema.

Desse modo, o estímulo ao compartilhamento de dados previsto no *open finance* exige compatibilização com a crescente preocupação da sociedade com a tutela dos dados pessoais, notadamente ante o novo arcabouço jurídico destinado à sua proteção.

Nesse contexto, o presente trabalho investiga a compatibilidade do padrão de proteção aos dados fixado na regulação do *open finance,* sobretudo pela adoção da base legal do consentimento como o instrumento autorizador do compartilhamento de dados no ecossistema em apreço, com a proteção dos direitos dos titulares dos dados, especialmente aquela conferida pela LGPD e pelos princípios aplicáveis a esta seara do direito em crescente evolução.

---

[36] Skinner.Chris. Is Open Banking all it's craked up to be? Disponível em: https://thefinanser.com/2023/09/is-open-banking-all-its-cracked-up-to-be. Acesso em 19 de novembro de 2023.

[37] CARVALHO. Laura Brodsky Liz. Data sharing and open baking. 05 de setembro de 2017. Disponível em: https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking. Acesso em 26 de janeiro de 2022.

[38] Disponível em: https://www2.deloitte.com/br/pt/pages/financial-services/articles/pesquisa-febraban-tecnologia-bancaria.html

[39]Disponível em: https://veja.abril.com.br/economia/bancos-tradicionais-se-rendem-as-fintechs/. Acesso em 05 de janeiro de 2023.

O ineditismo do *open finance*, o seu desenho regulatório e o almejado fomento à concorrência, bem como o elevado número de clientes bancários cujos dados estarão sujeitos ao compartilhamento delineiam a relevância do estudo de sua regulação e dos riscos à proteção destes dados a serem compartilhados, via prévio consentimento.

Outro ponto que merece destaque é a regulação ora em estudo ter por escopo estruturar o sistema ainda não existente, ou seja, o *open finance* está sendo construído a partir da regulação.

A antecedência da regulação em face do ecossistema fornece uma oportunidade ímpar para uma estruturação aderente aos objetivos traçados pelo órgão regulador, ao mesmo tempo que desperta a necessidade de antever riscos e mitigar seus impactos, em especial na sensível questão da proteção dos dados bancários a serem compartilhados e potenciais violações aos direitos de seus titulares, cujos contornos mais nítidos também estão em construção no mundo jurídico.

O presente trabalho propõe-se a enfrentar questões essenciais sobre a nova regulação e sua escolha pela base legal do consentimento, em detrimento das demais bases legais previstas na LGPD, com vistas a uma gestão adequada dos riscos e o desenvolvimento de uma compatibilização entre os objetivos da regulação e a proteção dos direitos dos titulares dos dados.

Para tanto, no primeiro capítulo aborda-se os principais tópicos do arcabouço jurídico da proteção de dados pessoais e suas intersecções com a regulação do *open finance*, construindo a base teórica hábil à identificação de potenciais riscos.

Sedimentado o conhecimento jurídico sobre a matéria, o segundo capítulo imerge no efetivo cotejo entre a proteção de dados pessoais e os preceitos do *open finance*, identificando os pontos de convergência e aqueles que exigem maior atenção, ante os potenciais riscos de violação dos direitos dos titulares de dados pessoais.

Assim, após o desenvolvimento de um estudo aprofundado sobre a regulação do *open finance*, sob a ótica de sua adequação à proteção de dados pessoais e suas potenciais violações, propõem-se, no capítulo derradeiro do presente trabalho, boas práticas e possíveis melhorias à regulação e/ou novos vieses interpretativos, com o escopo de contribuir para a conformidade das Instituições Financeiras atuantes neste novo modelo, bem como resguardar os dados pessoais dos clientes bancários.

Pretende-se, ao final, que o presente trabalho possa contribuir com os modelos de negócios a serem desenvolvidos no *open finance*, não apenas sob a ótica das exigências regulatórias mas, sobretudo, à luz do arcabouço jurídico da proteção de dados pessoais e das

bases legais hábeis ao compartilhamento dos dados, com vistas a subsidiar a atuação dos agentes envolvidos, notadamente as Instituições Financeiras, na proteção dos dados pessoais dos clientes bancários e na necessária relação de confiança entre sociedade e Sistema Financeiro Nacional, além da construção do entendimento a respeito da matéria, ainda com contornos pouco definidos.

2 ESTRUTURA JURÍDICO-NORMATIVA DA PROTEÇÃO DE DADOS PESSOAIS E DO *OPEN FINANCE*

2.1 CONCEITOS DA LEI GERAL DE PROTEÇÃO DOS DADOS PESSOAIS

A compreensão do novo arcabouço jurídico de proteção dos dados pessoais exige um prévio alinhamento sobre os conceitos basilares aplicáveis ao tema, porém, por rigor metodológico, restritos àqueles necessários a construção da base teórico-normativa hábil ao desenvolvimento do presente trabalho, sob o prisma do *open finance*.

De início, um questionamento singelo e aparentemente óbvio merece ser formulado. Afinal, quais são os dados a serem objeto da tutela jurídica em estudo?

Dado pessoal é a informação relacionada a pessoa natural identificada ou identificável, conforme artigo 5º, I, da Lei nº 13.709/18, ou seja, quaisquer dados relacionados ao indivíduo que permitam sua identificação, classificadas mediante seu grau de identificabilidade[40].

Nesse panorama, dado pessoal identificado é aquele de vínculo direto com seu titular, cujo conteúdo permite que a pessoa natural seja diretamente identificada, como, por exemplo, o número de inscrição no cadastro de pessoas físicas (CPF).

O Dado pessoal identificável, por sua vez, é aquele cujo vínculo com o titular possui caráter indireto ou mediato, de modo que, em uma análise contextual, o titular do dado torna-se identificável.

Note-se que a legislação pátria, fortemente inspirada no arcabouço jurídico europeu, consubstanciado no GDPR, englobou os dados identificáveis na seara dos dados pessoais, adotando, assim, o viés expansionista do conceito, em detrimento da orientação reducionista. Nesse sentido, veja-se o didático quadro apresentado pelo Professor Bruno Ricardo Bioni:

[40] Expressão utilizada por Paul M. Schwartz e Daniel J. Solove. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1909366. Acesso em 18 de dezembro de 2022.

Tabela 1 – Vocabulário analítico para a definição do conceito de dados pessoais

EXPANSIONISTA	REDUCIONISTA
Pessoa identificável	Pessoa identificada
Pessoa indeterminada	Pessoa específica, determinada
Vínculo mediato, indireto, impreciso ou inexato	Vínculo imeditado, direto, preciso ou exato
Alargamento da qualificação do dado como pessoal	Retração da qualificação do dado como pessoal

Fonte: BIONI. Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2ª ed. Rio de Janeiro. Forense. 2019. p. 68.

A adoção do conceito expansionista resguarda maior aderência às necessidades do atual estágio da sociedade da informação, pois o crescente uso da tecnologia do BigData resulta na preponderância do uso de bases de dados não estruturadas (NoSQL), as quais não têm uma linguagem organizada como nas bases relacionais, o que ensejaria uma maior dificuldade de subsunção da norma ao caso concreto, sob o viés reducionista[41].

Tem-se ainda a categoria dos dados sensíveis, conceituada pelo artigo 5º, II da Lei 13.709/18, como o 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.

O conceito de dados sensíveis adotado pelo ordenamento pátrio é muito próximo ao previsto no artigo 9º, 1º do GDPR, o qual prevê a proibição do tratamento de dados que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa, além de definir em seu artigo 4º os dados genéticos, dados biométricos e dados relacionados à saúde do usuário.

Em interpretação ao conceito legal, é possível asseverar que o dado sensível é aquele com potencial de ensejar eventual discriminação de seu titular. A dimensão do potencial discriminatório contido no dado sensível é explicada pelas palavras de Ana Frazão:

> "A razão da preocupação especial com os dados sensíveis diz respeito a assegurar não apenas a privacidade, mas também que tais dados não possam

[41] BIONI. Bruno Ricardo. Xeque-Mate: O tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. GpoPai/USP – Grupo de Pesquisa em Políticas Públicas para acesso à informação. São Paulo. 02.07.2015. Disponível em: http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf. Acesso em 17 de dezembro de 2022.

> ser utilizados contra os titulares, trazendo-lhes restrições ao acesso a bens, serviços e mesmo ao exercício de direitos. Basta imaginarmos o potencial dos dados biométricos, como imagens faciais ou impressões digitais, para se ter conhecimento de características físicas, psicológicas e comportamentais de um indivíduo.
> Acresce que discussões mais recentes apontam para a ocorrência de fenômeno de publicidade comportamental voltado à formação de perfis de consumo, fato que se relaciona diretamente à regulação do tratamento de dados pessoais, em especial os dados sensíveis. Na verdade, na seara consumerista, assim como na seara trabalhista, são inúmeros os riscos da utilização de tais dados para praticar toda sorte de discriminações e violações a consumidores, empregados e candidatos a emprego em processos de seleção ou recrutamento".[42]

Necessário pontuar que em recente decisão, nos autos de Agravo em Recurso Especial nº 2.130.619 – SP, o Superior Tribunal de Justiça (STJ), ao julgar pedido indenizatório em decorrência de vazamento de dados, entendeu que o predito artigo 5º, II, da LGPD traz um rol taxativo dos dados qualificáveis como sensíveis. Desse modo, afastou o enquadramento como dados sensíveis aos dados vazados, que correspondiam a dados básicos de qualificação da pessoa, fornecidos corriqueiramente em diversas situações do dia a dia.

> Processual Civil e Administrativo. Indenização por dano moral. Vazamento de dados pessoais. Dados comuns e sensíveis. Dano moral presumido. Impossibilidade. Necessidade de comprovação do dano.
> I - Trata-se, na origem, de ação de indenização ajuizada por particular contra concessionária de energia elétrica pleiteando indenização por danos morais decorrentes do vazamento e acesso, por terceiros, de dados pessoais.
> II - A sentença julgou os pedidos improcedentes, tendo a Corte Estadual reformulada para condenar a concessionária ao pagamento da indenização, ao fundamento de que se trata de dados pessoais de pessoa idosa.
> III - A tese de culpa exclusiva de terceiro não foi, em nenhum momento, abordada pelo Tribunal Estadual, mesmo após a oposição de embargos de declaração apontando a suposta omissão. Nesse contexto, incide, na hipótese, a Súmula n. 211/STJ. In casu, não há falar em prequestionamento ficto, previsão do art. 1.025 do Código de Processo Civil (CPC)/2015, isso porque, em conformidade com a jurisprudência do STJ, para sua incidência deve a parte ter alegado devidamente em suas razões recursais ofensa ao art. 1022 do CPC/2015, de modo a permitir sanar eventual omissão através de novo julgamento dos embargos de declaração, ou a análise da matéria tida por omissa diretamente por esta Corte. Tal não se verificou no presente feito. Precedente: AgInt no Resp 1737467/SC, Rel. Ministro Napoleão Nunes Maia Filho, Primeira Turma, julgado em 8/6/2020, Dje 17/6/2020.
> IV - O art. 5º, II, da LGPD, dispõe de forma expressa quais dados podem ser considerados sensíveis e, devido a essa condição, exigir tratamento diferenciado, previsto em artigos específicos. Os dados de natureza comum, pessoais mas não íntimos, passíveis apenas de identificação da pessoa natural não podem ser classificados como sensíveis.

[42] FRAZÃO. Ana. Nova LGPD: o tratamento dos dados pessoais sensíveis. A quinta parte de uma série sobre as repercussões para a atividade empresarial. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018. Acesso em 25 de novembro de 2022.

> V - O vazamento de dados pessoais, a despeito de se tratar de falha indesejável no tratamento de dados de pessoa natural por pessoa jurídica, não tem o condão, por si só, de gerar dano moral indenizável. Ou seja, o dano moral não é presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações.
> VI - Agravo conhecido e recurso especial parcialmente conhecido e, nessa parte, provido.
> (...)
> Já em relação a alegada ofensa ao art. 5º, II, da LGPD, constata-se assistir razão à concessionária recorrente a esse respeito, isso porque o referido dispositivo traz um rol taxativo daquilo que seriam dados pessoais sensíveis e, por ostentarem essa condição, exigem tratamento diferenciado, conforme previsão no art. 11 da mesma LGPD. Destaca-se do texto legal o seguinte.
> (AResp 2.130.619. Ministro Relator Francisco Falcão. Data do julgamento: 07/03/2023. Dje 10/03/2023. Sem grifos no original)

Ainda que seja uma decisão pontual sobre a natureza do rol dos dados sensíveis, trata-se de uma importante sinalização da Corte Superior pela taxatividade desse rol, o que agrega maior segurança no desenvolvimento de novos modelos de negócios que se valham de dados pessoais, evitando-se eventuais surpresas no sentido de que determinado dado estaria sujeito ao tratamento diferenciado do dado sensível.

No contexto do *open finance*, é comum deparar-se com afirmações genéricas de que os dados financeiros são dados sensíveis[43]. Contudo, sob a ótica da qualificadora jurídica de dado sensível e o recente posicionamento do STJ, os dados bancários e/ou financeiros, em geral, não mereceriam tal alcunha.

Em que pese o predito julgamento, centrado no conteúdo em si do dado pessoal, não se pode perder de vista o posicionamento doutrinário de que um dado isoladamente considerado não é parâmetro para aferir seu grau de sensibilidade. O enquadramento como dado sensível dá-se pelos efeitos de seu tratamento, a depender de seu uso e finalidade[44]. Desse modo, "um dado, em si, não é perigoso ou discriminatório, mas o uso que dele se faz, pode sê-lo"[45].

---

[43] Exemplos: "Dados financeiros são informações confidenciais e sensíveis, por isso investir em uma excelente segurança de dados é muito importante para que as pessoas possam ser protegidas." (https://www.bv.com.br/bv-inspira/open-banking/seguranca-de-dados. Acesso em 01 de julho de 2023). "O Open Finance é seguro? Sim, o Open Finance é seguro. Esse é um ponto essencial porque a iniciativa digital foi criada para facilitar e padronizar a troca de dados sensíveis entre instituições financeiras, de maneira criptografada e mantendo o sigilo bancário e a confidencialidade. Isto é possível graças às APIs (interfaces de programação de aplicações) e aos ambientes desenvolvidos pelas instituições financeiras com múltiplas camadas de proteção e dentro de padrões globais de cibersegurança. (https://www.serasaexperian.com.br/conteudos/open-finance/mas-afinal-e-open-banking-ou-open-finance/. Acesso em 01 de julho de 2023).

[44] MULHOLLAND. Caitlin. Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (lei 13.709/2018). Disponível em: https://www.jur.puc-rio.br/wp-content/uploads/2021/07/IBERC_Responsabilidade-civil-e-dados-sensi%CC%81veis.pdf. Acesso em 03 de setembro de 2023.

[45] DONEDA, Danilo. Da Privacidade à Proteção de dados pessoais: Fundamentos da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters, 2020.

A prevalência de referido entendimento enseja o alargamento da esfera de dados potencialmente enquadráveis como sensíveis, e, portanto, sujeitos à critérios mais rígidos para o consentimento e tratamento de dados (diferentes daqueles incidentes nos dados pessoais em geral e, em larga medida, replicados na regulação do *open finance*), o que gera relevante repercussão, de caráter restritivo, ao tratamento de dados pessoais no *open finance*, tendo em vista, especialmente, os riscos de eventuais vieses discriminatórios em sede de perfilamento, conforme se demonstrará adiante.

Reforce-se, nesse aspecto, que o *open finance* abrange dados não apenas bancários, mas também dados referentes a produtos e serviços das searas previdenciária e securitária, o que alarga ainda mais o campo de incidência de potenciais vieses discriminatórios, ainda que no tratamento de dados, a princípio, não elencados no rol dos dados sensíveis. Nesse cenário, dados de saúde disponibilizados na contratação de um seguro têm o condão de, potencialmente, resultarem em tratamento discriminatório, ainda que referido dado não esteja no rol dos dados sensíveis preconizado pela Lei. Tal situaçao reforça posição doutrinária de que a aferição dos aspectos sensíveis dos dados, em larga medida, decorre muito mais do uso que será feito deles do que dos dados em si, previamente elencados no artigo legal.

O dado anonimizado, em contraponto aos dados supramencionados, é o dado pessoal ou sensível que, pelo emprego de meios técnicos razoáveis, resta dissociado de seu titular, porém, é apto a gerar informações sobre perfis de usuários.

Conquanto a distinção conceitual do dado anonimizado permita inferir sua exclusão à tutela conferida pela LGPD, o artigo 12 de referida Lei explícita tal aspecto, referendado pela doutrina:

> "O conceito de dados pessoais é um elemento central para que se aperfeiçoe a normatização sob análise, na medida em que se estabelecem os limites da própria tutela jurídica em questão. Em outras palavras, um dado que não avoque tal qualidade não poderia ser cogitado como um prolongamento da pessoa por lhe faltar tal centro de imputação."[46]

Outrossim, tendo em vista a adoção do conceito expansionista de dados pessoais e a célere evolução tecnológica dos dias atuais, a mera dicotomia conceitual não se mostra suficiente para evitar debates sobre a reversibilidade da anonimização e, por conseguinte, sua submissão aos preceitos protetivos a que se sujeitam os dados pessoais.

[46] BIONI. Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2ª ed. Rio de Janeiro. Forense. 2019. p.67-68.

Na busca de solucionar tal aspecto, o artigo 12 §1º da LGPD adotou um perímetro de elasticidade do conceito, ao impor um filtro de razoabilidade na análise da anonimização dos dados e sua potencialidade de conversão em dados identificáveis, cujos parâmetros são a tecnologia existente e razoabilidade de custo e tempo para a reversão.

Desse modo, o dado será considerado anonimizado à luz da tecnologia existente à época do procedimento de anonimização e do custo e tempo exigidos para sua reversão.

A fixação de parâmetros para definir o dado anonimizado tem por escopo evitar eventual incongruência do próprio texto legislativo, dada a adoção do conceito expansionista, na medida em que os dados anonimizados são, em última análise, também dados relacionados à uma pessoa potencialmente identificável (sobretudo mediante desenvolvimento de novas ferramentas e tecnologias, cuja evolução ocorre numa rapidez nunca antes percebida e dificilmente mapeável)[47].

Ao mesmo tempo, a definição de parâmetros compatibiliza a tutela jurídica dos dados pessoais ao contexto da sociedade da informação e ao fomento à inovação, que são fortemente dependentes de ferramentas lastreadas em *Big Data* e *Big Analytics*, cujo uso seria potencialmente restringido por eventual óbice à utilização dos dados anonimizados[48].

Dada a pertinência com o setor financeiro e especificamente ao *open finance*, necessário evidenciar o entendimento que o princípio da autodeterminação informativa protege também o livre desenvolvimento da personalidade, de modo que tratamentos que interfiram na construção da personalidade do titular de dados são atraídos para o arcabouço jurídico da proteção de dados pessoais, ainda que se valham de dados anonimizados na construção de perfis.

Interpreta-se que referido entendimento está prestigiado pelo artigo 12 §2º da LGPD[49], ao definir que dados utilizados na construção de perfis de grupos de usuários podem ser considerados dados pessoais, visão que repercute, em especial, nas análises automatizadas de concessão de crédito e no desenvolvimento de novos modelos de negócios no *open finance,* fortemente dependentes de perfilamento.

> "De maneira bastante sintética, esse é o pano de fundo do debate em torno da agenda de regulação de algoritmos e de inteligência artificial. O desafio está em arquitetar processos de governança que impeçam a ocorrência de efeitos indesejados ao se introjetar tais tecnologias nos circuitos decisórios do nosso cotidiano.

---

[47] BIONI. Bruno Ricardo. Op. Cit. p.75.

[48] FRAZÃO. Ana. A nova Lei Geral de Proteção de Dados. Repercussões para a atividade empresarial: o alcance da LGPD. Parte II. Disponível em: http://anafrazao.com.br/files/publicacoes/2018-09-05-A_nova_Lei_Geral_de_Protecao_de_Dados_Repercussoes_para_a_atividade_empresarial_o_alcance_da_LGPD_Parte_II.pdf. Acesso em 25 de novembro de 2022.

[49] Artigo 12 §2º da LGPD: Poderão ser igualmente considerados como dados pessoais, para fins desta Lei, aqueles utilizados para a formação de perfil comportamental de determinada pessoa natural, se identificada.

> Leis de proteção de dados pessoais compõem necessariamente esse arranjo de governança, na medida em que suas normas abraçam todo e qualquer processamento de dados que sujeito um indivíduo ou uma coletividade a uma decisão automatizada. Pouco importa se tal tratamento se centra em uma informação isolada ou agregada e que não revele uma pessoa direta ou indiretamente (dados anonimizados), desde que ele impacte a sua vida e, portanto, o livre desenvolvimento da personalidade."[50]

Algoritmos desenvolvidos com base em dados anonimizados também podem ensejar conclusões discriminatórias à determinado perfil de usuário e, portanto, repercutir na esfera dos direitos de personalidade. Note-se que a celeuma não é o uso em si do dado anonimizado, que, em regra, afasta a incidência da LGPD, mas a aplicação da construção algorítmica no caso concreto de tratamento do dado pessoal.

Diante da delicadeza do tema, a doutrina já apresenta as linhas gerais para o tratamento de dados anonimizados, aspectos que devem nortear, desde já, a utilização de tais dados, com vistas a evidenciar a observância do parâmetro legal da não reversibilidade, à luz da tecnologia existente por ocasião da anonimização:

> "Sendo assim, é importante que o método escolhido pela instituição como processo de anonimização possa demonstrar que impossibilita a sua reversão para aquele que recepcionou o dado classificado como anonimizado, evitando riscos para uma responsabilização futura, ainda mais em discussões em sede judicial de Juizado Especial, com debate de tema consumerista que não permite necessariamente a condução de perícia técnica adequada para o nível de complexidade que a matéria exige. Provavelmente será necessário evoluir para o uso de soluções certificadas para evitar discussões e incertezas na aplicação de soluções de anonimização."[51]

Os dados anonimizados não são, portanto, a chave de ouro para a conformidade legal, sendo juridicamente sensato o estabelecimento cauteloso de limites objetivos e rígidos no uso de inteligência analítica no tratamento de dados anonimizados, evidenciando o perímetro de elasticidade de não incidência da LGPD, para afastar eventuais entendimentos pela violação à proteção de dados pessoais.

Definido o objeto da tutela jurídica, o próximo passo é delimitar as atividades abrangidas, o que convencionou-se denominar de "tratamento de dados pessoais", cujo conceito está previsto no artigo 5º, X da LGPD, em redação muito similar ao artigo 14, II do Regulamento ao Marco Civil da Internet (Decreto nº)[52], nos seguintes termos:

---

[50]BIONI. Bruno Ricardo. op.cit p. 79

[51] Ibidem. p. 82

[52] Artigo 14, II do Decreto 8.771/2016. Para os fins do disposto neste Decreto, considera-se: II - tratamento de dados pessoais - toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento,

> Art. 5º Para os fins desta Lei, considera-se:
> (...)
> 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;

Trata-se de um rol exemplificativo de larga abrangência do conceito aberto de tratamento de dados pessoais, de tal sorte que a proteção conferida alcança toda e qualquer inteiração a que os dados pessoais possam ser submetidos.

Tendo em vista que o cerne do *open finance* é o compartilhamento de dados entre as Instituições Financeiras Participantes, singelo concluir o enquadramento de referida atividade no conceito legal de tratamento de dados pessoais.

A LGDP define, ainda, em seu artigo 7º[53], as hipóteses em que o tratamento de dados pessoais é legalmente permitido.

---

arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

[53] Art. 7º da Lei 13.709/18: 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;

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 Nos casos de aplicação do disposto nos incisos II e III do *caput* deste artigo e excetuadas as hipóteses previstas no art. 4º desta Lei, o titular será informado das hipóteses em que será admitido o tratamento de seus dados.

§ 2º A forma de disponibilização das informações previstas no § 1º e no inciso I do *caput* do art. 23 desta Lei poderá ser especificada pela autoridade nacional.

§ 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.

Ao perquirir sobre o supracitado artigo7º, a doutrina condensou em 10 (dez) hipóteses de tratamento de dados pessoais, sem qualquer hierarquia entre elas[54] e convencionou chamá-las de "bases legais para o tratamento de dados pessoais".

As bases legais para o tratamento de dados pessoais são as hipóteses definidas em lei que autorizam tal tratamento, de modo que toda atividade de tratamento de dados deve ser precedida da prévia subsunção à uma das bases legais definidas.

Em que pese divergências meramente terminológicas, extrai-se as seguintes bases legais para o tratamento de dados pessoais:

1) o consentimento;

2) o cumprimento de obrigação legal;

3) a execução de políticas públicas;

4) estudos por órgãos de pesquisa;

5) execução de contratos e diligências pré-contratuais;

6) exercício regular de direitos;

7) proteção da vida;

8) tutela da saúde;

9) interesses legítimos do controlador ou terceiro;

10) proteção ao crédito.

Conquanto detalhado adiante, consigna-se, desde já, o entendimento de que todas as bases legais são potencialmente elegíveis ao *open finance*, sob a ótica da proteção de dados e ressalvados os limites impostos pela Lei do Sigilo Bancário, o que justifica a preferência pela base legal do consentimento, curvando-se a regulação aos ditames legais, em observância à hierarquia das normas.

Outrossim, para que não se disperse do objetivo deste estudo e dada a maior relevância, dedicar-se-á maior atenção ao consentimento, dado seu protagonismo na regulação do *open finance*.

[54] Enunciado 4889 aprovado na IX Jornada de Direito Civil: *não há hierarquia entre as hipóteses legais previstas na LGPD, inclusive entre aquelas que respaldam o tratamento de dados pessoais sensíveis*

2.1.1 Base legal do consentimento

O consentimento, elemento volitivo do titular acerca do tratamento de seus dados pessoais, permeia, com relevante proeminência, toda a evolução geracional das leis de proteção de dados pessoais, notadamente sob a égide do princípio da autodeterminação informativa.

Adiantando-se sobre o regime jurídico adotado no *open finance*, imperioso já pontuar a adoção do consentimento também como base legal protagonista no compartilhamento de dados no sistema financeiro aberto, razão pela qual o consentimento, sob a ótica da proteção de dados merece especial atenção nas linhas a seguir, com vistas a viabilizar o oportuno cotejo.

Embora em uma primeira e superficial análise do sistema protetivo dos dados, a relevância da conceituação da base legal do consentimento não salte aos olhos do intérprete (afinal, dentre tantos conceitos novos e carentes de uma construção hermenêutica, o consentimento passa ao largo de ser instituto desconhecido na seara do direito), necessário pontuar que importantes discussões acerca de seu alcance foram travadas tanto na seara contratualista[55] como na seara da seara da proteção de dados.

"Consentimento é um típico elemento de direito contratual. (...) E, essa mesma autonomia é captada e transportada para a proteção dos dados pessoais, na medida em que é o próprio cidadão quem deve governar seus dados pessoais"[56], premissa que corresponde ao cerne do princípio da autodeterminação informativa.

Na seara da evolução histórica da proteção de dados pessoais, dividida em quatro fases geracionais, o consentimento sempre permeou as leis sobre o tema, porém ganha maior relevância na terceira geração, nascedouro dos contornos preambulares da autodeterminação

---

[55] O consentimento encontra-se na gênese dos contratos, dando azo ao elemento da livre manifestação da vontade pelos contratantes, cuja inspiração remonta as ideias do liberalismo e racionalismo dos séculos XVIII e XIX. Conquanto persista a essencialidade do consentimento, as desigualdades entre as partes infirmaram o caráter absoluto da livre manifestação da vontade e ensejaram uma revisita ao instituto e aos preceitos da liberdade contratual e liberdade de contratar.

Neste curso histórico vislumbra-se a relevância do consentimento à formação do contrato, o que levou, por exemplo, a teoria normativista a defender que os contratos de adesão não teriam natureza contratual, mas seriam sim um ato unilateral, na medida em que viciadas as manifestações de vontade dos hipossuficientes. Superada tal teoria, os contratos de adesão hoje revestem-se de natureza contratual, reconhecendo-se a inexistência da liberdade contratual e a mitigada liberdade de contratar, o que atrai a incidência do dirigismo estatal para relações desta espécie. O percurso histórico do consentimento e a possibilidade do dirigismo estatal em relações consentidas pela manifestação livre da vontade, tal qual nos contratos de adesão citados à guisa de exemplo, tenha muito a contribuir para a seara da proteção de dados, porém, há elementos específicos deste novo arcabouço jurídico que desafiam uma nova hermenêutica jurídica.

56 BIONDI. Bruno. Xeque-Mate: o tripé de proteção aos dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. São Paulo: GPoPAI/USP, 2015. Disponível em: https://www.academia.edu/28752561/Xeque_Mate_o_trip%C3%A9_de_prote%C3%A7%C3%A3o_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil. Acesso em: 27 de novembro de 2022.

informativa e cujo signo é a decisão da Corte Constitucional alemã pela inconstitucionalidade parcial da Lei do Censo de 1983.

Apesar do percurso histórico do consentimento nas leis sobre proteção de dados pessoais, visto como uma carta coringa regulatória num cenário de elevado grau de complexidade para se modelar a atividade de tratamento de dados pessoais, seu protagonismo não se traduz em pacificação jurídica a respeito do tema, notadamente em face dos novos modelos de negócios impulsionados pela economia digital[57].

> "(...) ainda que se considere o riquíssimo e fundamental conceito cunhado em 1983 pelo Tribunal Constitucional Alemão, é efetivamente em torno do conceito de consentimento que é possível medir e articular uma comparação minimamente relevante entre os diversos marcos regulatórios sobre proteção de dados – inclusive aqueles que não são dotados de uma regulamentação central e uniforme. Ao mesmo tempo, parcela considerável das discussões relacionadas a proteção de dados toca em território direta ou indiretamente ligado ao consentimento, seja Big Data ou inteligência artificial, os mecanismos de vigilância, as implicações de SmartCities e tantos outros". [58]

A transposição de uma tutela individual, preconizada pela terceira geração, para uma tutela coletiva dos dados pessoais, defendida na quarta fase geracional (na qual insere-se as atuais Leis sobre o tema, tais como a LGPD e o GDPR), não repercutiu na perda do protagonismo do consentimento.

Assim, apesar da quarta geração de leis sobre proteção de dados pessoais propor a superação da centralidade do indivíduo para a consagração de uma tutela coletiva, o que repercute na relativização do consentimento individual, este continua exercendo um papel central no arcabouço jurídico aplicável à espécie.

À guisa de exemplo, veja-se sua adoção como base principal no *open finance* e das orientações emanadas pela Autoridade Nacional de Proteção de Dados (ANPD), como o Guia Orientativo - Cookies e Proteção de Dados[59], que restringe a não obtenção do consentimento apenas para os cookies necessários, aqueles destinados a coleta de dados essenciais ao funcionamento da página eletrônica ou à prestação do serviço.

Todo o prestígio historicamente atribuído ao consentimento não o isenta de severas críticas tecidas pela doutrina hodierna, em larga medida decorrentes, justamente, dessa

---

[57] BIONI. Bruno Ricardo. Xeque-Mate: O tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasi. GpoPai/USP – Grupo de Pesquisa em Políticas Públicas para acesso à informação. São Paulo. 02.07.2015. Disponível em: http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf. Acesso em 17 de dezembro de 2022.

[58] DONEDA. Danilo. Prefácio da obra Proteção de dados pessoais. A função e os limites do consentimento. p. XIV.

[59] Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf. Acesso em 27 de novembro de 2022.

exigência padrão pelo consentimento em um contexto de sociedade informacional, com preponderância do uso de BigData e desenvolvimento de novos tecnologias numa velocidade sem precedentes, o que enseja uma sobrecarga de transações de consentimento, o que convencionou-se denominar fadiga do consentimento.

Referida preocupação foi, inclusive, externalizada nas Diretrizes 05/2020 relativas ao consentimento na acepção do Regulamento 2016/67, elaboradas pelo European Data Protection Board (EDPB)[60].

A recorrência no uso do consentimento repercute num excesso de transações de consentimento, excesso de informação e inexistência de escolha significativa[61], o que deslegitima o instituto e os esforços, inclusive estatais, em prol da proteção dos dados pessoais:

> Esse conjunto de características permite caracterizar esse consentimento, se o cotejarmos com a função que dele se pretende, qual seja a de ser um instrumento para a livre construção da esfera privada, "uma ficção". Sua utilização pode ser instrumentalizada pelos interesses que pretendem que seja não mais que uma via para legitimar a inserção dos dados pessoais no mercado. Por outro lado, o consentimento pode ser incentivado pelo próprio Estado sob a (falsa) premissa de conceder aos cidadãos um instrumento forte e absoluto para determinar livremente a utilização de seus próprios dados pessoais – conforme observou Stefano Rodotà, o Estado assim teria um falso álibi para não intervir em uma situação na qual deveria agir positivamente na defesa de direitos fundamentais – e, assim, "lavar as mãos".[62]

Em que pese as devidas ressalvas à hipervalorização da base legal do consentimento e a perspectiva de sua relativização ante os novos modelos de negócios e os vieses interpretativos preconizados pela quarta geração de leis sobre a matéria, imperioso adentrar aos aspectos conceituais do instituto, sob o qual escora-se o *open finance*.

Isto porque, "tal como na seara contratual em que o consentimento pode se vestir de várias roupagens, não é diferente quanto à proteção de dados pessoais."[63]

As leis sobre proteção de dados pessoais conferem elevada carga de adjetivação ao consentimento, objetivando bem delimitá-lo.

---

[60] Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pt.pdf. Acesso em 30 de julho de 2023.

[61] SCHERMER, Bart et al. The Crisis of Consent: how stronger legal protection may lead to weaker consent in data protection. Ethics and Information Technology, 2014, vol. 16: 171-182. Disponível em: Disponível em: https://ssrn.com/abstract=2412418 ou http://dx.doi.org/10.2139/ssrn.2412418. Acesso em 30 de julho de 2023.

[62] DONEDA, Danilo. Da Privacidade à Proteção de dados pessoais: Fundamentos da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters, 2020. p. 294

[63] BIONI. Bruno Ricardo. Xeque-Mate: O tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasi. GpoPai/USP – Grupo de Pesquisa em Políticas Públicas para acesso à informação. São Paulo. 02.07.2015. Disponível em: http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf. Acesso em 17 de dezembro de 2022.

O GDPR, por exemplo, o adjetiva como “livre”, “específico”, “informado”, “explícito” e “inequívoco”. Da mesma sorte, a LGPD emprega adjetivos similares em seu artigo 5º, XII.

O consentimento do titular dos dados pessoais, na definição da LGPD, é a “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”[64], sem forma pré-determinada pela lei.

“Livre”, em sua concepção mínima, refere-se a voluntariedade do ato, obtido espontaneamente, sem coação física ou moral. Merece especial atenção nas hipóteses de assimetria de poder, a exemplo das relações laborais ou centradas da premissa do take-it ou leave-it (pegar ou largar).

O conceito de consentimento livre tem evoluído para uma interpretação de consentimento granular, a ser outorgado de forma fragmentada, com vistas a mitigar a força coercitiva da lógica binária do pegar ou largar. Assim, o consentimento é escalonado de maneira gradual e correlata ao fluxo de dados, viabilizando o acesso ao serviço e/ou produto pretendido pelo cliente.

Por “informado” entende-se a divulgação de informações suficientes à tomada de decisão pelo titular dos dados, permitindo-lhe a integral compreensão do ato, seus riscos e seus efeitos.

“Inequívoco” corresponde a externalização expressa do consentimento, o que afasta a ideia de consentimento implícito ou tácito. Aqui não há exigência de forma, mas sim de um ato indene de dúvidas, uma certeza sobre a outorga do consentimento, independente da forma.

Finalidade determinada, por sua vez, obsta consentimento genérico. Faz-se necessário demonstrar o “para que” o dado pessoal será tratado, sem, contudo, exigir uma pormenorização técnica.

Veja-se que os qualificadores ao consentimento buscam delimitar sua obtenção não sob aspectos formais (escrito ou verbal), mas prestigiando elementos que explicitem o nível de interação e conhecimento do titular ao autorizar o tratamento de seus dados.

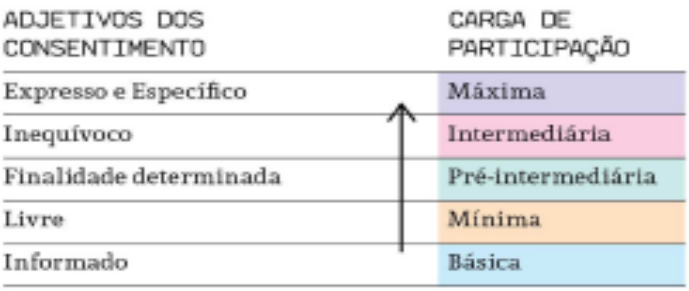
Nesse espectro, Bruno Ricardo Bioni propõe a sistematização abaixo, adotando uma escala progressiva da adjetivação do consentimento de acordo com a carga participativa do titular dos dados pessoais:[65]

---

[64] Artigo 5º, XII da Lei 13.709/2018.

[65] BIONI. Bruno Ricardo. Xeque-Mate: O tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasi. GpoPai/USP – Grupo de Pesquisa em Políticas Públicas para acesso à informação. São Paulo. 02.07.2015. p. 46. Disponível em: http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf. Acesso em 17 de dezembro de 2022.

Figura 1 – Escala progressiva da adjetivação do consentimento



Fonte: BIONI. Bruno Ricardo, 2015.

Especificamente na legislação pátria, a importância do consentimento não se esgota em sua elevada carga de adjetivação. O consentimento é ainda detalhado pela LGPD e a ele é feita menção mais de 35 (trinta e cinco) vezes em todo o texto legal.

A interpretação sistemática do novo arcabouço jurídico, especialmente à luz de sua elevada carga principiológica, permite inferir a adoção do consentimento como sua espinha dorsal.

O próprio conceito de consentimento, com suas fortes qualificadoras, demonstra seu amoldamento ao princípio da finalidade, o qual preconiza que os propósitos do tratamento de dados sejam legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades, correlação reforçada pelo artigo 8º § 4º da lei em comento.[66]

Sob a égide do princípio da transparência, do livre acesso e da prestação de contas, o consentimento é balizado pelos ditames do artigo 9º da Lei Geral de Proteção de Dados[67], além de reforçada a finalidade específica do tratamento.

---

[66] Lei 13.708/19. 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. (...) § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

[67] Lei 13.708/19. 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;

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.

No mesmo sentido, o caráter inequívoco do consentimento exige a observância, e em caso de judicialização, da prova de atos positivos ao consentimento emanados pelo titular dos dados pessoais. Porém, não está relacionado a nenhuma obrigatoriedade de este dar-se por escrito, na medida em que o texto do supracitado artigo 8º da Lei nº 13.708/19 autoriza a manifestação da *vontade por escrito ou por outro meio*.

Não obstante o provável posicionamento da jurisprudência favoravel à inversão do ônus da prova fundamentado no Código de Defesa do Consumidor (CDC) em eventuais litígios entre usuários e as instituições participantes sobre proteção de dados pessoais no segmento bancário e especificamente no *open finance*, cabe consignar que referida celeuma mostra-se inócua, na medida em que o artigo 8º, §2º atribui, explicitamente, o ônus probatório sobre o consentimento ao controlador dos dados.

Ademais, em que pese o protagonismo histórico do consentimento nas leis sobre proteção de dados pessoais e o atual protagonismo na regulação do *open finance*, imperioso destacar que o consentimento, por si só, não tem o condão de permitir todo e qualquer tratamento de dados pessoais, aspecto que merece especial atenção no desenho regulatório do *open finance*.

O direito à proteção de dados pessoais, inserto na seara dos direitos da personalidade, sujeita-se aos limites da autonomia privada esculpidos no Código Civil, com especial destaque para a irrenunciabilidade e intransmissibilidade previstos no artigo 11 do referido diploma legal, conforme ponderações de Bruno Ricardo Bioni:

> "A negociabilidade dos direitos da personalidade cinge-se à fruição de tais bens (latu sensu) e, não, propriamente, à sua titularidde (stricto sensu), de acordo com a intelecção dos vocábulos "intransmissibilidade" e "irrenunciabilidade" contidos no artigo 11 do Código Civil. A limitação voluntária dos direitos da personalidade é admitida em uma perspectiva de disponibilidade relativa por seu titular. No entanto, o grande desafio é parametrizar qual deve ser o sentido dessa liberdade, notadamente, quais são os limites impostos a tal esfera de autonomia relativa.
> (...)
> Zonas de autonomia devem ser esculpidas, levando-se em conta parâmetros que não esvaziem o valor social que a proteção de dados pessoais tem a cumprir. Deve-se verificar em que medida o fluxo informacional é (in)apropriado para garantir o engajamento social, notadamente se ele

§ 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.

> estabelece uma excessiva interferência ao livre desenvolvimento da personalidade do titular das informações pessoais em circulação."[68]

Diante das incertezas no contexto da proteção de dados, novamente o consentimento tem seu espectro de atuação restringido ante a critérios interpretativos ainda em construção, para os quais propõe-se, no desenvolvimento dos modelos negociais, o norteamento pelos qualificadores do consentimento e os princípios da transparência, finalidade e adequação do tratamento de dados.

A interpretação sistemática do novo arcabouço jurídico, especialmente à luz de sua elevada carga principiológica, impõe a compatibilização da base legal do consentimento, outorgada de modo individual pelo titular dos dados, com as demais diretrizes que norteiam a proteção de dados pessoais, alçada a condição de direito fundamental[69], bem como à sua tutela coletiva.

Desse modo, as qualificadoras do consentimento constrõem o amoldamento desta base legal aos princípios da transparência, da especificação de propósitos, de acesso e qualidade de dados, adequação e necessidade e da prestação de contas, de modo a reforçar que os propósitos do tratamento de dados sejam legítimos, específicos, explícitos e informados ao titular, inclusive quanto a forma e duração do tratamento, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

A única exceção prevista quanto aos preditos princípios, capaz de limitar especialmente o dever de informar, remonta ao segredo comercial ou industrial, conforme artigo 9º, II da Lei 13.709/18, o que enseja caloroso debate no sentido de enquadrar os algoritmos e a inteligência analítica em tal excepcionalidade.

Desse modo, os modelos negociais escorados no segredo comercial revestem-se do risco de serem vistos como potenciais afrontas à proteção dos dados pessoais, o que merece ser sopesado com extrema cautela nos modelos de negócios originados pelo *open finance*.

Outro ponto de atenção refere-se às nuances do consentimento em condições de assimetria entre as partes, sobretudo em face da omissão da LGPD sobre o tema, o escasso enfrentamento da matéria pelas legislações paradigmas e a tradição protecionista do Judiciário brasileiro.

---

[68] BIONI. Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro. Forense. 2019. p.220-222.

[69] Artigo 5º, LXXIX da Constituição Federal: É assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. (Incluído pela Emenda Constitucional nº 115 de 2020).

Na seara consumerista, o crescente tratamento dos dados pessoais pelas empresas deu ensejo a expressão "consumidor de vidro"[70] e, hodiernamente, sob a ótica do protagonismo do consentimento, argumenta-se por um agravamento da vulnerabilidade do consumidor, centrada na dimensão algorítmica e informacional, dado o cenário de obtenção de consentimento involuntário (ou irrefletido) do consumidor para a coleta indevida e utilização mercadológica de seus dados pessoais[71].

Nesse cenário, a doutrina já apresenta teses protetivas aos hipossuficientes nas relações de consumo e trabalhista, aplicáveis em especial quanto ao consentimento e maiores cautelas na aferição de sua obtenção de forma efetivamente livre e bem-informada[72], preceitos os quais têm o condão de balizar eventuais litígios entre usuários e instituições participantes do *open finance.*

De todo o escorço, tem-se que o consentimento, ainda que mantido o seu status de protagonista, deverá ser interpretado pelo viés coletivo da quarta fase geracional da proteção de dados pessoais, o que enseja matizes hermenêuticas obstativas a que referida base legal seja o verniz capaz de autorizar todo e qualquer tratamento de dados pessoais.

Assim, além da observância dos requisitos legais para o consentimento, a tutela coletiva do consentimento, notadamente nas relações assimétricas, apresenta o condão de suscitar debates acerca da voluntariedade na outorga do consentimento.

Conclui-se, portanto, que o consentimento a ser obtido pelos modelos negociais aderentes à proteção de dados pessoais vai além da conhecida manifestação livre da vontade e dos requisitos formais de cláusulas gerais destacadas do contrato e possibilidade de revogação do consentimento, a qualquer momento.

A interpretação a respeito do consentimento está sujeita à evolução de um dirigismo estatal e de sua judicialização, cujas linhas norteadoras de eventual posicionamento jurisprudencial ainda estão em construção.

Não se pode, contudo, diante deste cenário, perder de vista a necessidade de que o consentimento deve atender as qualificações constantes de seu conceito legal e da observância por toda a estrutura do negócio quanto ao zelo pelos princípios do sistema protetivo, em especial

---

[70] LACE, Susane. The Glass Consumer: life in a surveillance society. Bristol. Policy Press. 2005.

[71] OLIVEIRA. Lis Arrais e VERBICARO. Dennis. A vulnerabilidade algorítimica do consumidor: a extração e o compartillhamento de dados pessoais nas relações de consumo digitais. In: Direito do Consumidor e Novas Tecnologias. Coord. Marcos Ehrhardt Júnior, Marcos Catalan, Pablo Malheiros. Belo Horizonte. Editora Foco. 2021.p. 45-46.

[72] FRAZÃO. ANA. Nova LGPD: A importância do consentimento para o tratamento de dados pessoais. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-a-importancia-do-consentimento-para-o-tratamento-dos-dados-pessoais-12092018. Acesso em 26 de junho de 2022.

transparência, finalidade, prestação de contas e adequação, como postura mitigadora de alegações quanto à eventual vício volitivo.

2.1.2 Consentimento no *open finance*

Apresentadas as diretrizes do consentimento, como base legal para o tratamento de dados pessoais, especialmente sob a ótica da LGPD, mister avançar para o consentimento preconizado na regulação do *open finance* e o devido cotejo.

Os dados pessoais submetidos à guarda das Instituições Financeiras e, em especial, os dados transacionais bancários estavam (e ainda estão) sujeitos aos rigorosos ditames do sigilo bancário, preconizado pela Lei Complementar 105/2001 e pelas correlatas Regras de Segurança Cibernética, consubstanciadas, em síntese, pela Resolução CMN nº 4.893/2021 e Resolução BCB nº 85/2021, esta especifica às instituição de pagamento.

O sigilo bancário, historicamente, caracteriza-se como uma "obrigação do banqueiro – a benefício do cliente – de não revelar certos fatos, atos, cifras ou outras informações de que teve conhecimento por ocasião do exercício de sua atividade bancária e notadamente aqueles que concernem a seu cliente, sob pena de sanções muito rigorosas, civis, penais ou disciplinares"[73].

Nesse contexto, os esforços necessários ao cumprimento das normas sobre sigilo bancário forjaram uma cultura de que os dados dos clientes bancários pertenceriam às Instituições Financeiras, fazendo-as atuar como titulares de tais dados, centralizando o uso, exclusivamente, para si.

Assim, as instituições financeiras detinham, até então, o controle dos dados de seus clientes, desde os dados cadastrais até perfil creditício e de consumo, com compartilhamento apena pontual e direcionado de informações, a exemplo do Sistema de Informações de Crédito (SCR) do Banco Central e do cadastro positivo.

Por outro lado, o *open finance* autoriza o compartilhamento dos dados pessoais entre as Instituições Participantes, mediante o prévio consentimento de seu titular, conforme artigo 10 da Resolução Conjunta do Banco Central[74].

---

[73] Tradução livre do original: "Obrigation faite au banquier – et beneficiant au chent – de ne pas reveler certains faits, actes, chiffres ou autres informations don il a eu connaissance à l'exercice de son activité bancaire et notamument ceux qui concernent son client, sous peine de sanctions très rigoreuses d'ordre divers, civiles, pénales et disciplinaires". (FARHAT. Raymond. Le Secret Bancaire: étude de droit comparé. France. Suisse, Liban. Paris. Librairie Genérale de Droit et de Jurisprudence.1980. p. 256)

[74] Artigo 10 da Resolução Conjunta nº 1 do Banco Central: A instituição receptora de dados ou iniciadora de transação de pagamento, previamente ao compartilhamento de que trata esta Resolução Conjunta, deve identificar o cliente e obter o seu consentimento.

O consentimento, no *open finance*, é definido 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 de serviços para finalidades determinadas[75].

A adoção de uma hipótese legal específica para o tratamento de dados pessoais – o consentimento - denota, à primeira vista, uma aderência aos atuais preceitos de proteção de dados pessoais, em especial ao princípio da autodeterminação informativa, colocando o titular dos dados pessoais como protagonista, atribuindo-lhe o direito de decidir a respeito do tratamento de seus próprios dados, em contraposição à cultura até então vigente, além de replicar as qualificadoras ao consentimento previstas na LPGD.

Por obediência à hierarquia das normas, a regulação do *open finance*, ainda que tenha por escopo perseguir os objetivos propostos com a sua implementação[76], não pode se afastar da observância à LGPD, preocupação identificada no posicionamento do Banco Central do Brasil (Bacen).

> "É importante ressaltar que o Open Banking está em linha com a edição da Lei de Proteção de Dados Pessoais (LGPD), que criou o marco legal para o tratamento dos dados da pessoa natural, e parte do princípio de que os dados bancários pertencem aos clientes e não às instituições financeiras. Dessa forma, desde que autorizadas pelos clientes, as instituições financeiras compartilharão dados, produtos e serviços com outras instituições, por meio de abertura e integração de plataformas e infraestruturas de tecnologia, de forma segura, ágil e conveniente"[77].

Desde os estudos embrionários para o desenvolvimento do *open finance* desenvolvidos entre Banco Central e Federação Nacional dos Bancos (Febraban), o consentimento para o compartilhamento dos dados pessoais recebeu especial atenção, inclusive com a designação de um grupo temático específico, denomiado "Grupo 1 - Modelo de Autenticação e Consentimento".

---

[75] Artigo 2, VII da Resolução Conjunta nº 1 do Banco Central.

[76] Comunicado 33.455 do Banco Central. (...) 2. Essa iniciativa [open banking] tem como objetivo aumentar a eficiência no mercado de crédito e de pagamentos no Brasil, mediante a promoção de ambiente de negócio mais inclusivo e competitivo, preservando a segurança do sistema financeiro e a proteção dos consumidores.

Artigo 3º da Resolução Conjunta nº 1 do Banco Central: Constituem objetivos do Open Finance:

I - incentivar a inovação;

II - promover a concorrência;

III - aumentar a eficiência do Sistema Financeiro Nacional e do Sistema de Pagamentos Brasileiro;

IV - promover a cidadania financeira.

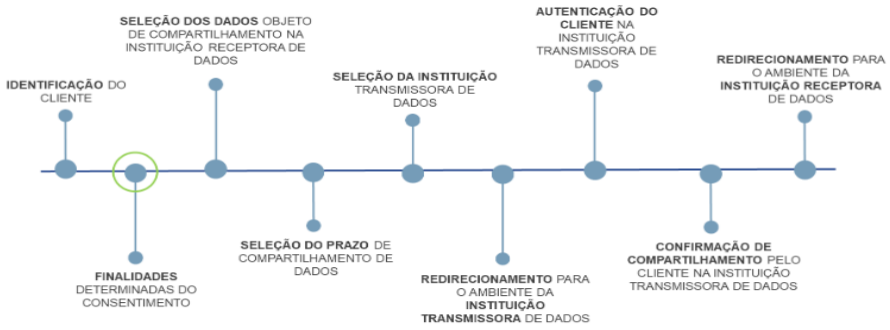
[77] NETO. Roberto Campos. Apontamentos do Presidente do Banco Central do Brasil, Roberto Campos Neto. Workshop sobre Open banking. Maio/19. Disponível em *https://www.bcb.gov.br/conteudo/home-ptbr/TextosApresentacoes/Apontamentos%20do%20Presidente_Open%20Banking%20v1.pdf*. Acesso em 20 de outubro de 2022.

A Febraban, no exercício de suas atribuições na seara da autorregulação bancária, publicou o Normativo de Proteção de Dados, com a definição das boas práticas a serem observadas pelas Instituições Financeiras na proteção dos dados pessoais, em todas as suas atividades.

No que tange ao open finance, prestigia-se a base legal do consentimento como o cerne autorizativo do compartilhamento dos dados.

Operacionalmente, tal compartilhamento é estruturado em três etapas sucessivas, ininterruptas e realizada, exclusivamente, por meios eletrônicos: (i) consentimento do cliente; (ii) autenticação, e (iii) confirmação, bem detalhadas na figura abaixo:

Figura 2 – Fluxo operacional do consentimento



Fonte: BNDES, 2023.

A obtenção do consentimento de forma válida, que corresponde ao cumprimento adequado da primeira etapa e é o cerne da interlocução entre o titular dos dados e a Instituição receptora, deve observar os requisitos previstos no artigo 10 da Resolução Conjunta nº 1 do Banco Central do Brasil: (i) uso de linguagem clara, objetiva e adequada; (ii) finalidades determinadas; (iii) prazo de validade compatível com a finalidade do compartilhamento, limitado a 12 (doze) meses; (iv) identificação da instituições transmissora dos dados ou detentora da conta; (v) identificação dos dados ou serviços que serão compartilhados; (vi) identificação do cliente titular dos dados; e (vii) ser posterior a data de início de vigência da Resolução, observando-se o cronograma de implementação do sistema.

Note-se a similitude dos requisitos supracitados ao consentimento delineado pela LGDP (manifestação livre, informada, prévia e inequívoca de vontade, feita por meio eletrônico, pela qual o cliente concorda com o compartilhamento de dados ou de serviços para finalidades determinadas e com possibilidade de revogação a qualquer momento).

Ambos têm por cerne o consentimento informado, de modo a resguardar a decisão informada do titular sobre o tratamento de seus dados pessoais, zelando por sua outorga de forma livre e inequívoca.

Desse modo, os apontamentos e as cautelas jurídicas indicadas no tópico precedente são, em sua integralidade, aplicáveis ao *open finance*. Pertinente, outrossim, especial ressalva quanto a evolução do conceito de consentimento livre.

Rememore-se que o entendimento doutrinário caminha para além dos preceitos de voluntariedade, buscando agasalhar a ideia de consentimento granular.

> O consentimento granular estabelece, portanto, limites à microeconomia dos dados pessoais, na medida em que resguarda a opção do titular em emitir autorizações, de forma fragmentada, no tocante ao fluxo de seus dados pessoais. Por exemplo, uma aplicação pode oferecer inúmeras funcionalidades cujo funcionamento demanda, indispensavelmente, uma gama de dados pessoais para a sua operacionalização. Com a ressalva do consentimento granular, o titular poderá fazer o uso de tal aplicação, determinando, de forma correlacionada, quais dados pessoais seus serão tratados de acordo com as funcionalidades que pretende fazer uso. O titular possuiria, assim, um controle sobre seus dados pessoais em face do próprio produto e/ou serviço, na medida em que pode, de forma compartimentalizada, escolher como se dará o tratamento de suas informações pessoais"[78]

Nesse espectro, a interpretação sistemática do arcabouço jurídico de proteção de dados pessoais, sobretudo à luz do princípio da finalidade, tende a fortalecer a recomendação pelo consentimento granular, ainda que não expressamente previsto na LGPD e tampouco na regulação do *open finance*.

Para além dos preditos requisitos do consentimento no *open finance*, o artigo 10 §3º da Resolução Conjunta nº 1 do Banco Central do Brasil ainda obsta a obtenção do consentimento por meio de contrato de adesão, formulário com opção de aceite previamente preenchida ou de forma presumida, sem manifestação ativa do cliente titular dos dados.

Há também informações a serem prestadas, obrigatoriamente, pelas Instituições Participantes ao titular dos dados pessoais, a saber: (i) a identificação das Instituições Participantes; (ii) os dados e serviços objeto de compartilhamento; (iii) período de validade do consentimento; (iv) data de requisição do consentimento; (v) finalidade do consentimento, no caso de instituição receptora de dados ou iniciadora de transação de pagamento.

---

[78] BIONI. Bruno Ricardo et al. Contribuição do grupo de políticas públicas em acesso à informação da Universidade de São Paulo (GPOAI/USP) à consulta pública do anteprojeto de lei de proteção de dados pessoais. São Paulo. 2015. Disponível em: https://gpopai.usp.br/wordpress/wp-content/uploads/2015/08/Contribuicao-GPoPAI-Dados-Pessoais_Diagramada.pdf>

Destaca-se, ainda, que há um período de validade do consentimento, fixado em 12 (doze) meses, exceto as transações de iniciação de pagamento, cujo limite deve coincidir com a data de encerramento de referida transação.

Na iniciação de pagamento, o prazo de finalização de pagamento pode alcançar período superior a 1 (um) ano, situação identificada nas hipóteses de operação de tratamento sucessivo. Em tais situações, além do consentimento abarcar o compartilhamento da forma, valor da transação, informações sobre o recebedor do pagamento e data, devem ser também indicados a periodicidade e o prazo da transação de pagamento.

Sem prejuízo dos prazos fixados, o consentimento pode ser revogado pelo titular dos dados a qualquer momento. E, durante o período de validade do consentimento, em caso de alteração na finalidade do tratamento de dados, as Instituições devem notificar o cliente titular dos dados e obter novo consentimento.

Tais óbices e exigências trazidos pela Resolução acrescem condicionantes não expressamente previstos pela LGPD, os quais, porém, mostram-se em total alinhamento aos seus princípios, notadamente o princípio da autodeterminação informativa e da transparência.

Apresentadas as principais intersecções do arcabouço jurídico da proteção de dados pessoais com o *open finance*, prossegue o presente trabalho com o devido cotejo entre eles e a identificação dos potenciais riscos.

3 COMPATIBILIDADE DO OPEN FINANCE À PROTEÇÃO DE DADOS PESSOAIS

Conquanto o *open finance* apresente-se como um importante ecossistema para o atingimento dos objetivos estratégicos de inclusão bancária e aumento da competitividade no setor financeiro, o que enseja grande euforia, não se pode perder de vista os riscos que envolvem o tratamento de dados pessoais, notadamente, os dados cadastrais e transacionais bancários.

A estruturação do Sistema Financeiro Nacional (SFN) e de seus arranjos de pagamento é dada pelas diretrizes da Lei nº 4.595 de 31 de dezembro de 1964[79] e a Lei nº 12.865, de 9 de outubro de 2013[80], atribuindo as competências para a atuação do Banco Central e do Conselho Monetário Nacional (CMN).

Desse modo, embora a regulação do *open finance* explicite a relevância da proteção de dados na exposição de motivos da Resolução Conjunta nº 1, de 4 de maio de 2020[81], não se afasta o dever de harmonizar essa regulação aos preceitos da LGPD[82], além do próprio debate sobre o alcance da competência do Banco Central, a ser oportunamente tratado, ainda que de forma superficial ante a delimitação temática do presente trabalho.

Ressalvado o entusiasmo com os objetivos propostos pelo *open finance*, propõe-se a imersão sobre os riscos à proteção dos dados pessoais vislumbrados com sua implementação e operacionalização, sob a ótica do atual arcabouço jurídico protetivo conferido a esse novo bem jurídico.

---

[79] BRASIL, 1964.

[80] BRASIL, 2013.

[81] Exposição de Motivos da Resolução Conjunta nº1. (...). 2. Em comum, tais ações geralmente têm por objetivo aumentar a competitividade nos mercados financeiros, incentivar a inovação financeira, racionalizar os processos de instituições reguladas, possibilitar parcerias comerciais entre instituições financeiras e instituições não financeiras, e, também, em diversos casos, empoderar o consumidor financeiro. Importante ressaltar que o consumidor é reconhecido como o titular dos seus dados pessoais; no caso do Brasil a Lei Geral de Proteção de Dados Pessoais (LGPD), a Lei nº 13.709, de 14 de agosto de 2018, reforçará e sistematizará, a partir de sua entrada em vigor, a tutela desses dados**.** Com o Open Banking, o consumidor financeiro pode consentir com o compartilhamento padronizado de dados e serviços por meio de abertura e integração de sistemas de instituições financeiras e de pagamento, caso vislumbre algum benefício com esse compartilhamento, a exemplo do acesso a serviços financeiros adequados ao seu perfil

[82] BRASIL, 2018.

3.1 POTENCIAIS VIOLAÇÕES À PROTEÇÃO DE DADOS PESSOAIS NO *OPEN FINANCE*

Desde o Comunicado nº 33.455, de 24 de abril de 2019, do Banco Central[83], que trata dos requisitos fundamentais para a implementação do *open finance*, observa-se o entendimento do órgão regulador pela relevante vinculação entre a LGPD[84] e o sistema financeiro aberto[85].

Da mesma sorte, a exposição de motivos da Resolução Conjunta nº 1, de 4 de maio de 2020[86] reconhece a proteção dos dados pessoais pela LGPD[87], atribuindo-lhe o dever de reforçar e sistematizar tal tutela[88].

Para além das menções expressas, identifica-se a similitude principiológica entre os citados diplomas legais e normativos, sobretudo quanto aos princípios da transparência, segurança e privacidade de dados, qualidade e tratamento não discriminatório, bem como o prestígio ao consentimento como a base legal para o tratamento dos dados no *open finance.* Observa-se, ainda, congruência entre os requisitos necessários à validade de tal consentimento, conforme destacado no capítulo 1 do presente trabalho.

Em que pese a adequação principiológica, destaca-se que referida Lei também dispõe, em seu artigo 46, §1º[89], que compete à Autoridade Nacional de Proteção de Dados (ANPD) dispor sobre os padrões técnicos mínimos das medidas de segurança a serem adotadas pelos

---

[83] BANCO CENTRAL, 2019.

[84] BRASIL,2018.

[85] Comunicado 33.425. Artigo 3. O tema tem-se destacado mundialmente no contexto das inovações introduzidas no mercado financeiro. Reguladores de algumas jurisdições identificaram a necessidade de intervenção regulatória para disciplinar o assunto, de forma a assegurar o alcance de seus objetivos específicos. Nesse contexto, o Banco Central do Brasil vem acompanhando as discussões internacionais e as iniciativas locais. Além disso, a discussão torna-se mais relevante com a edição da Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais no País

[86] BANCO CENTRAL e CONSELHO MONETÁRIO NACIONAL, 2020.

[87] BRASIL,2018.

[88] Exposição de Motivos da Resolução Conjunta nº1. (...). 2. Em comum, tais ações geralmente têm por objetivo aumentar a competitividade nos mercados financeiros, incentivar a inovação financeira, racionalizar os processos de instituições reguladas, possibilitar parcerias comerciais entre instituições financeiras e instituições não financeiras, e, também, em diversos casos, empoderar o consumidor financeiro. Importante ressaltar que o consumidor é reconhecido como o titular dos seus dados pessoais; no caso do Brasil a Lei Geral de Proteção de Dados Pessoais (LGPD), a Lei nº 13.709, de 14 de agosto de 2018, reforçará e sistematizará, a partir de sua entrada em vigor, a tutela desses dados. Com o Open Banking, o consumidor financeiro pode consentir com o compartilhamento padronizado de dados e serviços por meio de abertura e integração de sistemas de instituições financeiras e de pagamento, caso vislumbre algum benefício com esse compartilhamento, a exemplo do acesso a serviços financeiros adequados ao seu perfil

[89] LGPD. 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.

agentes de tratamento, com vistas a proteger os dados pessoais de qualquer forma de tratamento inadequado ou ilícito.

Assim, ao final do dia, subsiste o risco de a ANPD, no exercício de suas atribuições, divergir de eventuais diretrizes e estruturas técnicas implementadas no *open finance,* ainda que sob a égide do Banco Central do Brasil, o que poderá abrir margem para, além do debate sobre a proteção dos dados pessoais, emergir a problemática dos conflitos de competência entre órgãos reguladores, a exemplo do histórico belicoso entre Banco Central e Conselho Administrativo de Defesa Econômica (CADE)[90].

Nesse contexto, imperioso pontuar que, após superadas as celeumas sobre o atraso na criação e estruturação da ANPD[91], mediante sua criação pela conversão da Medida Provisória nº 869, de 27 de dezembro de 2018[92], na Lei nº 13.853, de 14 de agosto de 2019[93] e sua estruturação pelo Decreto 10.474, de 26 de agosto de 2020,[94]mantém-se a lacuna normativa a respeito do posicionamento da autarquia[95] sobre o *open finance.*

Em outras áreas, a ANPD sinaliza pela predisposição para o diálogo interinstitucional, a exemplo do Acordo de Cooperação Técnica (ACT) nº 5/2021[96] firmado entre referida Autoridade e o CADE, com vistas ao aperfeiçoamento das ações voltadas à defesa, fomento e disseminação da concorrência no âmbito dos serviços de proteção de dados.

Dentre a ações preconizadas no Acordo de Cooperação Técnica destacam-se o compartilhamento de estudos, documentos, pesquisas e conhecimento das respectivas áreas de atuação, realização de diversas atividades para desenvolvimento do tema, produção conjuntas de estudos, eventos, pesquisas e material didático sobre livre concorrência nos serviços de proteção aos dados, cooperação em casos de ato de concentração com transferência ou outros tratamentos de dados pessoais e em casos de infrações à ordem econômica que envolvam dados pessoais.

---

[90] A esse respeito, veja-se o *leading case* o conflito de competência positivo nº 0001.006908/2000-25 suscitado pelo Banco Central em face do Conselho de Administrativo de Defesa da Concorrência.

[91] Sobre os atrasos na criação e estruturação da ANPD, ver: Revista Conjur Jurídico. Com dois anos de atraso, governo cria a estrutura de agência de proteção de dados. 27 de agosto de 2020. Disponível em: https://www.conjur.com.br/2020-ago-27/dois-anos-atraso-governo-cria-estrutura-anpd. Acesso em em 19 de junho de 2022.

[92] BRASIL, 2018.

[93] BRASIL, 2019.

[94] BRASIL, 2020.

[95] A Autoridade Nacional de Proteção de Dados teve sua natureza jurídica de órgão da administração pública federal, integrante do Poder Executivo alterada para autarquia de natureza especial por meio da Lei nº 14.460 de 25 de outubro de 2022.

[96] Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/act-tarjado-compactado.pdf

Na mesma direção, quanto ao perímetro de atuação da proteção consumerista, foi também firmado o Acordo de Cooperação Técnica nº 01/2021 entre a ANPD e a Secretária Nacional do Consumidor (Senacon), no qual vislumbra-se um intenso arsenal de cooperação e ações conjuntas entre as instituições, inclusive em maior grau do que aquele preconizado no Acordo de Cooperação Técnica firmado junto ao CADE, tendo em vista especialmente a previsão expressa de uniformização de entendimento e coordenação de ações, inclusive para direcionamento de reclamações e em casos de incidente de segurança.

Referidos acordos amoldam-se ao planejamento estratégico 2021-2013 da ANPD[97], notadamente ao objetivo estratégico de fortalecimento da cultura de proteção de dados pessoais, dentro do qual insere-se a ação estratégica de promoção do diálogo com entidades governamentais e não governamentais, inclusive com atuação em conjunto e incorporação das melhores práticas.

No entanto, até o presente momento, não se vislumbra um estreitamento entre a ANPD e o Banco Central do Brasil para uma coordenação regulatória institucionalizada.

A ausência de uma reflexão amadurecida sobre os temas afetos ao Sistema Financeiro Nacional e a pendência de sua inclusão na agenda regulatória da ANPD foram explicitadas pelas falas de sua Diretora, Mirian Wimmer e de sua Coordenadora Geral de Normatização, Isabela Maiolino, no evento virtual "Varandas – Convergindo visões: meios de pagamento, LGPD e impactos regulatórios" promovido pelo Instituto de Tecnologia e Sociedade (ITS Rio)[98].

Por outro lado, o Banco Central do Brasil e as instituições participantes prosseguiram com a implementação do *open finance*, inclusive com a definição e desenvolvimento dos padrões técnicos de suas interfaces, cujos principais aspectos serão submetidos à Convenção entre as instituições, conforme determina o artigo 44 da Resolução Conjunta nº 1.

Nesse cenário, a despeito da convergência principiológica entre os diplomas, não se pode descartar potenciais violações a serem identificadas pela Autoridade Nacional de Proteção de Dados em face dos casos concretos e dos modelos de negócios desenvolvidos sob a égide do sistema financeiro aberto, razão pela qual oportuno dedicar especial atenção à proteção de dados pessoais na estruturação tecnológica e jurídica do *open finance*, com vistas a mitigar eventuais ingerências e conflitos regulatórios dessa espécie.

---

[97] Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/planejamento-estrategico/planejamento-estrategico-2021-2023.pdf

[98] Disponível em: https://itsrio.org/pt/varandas/convergindo-visoes-meios-de-pagamento-lgpd-e-impactos-regulatorios/. Acesso em em 19 de junho de 2022.

Pelas mesmas razões, vislumbra-se potencial insegurança para a tomada de decisões na gestão de crise afeta a um incidente de segurança no *open finance* que envolva dados pessoais, pois há a competência legal da ANPD para a condução dos incidentes dessa espécie, por outro lado, a competência regulatória protagonizada pelo Banco Central do Brasil e os preceitos autorregulatórios sobre incidentes de segurança constantes da Resolução Conjunta nº 1, a exemplo dos artigos 33, III; 38 §3º; 40, IV e 48, III.

Nesse aspecto, conquanto as previsões regulatórias do open finance devam ser observadas, estas versam sobre condutas de cunho interno às Instituições Participantes e não preveem atuação específica do Banco Central. A estruturação do tratamento de incidentes de segurança e as respectivas competências para apuração e determinação das medidas a serem providenciadas, com vistas a mitigação dos danos, estão tratadas no artigo 48 da LGPD[99] e inserem-se no âmbito de atuação da ANPD, devendo nortear as ações na gestão de crise dessa natureza.

Nada obsta, outrossim, a atuação do Banco Central como um interveniente e eventual supervisor, dada a sua representatividade setorial, o que, mais uma vez, evidencia a importância de um diálogo institucional entre as autarquias e a celebração de convênios/acordos sobre o tema.

Para fins de facilitar a compreensão dos potenciais riscos ora identificados, propõe-se a divisão, meramente metodológica, dos aspectos exógenos e endógenos, nos moldes detalhados a seguir.

---

[99] 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.

3.1.1 Riscos exógenos – segurança da informação

Os riscos exógenos advêm da atuação de terceiros não participantes, direta ou indiretamente, do *open finance*, e envolvem, sobretudo, aspectos de segurança da informação.

O emprego da terminologia "exógeno" decorre, portanto, do caráter externo do agente causador do dano, ainda que este se valha de eventual fragilidade operacional do *open finance*.

Não se ignora o robusto aparato regulatório já incidente no setor financeiro sobre segurança da informação e normas de segurança cibernética, em especial a Lei Complementar nº 105/01 (Lei do Sigilo Bancário)[100], Resolução nº 4.893/21[101] e Circular nº 3.909/18 (Normas de Segurança Cibernética)[102], e de toda a avançada estrutura já existente para ampará-lo.

Contudo, a mudança de uma estrutura pautada no sigilo para uma estrutura de compartilhamento em *Application Programming Interface (API's*), com potencialidade de elevado fluxo de dados, inclusive para novos entrantes ainda não tão familiarizados com a amplitude regulatória do setor e até não atingidos por ela (a exemplo do contrato de parceria do artigo 36 da Resolução Conjunta nº 1/2020[103]), majora os riscos de ataques cibernéticos e fraudes, a exemplo do que aconteceu com o Sistema de Pagamento Instantâneo (PIX)[104].

Nesse contexto, emergem as principais preocupações: uma de aspecto técnico a respeito da interface tecnológica para a interoperabilidade e padronização mínima, e outra relativa aos custos de transação e seus potenciais impactos concorrenciais, sem prejuízo da responsabilidade do participante, conforme previsto no artigo 31 da Resolução Conjunta nº1[105].

No cenário de sistema financeiro aberto, os cibercriminosos representam um relevante vetor de ataque. Esses ataques variam de infraestrutura técnica até engenharia social, aproveitando-se, sobretudo, do desconhecimento do cliente. Isso pode resultar em perda de dados, roubo de identidade, fraude e prestação de serviço intermitente[106].

---

[100] BRASIL, 2001.

[101] BANCO CENTRAL, 2021.

[102] BANCO CENTRAL, 2018.

[103] Resolução Conjunta nº 1. Art. 36. É admitida a contratação de parceria por parte das instituições de que trata o art. 1º com entidades não autorizadas a funcionar pelo Banco Central do Brasil com o objetivo de compartilhar dados de que trata o art. 5º, inciso I, alíneas "c" e "d", bem como de outros dados e serviços que venham a ser incluídos no escopo do Open Finance nos termos do art. 5º, § 1º. (Redação dada, a partir de 2/5/2022, pela Resolução Conjunta nº 4, de 24/3/2022.). BANCO CENTRAL DO BRASIL, 2020.

[104] Sobre o uso da engenharia social e aumento dos golpes após a criação do PIX, ver: https://www.infomoney.com.br/minhas-financas/de-urubu-do-pix-ao-sequestro-relampago-veja-em-quais-casos-e-possivel-recuperar-dinheiro-perdido-em-golpes. Acesso em 13 de janeiro de 2023.

[105] Resolução Conjunta nº 1. Art. 31. A instituição participante é responsável pela confiabilidade, pela integridade, pela disponibilidade, pela segurança e pelo sigilo em relação ao compartilhamento de dados e serviços em que esteja envolvida, bem como pelo cumprimento da legislação e da regulamentação em vigor,

[106] PREMCHAND, Anshu; CHOUDHRY, Anurag. Open Banking & APIs for Transformation in Banking. 2018. International Conference on Communication, Computing and Internet of Things (IC3IoT). IEEE. 2018. p. 25-29.

Aliado a tais riscos e pela referida expertise desenvolvida pelo setor (impulsionada tanto pelo *compliance* como pelos custos de transação envolvidos), vislumbra-se, numa perspectiva empírica, que o *accountability* na seara da segurança da informação encontra-se jurídica e culturalmente sedimentado no setor financeiro, tendo sido, naturalmente, incorporado às preocupações do *open finance*. Desse modo, o desenvolvimento das tecnologias de interfaces para o compartilhamento dos dados tem recebido especial dedicação dos participantes.

Nesse esforço conjunto, a regulamentação dos aspectos tecnológicos tem como ponto de partida o Comunicado nº 33.455, de 24 de abril de 2019[107]. Seu texto apresenta conteúdo genérico, sem definição da técnica a ser empregada e com atribuição de seu desenvolvimento à autorregulação.[108]

A Resolução Conjunta nº 1 apresenta maiores contornos, mediante exposição dos princípios gerais, além de claramente delegar a construção das interfaces de compartilhamento e suas nuances técnicas à Convenção entre os participantes, conforme seu artigo 44, resguardada a supervisão do Banco Central (artigo 47 da Resolução Conjunta nº 1),[109] o que desnatura a proposta originária de autorregulação.

Tem-se, ainda, a Resolução nº 32, onde aparece pela primeira vez, de forma expressa, a adoção das *Application Programming Interface*[110] como a ferramenta a ser utilizada para o compartilhamento dos dados, além da orientação de que os requisitos técnicos e procedimentos operacionais serão tratados por meio de manuais.[111]

O Manual de API's é, inicialmente, consubstanciado pela Instrução Normativa nº 95, de 21 de abril de 2021[112], posteriormente revogada pela Instrução Normativa nº 130, de 22 de julho

---

[107] BANCO CENTRAL, 2019.

[108] Comunicado 33.455. Bacen. Item 8. Quanto à autorregulação, a expectativa é que fiquem a cargo das próprias instituições participantes a padronização tecnológica e de procedimentos operacionais, os padrões e certificados de segurança e a implementação de interfaces, tudo em conformidade com a própria regulamentação.

[109] Resolução Conjunta nº 1. Banco Central do Brasil. Art. 47. O conteúdo da convenção de que trata o art. 44, bem como suas alterações, devem ser submetidos à aprovação do Banco Central do Brasil, nos prazos por ele estabelecidos.

[110] Resolução Conjunta n° 32. Banco Central do Brasil. Art. 2º. Para os fins do disposto nesta Resolução, considera-se: (...) III - Application Programming Interface (API): interface dedicada ao compartilhamento entre instituições participantes de dados e serviços do escopo do Open Banking

[111] Resolução nº 32. Banco Central do Brasil. Art. 3º. O detalhamento dos requisitos técnicos e dos procedimentos operacionais para a implementação do Open Banking estará previsto em:

I - Manual de Escopo de Dados e Serviços do Open Banking;

II - Manual de APIs do Open Banking;

III - Manual de Serviços Prestados pela Estrutura Responsável pela Governança do Open Banking;

IV - Manual de Segurança do Open Banking; e

V - Manual de Experiência do Cliente no Open Banking.

Parágrafo único. Os manuais de trata o caput serão elaborados pelo Banco Central do Brasil e mantidos atualizados em seu sítio eletrônico na internet

[112] BANCO CENTRAL DO BRASIL, 2021.

de 2021[113], que divulga a versão 3.0 do Manual de *APIs* do *Open Banking*, atualmente superada pela versão 4.0 do Manual de *APIs* do *Open Finance*, instituído pela Instrução Normativa nº 306 de 19 setembro de 2022[114].

O Manual estabelece os padrões a serem observados pelos participantes, abordando aspectos técnicos tais como o desenho das API's, protocolos para o compartilhamento dos dados, controles de acesso, especificações dos parâmetros de desempenho nos procedimentos de compartilhamento de dados e os limites de chamadas de API's.

As API's já são ferramentas largamente utilizadas pela ciência computacional para viabilizar a interoperabilidade e padronizações mínimas.

Especificamente quanto aos sistemas financeiros abertos ao redor do mundo, tem-se uma supremacia na adoção de tal estrutura, diferenciadas apenas pelos aspectos operacionais advindos das diferenças regulatórias de cada país, obviamente, espelhadas na programação das API's.

As API's empregadas no *open finance* exercem um papel de "ponte entre dois mundos", permitindo que os clientes utilizem o serviço bancário mediante combinação das funcionalidades de diversos bancos e de instituições não bancárias, capazes de serem inseridas nesse ecossistema graças à estrutura das API's.[115]

A estruturação das API's no *open finance* pátrio, em cumprimento às normas regulatórias, observa a obrigatoriedade da criptografia dos dados e a divisão do compartilhamento em três etapas: consentimento, autenticação e confirmação.

Tendo em vista a conformidade dos aspectos técnicos do *open finance* à regulamentação proposta, a adoção de um estrutura tecnológica já consolidada, inclusive nos sistemas financeiros abertos estrangeiros e sem notícias de intercorrências advindas pela adoção de tal estrutura, e toda a reconhecida expertise no Sistema Financeiro Nacional no enfrentamento de ataques cibernéticos (razão pela qual, acertadamente, lhe foi dado protagonismo na construção das API's), pode-se concluir que o sistema é robusto ante os riscos à segurança da informação.

Outrossim, a experiência nacional com o Sistema de Pagamento Integrado e os modelos de fraudes a ele impetrados, bem como recentes notícias quanto a fraudes em aplicativos bancários denotam relevantes preocupações com a experiência do usuário e a necessidade de

[113] BANCO CENTRAL DO BRASIL, 2021.
[114] BANCO CENTRAL DO BRASIL, 2022.
[115] EURO BANKING ASSOCIATION. Understanding the business relavance of Open APIs and Open Banking for Banks. Euro Banking Association. v.1.0. p. 35. 2016.

intensificar e aprimorar os programas de conscientização quanto às cautelas que devem ser adotadas.

Ações educativas junto aos clientes bancários sobre o *open finance* mostram-se incipientes e, em sua esmagadora maioria, com enfoque apenas no incentivo à adesão ao sistema, sem maiores alertas quanto às medidas de segurança sob responsabilidade do usuário.

3.1.2 Riscos endógenos

Seguindo o mesmo critério metodológico, os riscos endógenos são aqueles atribuíveis à própria atuação dos participantes do *open finance* e, nessa seara, evidenciam uma grande amplitude para suas hipóteses de incidência.

Sem a pretensão de esgotar o tema, investigam-se os riscos advindos, em linhas gerais, da atuação dos participantes tanto no sentido de restringirem o compartilhamento dos dados, em afronta ao consagrado direito dos titulares dos dados à autodeterminação informativa, como de extrapolarem os limites para o tratamento dos dados para além das bases legais previstas na Lei Geral de Proteção de Dados e de toda a principiologia protetiva dos dados, em seus atuais contornos.

Numa perspectiva empírica, aqui o desafio é maior. O entusiasmo com o potencial disruptivo do *open finance*, em especial seu fomento à competitividade no setor, turvam o olhar sobre os riscos de tratamento inadequado dos dados pessoais.

Consigne-se que condutas destinadas a restringir o compartilhamento de dados, não raro, revestem-se de aspectos anticoncorrenciais, sobretudo em mercados de elevada concentração como o bancário, com reconhecida desproporcionalidade de poder entre as diferentes instituições participantes do *open finance*. Outrossim, o cerne do presente trabalho são os riscos sob o enfoque da proteção de dados pessoais, ainda que subjacentes eventuais desdobramentos concorrenciais.

A regulamentação do *open finance* enfrenta o desafio de encontrar o ótimo de Pareto entre o arcabouço jurídico de proteção aos dados pessoais e o fomento ao seu compartilhamento, capaz de ensejar o almejado aumento da competitividade no setor.

A Resolução Conjunta nº 1[116], em aderência à Lei Geral de Proteção de Dados[117], afasta-se da ideia tão arraigada no setor financeiro (em larga medida decorrentes das imposições legais do sigilo bancário) de as instituições financeiras serem as responsáveis pelos dados sob sua

[116] BANCO CENTRAL DO BRASIL. Conselho Monetário Nacional, 2020.
[117] BRASIL. 2018.

custódia, assumindo o papel de titular de tais dados, e avança para a atribuição da responsabilidade ao titular dos dados mediante o compartilhamento consentido, colocando-o no papel central de gestor das suas informações, em prestígio ao princípio da autodeterminação informativa.

Essa mudança regulatória sobre a proteção de dados cadastrais e transacionais (sem perder de vista que o regramento do sigilo bancário continua vigente e dele as Instituições não podem se eximir) precisa ser espelhada na estrutura do *open finance*, cuja construção está a cargo dos participantes por meio de Convenção, a ser submetida a validação do Banco Central, nos moldes dos artigos 44 e 47 da supracitada Resolução Conjunta nº 1.

Nesse espectro, o papel de supervisão do Banco Central ganha especial relevância para que a estrutura tecnológica adotada pela Convenção não repercuta em custos de transação capazes de inviabilizar a entrada de novos atores e obstar a tão pretendida concorrência no setor.

Além das repercussões concorrenciais advindas de um modelo regulatório restritivo a novos entrantes, especialmente considerando a importância dos dados nos tempos hodiernos e a capacidade de investimentos de que gozam as instituições financeiras já consolidadas, a jornada do compartilhamento de dados do usuário também pode configurar cerceamento ao direito do titular de dados à autodeterminação informativa. Cita-se, como exemplo, uma jornada do consentimento estruturada com *design* pouco amigável à pretensão do titular de compartilhar os seus dados.

Nesse espectro, deve-se sopesar, inclusive, a elevada concentração do setor financeiro em 5 (cinco) grandes bancos múltiplos, de modo que a esmagadora maioria dos dados cadastrais e transacionais bancários a serem compartilhados estão com estes participantes já consolidados do setor.

Diante de cenário posto, a jornada do compartilhamento prevista no artigo 8º e seguintes da Resolução Conjunta nº 1 preconiza que o pedido de compartilhamento de dados e seu respectivo consentimento origina-se por meio da instituição receptora dos dados, que redireciona o usuário para a instituição transmissora, em ambiente no qual dar-se-á a autenticação (login/senha do usuário, nos moldes padrões adotados por cada instituição) e a confirmação do pedido, seguindo-se do retorno à instituição receptora para efetivar o compartilhamento, conforme didaticamente exposto no Portal do Open Banking no Brasil:

Figura 3 – Jornada do Consentimento

Fonte: Banco Central. 2022.

Nota-se que o desenho regulatório para a originação do pedido de compartilhamento de dados por meio da instituição receptora tem o condão de construir uma experiência do usuário facilitada pelo interesse desta instituição em ter acesso aos dados, o que, caso iniciada junto à instituição transmissora poderia ensejar interesses conflitantes, com potencialidade de restringir o exercício da autodeterminação informativa.

Por outro lado, a instituição receptora deve zelar pelo cumprimento dos requisitos à obtenção do consentimento e, sobretudo, pela ciência do usuário sobre seus direitos e responsabilidades.

Considerando toda a problemática já mapeada sobre o tratamento indevido de dados em outras atividades econômicas atrelada ao contexto de que dados cadastrais e transacionais bancários abrangem aspectos relevantes da vida das pessoas (histórico financeiro, histórico de pagamento e seu respectivo comportamento de consumo, a título de exemplo), é de se supor os efeitos adversos ainda mais robustos decorrentes do tratamento indevido de tais dados.

Logo, no setor financeiro, as cautelas sobre o compartilhamento de dados e os esclarecimentos a serem prestados aos usuários devem observar critérios mais rigorosos, de modo que não se caia no lugar comum de uma adesão do usuário à uma política de privacidade ininteligível ou obtida por meio de um consentimento irrefletido.

À guisa de exemplo da complexidade dos aceites às políticas de proteção de dados prestados pelos usuários em segmentos diversos, um estudo elaborado por Lior Strahilevitz e Matthew Kugler demonstrou que, ainda que os usuários leiam os termos de política de privacidade, seus conhecimentos pessoais e as normas sociais são mais úteis no entendimento da política de privacidade do que o texto em si[118].

Nesse espectro, salutar que as informações a serem prestadas aos usuários do *open finance* tragam esclarecimentos aprofundados sobre o funcionamento do sistema financeiro aberto, seu alcance, finalidade e vantagens do compartilhamento de seus dados.

Imperioso um olhar nos canais de comunicação adotados pelas instituições participantes, as quais, em sua maioria, redirecionam ao Portal do *Open Banking* no Brasil[119], mantido pela Estrutura Responsável pela Governança do *Open Banking*, que apresenta as seguintes informações aos clientes bancários:

Figura 4 – Informações do Portal do Open Banking

Fonte: https://openbankingbrasil.org.br/conheca-o-open-banking/. Acesso em 22 de junho de 2022

[118] STRAHILEVITZ. Lior; Kugler.Matthew B. Is privacy policy language irrelevante to consumers? Coase-Sandor Working Paper Series in Law and Economics, nº 776 (2016). Disponível em: https://chicagounbound.uchicago.edu/law_and_economics/796/. Acesso em 26 de junho de 2022.

[119] Disponível em: https://openbankingbrasil.org.br/conheca-o-open-banking/. Acesso em 22 de junho de 2022

E, especificamente quanto as vantagens advindas do *open finance*, traz os seguintes exemplos pautados na experiência e necessidades cotidianas do usuário:

Figura 5 – Vantagens do open finance (casos de uso)

Fonte: Banco Central. 2022

Nota-se o uso de uma linguagem clara e acessível, trazendo exemplos de casos hábeis a dar concretude às vantagens do *open finance*, ressalvados os tópicos quanto ao uso do agregador de dados dos pagamentos, os quais poderiam ser mais didáticos e abster-se do uso de termos técnicos.

Caberia expor ao usuário qual a vantagem do agregador de dados, ou, em outros termos, qual a vantagem de reunir dados das instituições num único ambiente, e, quanto aos pagamentos, explanar sobre quais tipos de pagamentos podem ser feitos, evitando-se o uso da expressão “iniciação de pagamento”.

As informações prestadas também tangenciam a superficialidade quanto ao uso dos dados compartilhados, limitando-se a assertivas genéricas de que as informações servirão para oferecer soluções mais aderentes ao perfil do cliente.

Em que pese a regulamentação do *open finance* estar adstrita ao compartilhamento de dados entre as instituições participantes por meio da respectiva ferramenta para tanto, não se pode perder de vista o princípio da finalidade preconizado na Lei Geral de Proteção de Dados. Desse modo, cabe o questionamento sobre o alcance das assertivas genéricas sobre o tratamento dos dados para a identificação de produtos e serviços mais aderentes ao perfil do cliente, após a internalização dos dados pela instituição receptora, na medida em que sujeitos às diretrizes de referida Lei, em especial o princípio da finalidade.

Da mesma sorte, sob a ótica da transparência, advém o questionamento sobre a pertinência de que referida informação seja explicitada aos usuários (o que nesse momento não

está sendo feito), cientificando-lhes do que será feito com seus dados após o compartilhamento: servirão para fomentar qual tipo de oferta?; se compartilho dados de contas para demonstrar minha movimentação financeira com vistas a robustecer um pedido de financiamento imobiliário, esses dados poderão ser usados para ofertas de aplicações financeiras, ante a identificação pela instituição receptora de recursos para tanto?; o perfil de consumo identificado na fatura de cartão de crédito compartilhada com o objetivo de incremento do limite de crédito poderá ser utilizado para oferta de outros produtos financeiros (consumo em lojas de produtos infantis utilizado para oferta de previdência privada júnior, por exemplo).

Para além da imperiosa observância dos requisitos ao consentimento, para que a experiência do usuário seja plena e adequada à proteção de dados pessoais toda a jornada do tratamento de seus dados deverá ser a ele explicada. E, para tanto, as ferramentas devem ser desenhadas para orientar o usuário sobre o controle de seus dados.

> "É dizer, instrumentos regulatórios podem servir como indutores da utilização de tecnologias que ajudem os clientes das instituições financeiras a receberem informações inteligíveis e de qualidade e possam, assim, exercer a autodeterminação informativa, gerindo, da maneira que melhor lhes aprouver, a utilização de dados pessoais".[120]

Com vistas a trazer concretude para os riscos ora expostos, propõe-se, nas linhas seguintes, a título meramente exemplificativo, maior imersão sobre algumas das consequências do tratamento dos dados internalizados por meio do compartilhamento autorizado via *open finance*.

3.2 TRATAMENTO DOS DADOS PESSOAIS COM FULCRO NO CONSENTIMENTO

Não é demais reforçar que a LGPD possui um alcance horizontal, ou seja, aplica-se indistintamente a todas as atividades econômicas, inclusive ao setor financeiro.

Nesse espectro, todas as bases legais para o tratamento de dados pessoais previstas no artigo 7º da LGPD[121] são potencialmente elegíveis como hipóteses autorizativas ao tratamento

---

[120] Ragazzo. Carlos; Leite. Douglas. Desafios do compliance de dados para o setor financeiro: PIX, open Banking e a LGPD. In Compliance e políticas de proteçao de dados. Ana Frazão e Ricardo Villas Boas Cueva, pg. 948

[121] 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;

de dados pessoais no *open finance*, ressalvados os limites impostos pela Lei do Sigilo Bancário, sendo a adoção do consentimento, portanto, uma escolha do órgão regulador.

Imperioso esclarecer que referida escolha coloca o consentimento como a base legal hábil à operacionalização do *open finance*, mas não implica a vedação à incidência das demais bases legais previstas na LGPD, em caráter casuístico, subsidiário e restritivo, e, tampouco o tratamento de dados anonimizados, nos estritos termos autorizados pela lei.

Dito de outro modo, o consentimento é a base legal que viabiliza a operacionalização do *open finance*, é aquela válida para que os usuários titulares de dados autorizem o compartilhamento pelo *open finance.*

Inobstante, as demais hipóteses legais para o tratamento de dados podem incidir, no caso concreto, demandando o tratamento dos dados, desde que, obviamente, enquadradas na LGDP e no regramento de Sigilo Bancário. Destacam-se, nesse contexto, as bases legais do cumprimento de obrigação legal ou regulatória, execução contratual, legítimo interesses ou proteção ao crédito.

À guisa de exemplo, em caso de litígio entre o consumidor bancário e a Instituição Receptora dos dados poderá ser necessário a imersão probatória sobre o objeto e finalidade do compartilhamento autorizados no *open finance.* Nesse contexto, deverá ser providenciada a juntada aos autos das informações pertinentes e, portanto, atraindo a incidência da base do exercício regular de direitos em processo judicial, administrativo ou arbitral, previsto no artigo 7º, VI da LGPD.

A possibilidade de tratamento de dados pessoais no *open finance* por hipóteses diversas do consentimento coaduna-se com as Orientações sobre proteção de dados nos serviços financeiros[122], publicado pelo European Data Protection Supervisor, bem como pela Diretriz 06/2020[123], que trata da interação entre a Segunda Diretiva de Serviços de Pagamento e o GDPR.

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, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

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.

[122] Disponível em: https://edps.europa.eu/sites/edp/files/publication/14-11-25_financial_guidelines_en.pdf. Acesso em 18 de dezembro de 2022.

[123] Disponível em: https://edpb.europa.eu/system/files/2021-06/edpb_guidelines_202006_psd2_afterpublicAcessotion_pt.pdf. Acesso em 18 de dezembro de 2022.

Ressalvada a possibilidade casuística de incidência das demais bases legais para tratamento de dados pessoais no *open finance*, indubitável que as estruturas jurídica e operacional do sistema financeiro aberto estão fortemente calcadas no consentimento, conforme detalhado do capítulo anterior.

O papel relevante atribuído ao consentimento nos dias atuais, como ferramental primordial à concretização da autodeterminação informativa, merece ser observado com cautela e sob a perspectiva de adequações à sua intelecção, ante os novos modelos de negócio da economia digital.

A necessidade de atualização de seu escopo e aplicabilidade convergem às críticas aplicadas ao consentimento também na seara contratual, berço do protagonismo do elemento volitivo.

> "Imaginar que os contratos seriam fruto de vontade livre e incondicionada, como queriam os liberais, nos séculos XVIII e XIX, é desdenhar todo o avanço das ciências que estudam a mente humana, como a psicologia e a psicanálise. (...) Toda essa revolução mexe com a principiologia do Direito Contratual. Os fundamentos da vinculatividade dos contratos não podem mais se centrar exclusivamente na vontade, segundo o paradigma liberal individualista. Os contratos passam a ser concebidos em termos econômicos e sociais. Nasce a Teoria Preceptiva. Segundo esta teoria, as obrigações oriundas dos contratos valem não apenas porque as partes as assumiram, mas porque interessa à sociedade a tutela da situação objetivamente gerada, por suas conseqüências econômicas e sociais."[124]

Nesse espectro, propõe-se a evolução do conceito calcado no mero acordo de vontades para um novo conceito de contrato, que abrange sua função econômica e o escopo de satisfação das necessidades individuais e promoção da dignidade humana:

> "Ato jurídico lícito, de repercussão pessoal e sócio-econômica, que cria, modifica ou extingue relações convencionais dinâmicas, de caráter patrimonial, entre duas ou mais pessoas, que, em regime de cooperação, visam atender necessidades individuais ou coletivas, em busca da satisfação pessoal, assim promovendo a dignidade humana"[125].

Especificamente na seara da proteção de dados pessoais, as principais críticas ao seu protagonismo como base legal ao tratamento de dados advêm de suas limitações ante o contexto social de crescente uso de *Big Data* e da publicidade comportamental, aspectos ante aos qual o

---

[124] FIUZA, Cesar. Por uma redefinição da contratualidade. Março/2017. Âmbito Jurídico. Disponível em: https://ambitojuridico.com.br/cadernos/direitocivil/por-uma-redefinicao-da-contratualidade/. Acesso em 27 de novembro de 2022.

[125] FIUZA, Cesar. Por uma redefinição da contratualidade. Março/2017. Âmbito Jurídico. Disponível em: https://ambitojuridico.com.br/cadernos/direitocivil/por-uma-redefinicao-da-contratualidade/. Acesso em 27 de novembro de 2022.

controle individualizado do fluxo de dados, preconizado pelo consentimento, mostra-se insuficiente e exaustivo.

O atual contexto enseja maior assimetria técnico-informacional, de modo que o titular dos dados figura numa posição de limitação cognitiva sobre todos os riscos e vantagens envolvidos no tratamento de seus dados pessoais, agravados diante de toda a amplitude que este tratamento pode assumir com o uso do *Big Data*, inclusive com o cruzamento de dados e obtenção de novas informações, diversas da finalidade de origem, além das repercussões da publicidade comportamental no exercício de seu autodeterminação informativa[126].

Ademais, as contribuições da economia comportamental mitigaram o postulado da racionalidade humana na busca da maximização de riquezas e evidenciaram a existência de vieses e heurísticas que interferem na tomada de decisão[127].

Nesse espectro, oportuno rememorar que a interação social nos dias atuais depende do fluxo informacional, de modo que o indivíduo, como parte mais vulnerável, consente ao tratamento de seus dados para assim alcançar sua conformação social, sob pena de sua exclusão, o que passa ao largo do almejado empoderamento do titular dos dados pessoais preconizado pelo princípio da autodeterminação informativa.

Referido entendimento conduz a importantes fundamentos sobre a inaptidão do consentimento: a assimetria de poder entre os envolvidos e a maior vulnerabilidade do titular de dados.

Isto porque, a maioria das Políticas de Consentimento está baseada na dualidade de consentir ou não consentir ("*take it or leave it*"). Assim, o custo social de resguardar os dados pessoais é não desfrutar do serviço ofertado, ou seja, "o exercício de sua privacidade informacional requer abdicar de facilidades do mercado de consumo"[128], o que claramente impacta na autonomia decisória do titular dos dados[129].

---

[126] BIONI. Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro. Forense. 2019.

[127] Vide: SUNSTEIN. Cass R; THALER. Richard H. Nude: Como tomar melhores decisões sobre saúde, dinheiro e felicidade. Tradução Angelo Lessa. 1ª edição. Rio de Janeiro. Objetiva. 2019. KAHNEMAN. Daniel. Rápido e Devagar: Duas formas de pensar. Tradução Cássio de Arantes Leite. 1ª edição. Rio de Janeiro. Objetiva. 2012.

[128] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor. 1ª ed. Brasília: Saraiva, 2014. p.41.

[129] FONSECA. Gabriel C. Soares da. MENDES. Laura Schertel. Proteção de Dados para além do consentimento: tendências contemporâneas de materialização. In: Revista Estudos Institucionais. V. 6. nº 2, p. 515/516. Disponível em: https://www.estudosinstitucionais.com/REI/article/view/521/510. Acesso em 07 de janeiro de 2023.

A teoria da filósofa Helen Nissenbaum, desenvolvida na obra Privacy in Context: Technology, Policy, and the Integrity of Social Life,[130]propõe a superação do consentimento sob a ótica do público e privado e da quebra da privacidade pelo respectivo consentimento individualizado, mediante evolução para uma abordagem de integridade contextual do fluxo dos dados.

Para além de uma verificação contratualista sobre a outorga ou não do consentimento pelo titular dos dados, a abordagem de integridade contextual do fluxo de dados propõe uma análise de adequação do tratamento de dados ao contexto social e às normas informacionais, divididas em normas de apropriabilidade (*appropriateness*), referentes à aferição de se o tipo de informação a ser apropriada (tratada) é adequada ao contexto, e normas de "distribuição" (*distribution*), que remontam à adequação do compartilhamento (disseminação, distribuição) do dado ao contexto.

Nesse sentido, a abordagem da integridade contextual contribui com uma diretriz interpretativa para o *open finance*, de modo que o tratamento de dados pessoais esteja adequado não apenas aos limites do consentimento, mas, sobretudo, compatibilizado ao contexto social no qual fora outorgado pelo titular dos dados.

Em aderência à abordagem da integridade contextual, Bruno Bioni propõe que a análise da viabilidade jurídica do tratamento de dados pessoais não fique restrita ao consentimento e abarque também a aferição da legítima expectativa do titular dos dados dentro do contexto no qual se deu a outorga do consentimento.[131]

O arcabouço jurídico de proteção de dados pátrio denota influência da abordagem da integridade contextual, conforme depreende-se das qualificadoras ao consentimento contidas nos textos da LGPD e da regulamentação do *open finance*, bem como dos princípios elencados no artigo 6º de referida Lei[132].

---

[130] NISSENBAUM, Helen. Privacy in Context. Technology, Policy, and the Integrity of Social Life. Stanford, EUA: Stanford University Press, 2009.

[131] BIONI. Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro. Forense. 2019. p. 322

[132] 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;

Assim, o consentimento livre, informado, inequívoco e adstrito à sua finalidade, bem como a observância aos princípios da finalidade, adequação e necessidade, tais como preconizados no ordenamento jurídico, atendem ao escopo de mitigar os riscos atribuídos ao uso da base legal do consentimento.

Superados os aspectos eminentemente centrados na autonomia da vontade e na visão tradicional contratualista, vislumbra-se, especificamente no *open finance*, o uso excessivo da base legal do consentimento como um incentivo negativo ao engajamento do titular de dados na proteção de seus dados e na construção, como um todo, de uma cultura de proteção de dados pessoais.

Em um cenário de utilização massiva dos meios digitais, a sobrecarga informacional advinda dos recorrentes pedidos para a outorga do consentimento enseja adesões automatizadas, sem uma prévia e específica reflexão do titular em face de cada consentimento que lhe é solicitado, o que se convencionou denominar "fadiga do consentimento"[133].

Nesse cenário, conquanto identificadas as cautelas legais e normativas escoradas na integridade contextual, a adoção indiscriminada da base legal do consentimento pelos novos modelos de negócios impõe novos desafios de *privacy by design*, com vistas a compatibilizar os incentivos negativos advindos da fadiga do consentimento à necessária tutela dos dados pessoais.

As críticas ao uso indiscriminado do consentimento também evocam a possibilidade de um outro caminho, a regulação do *open finance* dedicar maior atenção ao tratamento de dados anonimizados, medida com potencial de alavancar, sobretudo, os novos modelos de negócios a serem desenvolvidos por meio dos contratos de parceria.

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.

[133] CHOI, Hanbyul; PARK, Jonghwa; JUNG, Yoonhyuk. The role of privacy fatigue in online privacy behavior. Computers in Human Behavior, v. 81, p. 42-51, 2018.

Para além da previsão expressa da LGPD sobre a não sujeição do tratamento dos dados anonimizados aos seus ditames, vislumbra-se a possibilidade de a regulação do open finance agasalhar, explicitamente, o tratamento de dados anonimizados em seu ecossistema, de forma a agregar maior segurança jurídica aos novos modelos de negócios que se valham de tais dados.

Nesse cenário, imperioso que a regulação defina os parâmetros técnicos de reversibilidade aceitáveis da anonimização dos dados tratados no *open finance*, em aderência aos preceitos da LGPD.

Tais iniciativas regulatórias centradas no estímulo ao tratamento de dados anonimizados têm o escopo de contribuir para o atingimento dos objetivos do *open finance* de aumento de competitividade e maior inclusão bancária, pois fornecerá maiores insumos para o desenvolvimento de novos modelos de negócios, ante as potencialidades do uso massivo de dados, sobretudo nos contratos de parceria, além de mitigar os riscos supra expostos advindos da fadiga do consentimento.

3.3 TRATAMENTO DE DADOS PESSOAIS COM FULCRO NA PROTEÇÃO DO CRÉDITO

A proteção ao crédito integra a base legal para tratamento de dados pessoais, conforme expressa previsão legal do artigo 7º, X da Lei nº 13.708/19[134].

Outrossim, a regulação do *open finance* privilegia a base legal do consentimento, sem adentrar ao mérito sobre a viabilidade de que os dados compartilhados no ecossistema sejam submetidos à análise creditícia, a despeito dos limites do consentimento outorgado.

Postas lado a lado, a proteção de dados pessoais e a proteção ao crédito protagonizaram uma das principais celeumas acerca da matéria, razão pela qual é necessária uma breve abordagem sobre o entendimento jurídico a respeito dos limites de sua incidência e, em seguida, seus impactos para o *open finance*.

Trata-se do embate entre instrumentos essenciais para a regulamentação das relações na sociedade da informação, sendo certo que a relevância da proteção dos dados pessoais restou demonstrada nas linhas antecedentes, consigna-se abaixo o contexto da proteção ao crédito:

> "Nesse contexto, os modelos de compartilhamento de informações - negativas e, especialmente, positivas - representam as estruturas mais eficientes de análise da decisão de concessão de crédito. Com o estabelecimento de um filtro capaz de selecionar os bons e maus pagadores, torna-se possível oferecer

[134] Lei 13.708/19. Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: (...) X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente

> taxas de juros personalizadas, de modo a corrigir as distorções de mercado supracitadas"[135]

As falhas informacionais na concessão do crédito incorrem em seleção adversa, na fase pré-contratual, e em falhas de mercado, especialmente em informação ou ação oculta, após o entabulamento do contrato.

Assim, a assimetria de informação no mercado de crédito enseja a majoração dos custos de transação e o uso de ferramentas de mitigação geram prejuízos replicados a toda sociedade, cenário que o compartilhamento de dados no *open finance* tem o condão de minimizar, o que se mostra salutar ante os custos sociais envolvidos.

Nessa ótica, a abordagem a respeito da proteção ao crédito perpassa, obrigatoriamente, os modelos de avaliação de crédito, comumente conhecidos pela sua espécie *credit scoring*, razão pela qual será adotada referida terminologia.

O uso de metodologia de análise de crédito é juridicamente amparado pelo Código de Defesa do Consumidor[136] e pela Lei do Cadastro Positivo[137] e foi reconhecido quando do julgamento proferido em sede de recurso repetitivo pelo Superior Tribunal de Justiça (STJ) nos autos do Recurso Especial nº 1.419.697[138], após a primeira audiência pública da história deste Tribunal, o qual culminou na Súmula 550, cujo conteúdo autoriza a adoção de um critério consubstanciado em pontuação para a avaliação do risco de crédito.

> Súmula 550 do STJ:
> A utilização do escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo. STJ. 2 Seção. Aprovada em 14.10.2015.

Note-se que a importância do referido julgamento para a proteção de dados pessoais vai além da declaração de licitude quanto ao uso de *credit scoring*, e recai, sobretudo, nas razões de decidir, cuja essencialidade ao tema impõe sua transcrição:

> "De um lado, a metodologia em si de cálculo da nota de risco de crédito (*credit scoring*) constitui segredo da atividade empresarial, cujas fórmulas matemáticas e modelos estatísticos naturalmente não precisam ser divulgadas (art. 5º, IV, da Lei 12.414⁄2011: (...) resguardado o segredo empresarial). De

[135] COLAÇO. Hian Silva; SAMPAIO. Carolina Vasques. Direito à autodeterminação informativa no mercado de créditos: análise econômica do cadastro positivo de dados no Resp. 1419697/RS. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/1493-3489-1-sm.pdf. Acesso em 26 de junho de 2022.

[136] BRASIL. Lei 8.178/1990.

[137] BRASIL. Lei nº 12.414/2011.

[138] Superior Tribunal de Justiça. 2ª seção. Acordão do Recurso Especial nº 1.419.697-RS, Relator Ministro Paulo de Tarso Sanseverino. Julgado em 12.11.2014. Publicação em 17.11.2014

> outro lado, não se pode exigir o prévio e expresso consentimento do consumidor avaliado, pois não constitui um cadastro ou banco de dados, mas um modelo estatístico. Com isso, não se aplica a exigência de obtenção de consentimento prévio e expresso do consumidor consultado (art. 4º). Isso não libera, porém, o cumprimento dos demais deveres estabelecidos pelo CDC e pela lei do cadastro positivo, inclusive a indicação das fontes dos dados considerados na avaliação estatística, como, aliás, está expresso no art. 5º, IV, da própria Lei nº 12.414/2011 (São direitos do consumidor cadastrado ... conhecer os principais elementos e critérios considerados para a análise do risco de crédito, resguardado o segredo empresarial)"

A decisão em apreço fornece importantes fundamentos jurídicos ao debate sobre proteção de dados pessoais, notadamente, (i) a qualificação do sistema de *credit scoring* não como um banco do dados, mas sim como uma metodologia de cálculo que utiliza modelos estatísticos e dados existentes no mercado, o que afasta a exigência de prévia obtenção do consentimento do titular; (ii) o reconhecimento da natureza de segredo empresarial a esta metodologia de cálculo, atribuindo-lhe a proteção correlata; (iii) incidência dos princípios gerais do código de defesa do consumidor, em especial a transparência e boa-fé; (iv) reconhecimento do direito à autodeterminação informativa.

O cotejo da LGPD com a decisão paradigma em apreço identifica importantes pontos de convergência, em especial a confirmação da licitude do uso de metodológicas para análise de crédito (artigo 7º, X, da Lei nº 13.709/18), proteção ao segredo industrial (artigo 6º, VI da Lei nº 13.709/18) e coerência principiológica (artigo 6º da Lei nº 13.709/18).

Com efeito, a base legal de proteção de crédito está alinhada com a atual interpretação jurisprudencial aplicável a matéria. Desse modo, o atual arcabouço jurídico protetivo dos dados pessoais não apresenta o condão de alterar o entendimento atual e obstar o uso dessa ferramenta metodológica para a concessão de crédito.

A base legal de proteção ao crédito, portanto, permite o tratamento de dados pessoais com vistas ao escrutínio da capacidade de pagamento do titular de dados, e, por tal razão confere sustentáculo jurídico as atividades dos birôs de crédito, que oferecem, por exemplo, serviços de análise de crédito com base nos dados que controlam, e cujo acesso a tais dados deu-se pelas mais diversas formas.

Diante do entendimento pacificado quanto a forma de atuação dos birôs de crédito e demais atividades embasadas no tratamento de dados sob a ótica da proteção ao crédito, mostra-se juridicamente possível estender tal entendimento às instituições receptoras dos dados no *open finance*.

Assim, após a internalização dos dados pessoais obtidos via *open finance,* eles podem ser submetidos a análises creditícias, sob a base legal de proteção ao crédito, sem a imposição

dos limites do consentimento outorgado, ainda que a doutrina pugne por algumas adequações sob a ótica das decisões automatizadas e do *profiling*[139], a ser detalhado no tópico seguinte.

3.4 DECISÕES AUTOMATIZADAS E *PROFILING* NO *OPEN FINANCE*

Antes de detalhar as precauções devidas ante às decisões automatizadas e o *profiling*, mister destacar que embora possam integrar um mesmo processo, não são etapas indissociáveis.

A decisão automatizada é a tomada de decisão sem a intervenção humana, lastreada em diversos tipos de dados, dentre os quais podem (ou não) estar presentes os dados de perfilamento.

Da mesma sorte, a definição do perfil pode decorrer de uma análise automatizada de dados ou mediante intervenção humana. "O profiling é, assim, a técnica que resulta na produção desse perfil, e outras ferramentas de tomada de decisões automatizadas poderão usá-lo como objeto de avaliação."[140]

E, por fim, uma decisão não automatizada pode valer-se da definição de perfil, identificado de modo automatizado ou não. A título de exemplo, a decisão tomada pelo gerente de um banco de conceder crédito ao cliente, balizada pelo parâmetro do *credit scoring*.

Feitas as devidas distinções, consigna-se que as decisões automatizadas são expressamente tuteladas por meio do artigo 20 da LGPD[141] e artigo 22 do GDPR[142], os quais

---

[139] Profiling é um processo de correlação entre dados em bancos de dados que podem ser usados para identificar e representar um sujeito humano ou não humano (indivíduo ou grupo) e/ou aplicação de perfis (conjunto de dados correlacionados) para individualizar e representar um sujeito ou identificar um sujeito como integrante de um grupo ou categoria (Tradução livre. HILDEBRANDT. Mireille. Defining Profiling: A New Type of Knowledge? Profiling the European Citizen: Cross Disciplinary Perspectives. Cham: Springer Science, 2008. p.19.

[140] MARTINS. Pedro Bastos Lobo. Profiling na Lei Geral de Proteção de Dados: o livre desenvolvimento da personalidade em face da governamentalidade algorítmica. Coord. Brunello Souza Stancioli. Indaiatuba – SP. Editora Foco. 2022. p. 98.

[141] Lei 13.709. 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.

[142] Decisões individuais automatizadas, incluindo definição de perfis: O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.

O n.o 1 não se aplica se a decisão: a) For necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento; b) For autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou c) For baseada no consentimento explícito do titular dos dados.

Nos casos a que se referem o n.o 2, alíneas a) e c), o responsável pelo tratamento aplica medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, designadamente o

conferem maior carga protetiva para situações desta espécie, bem como preveem a possibilidade de revisão para os casos de tomada de decisão totalmente automatizada. Outrossim, tais previsões legais não se mostraram suficientes para estancar os debates referentes ao tema.

Isto porque, o grau de participação humana necessária à descaracterização da decisão automatizada e, portanto, mitigação da carga protetiva, ainda padece de contornos objetivos.

O Article 29 Working Party (WP29)[143] enfrentou o tema, à época sob a égide do Regulamento 2016/679, ocasião na qual externalizou o entendimento que a participação humana deve ser relevante e não meramente simbólica, executada por quem detenha autoridade e competência para alterar a decisão e cuja análise pondere todos os dados pertinentes. A avaliação de impacto sobre a proteção de dados (AIPD) deverá, ainda, identificar e registrar o grau de intervenção humana e a fase na qual é realizada.[144]

Persiste, porém, o debate sobre o conceito de decisão automatizada em processos decisórios complexos, nos quais decisões intermediárias automatizadas tenham o condão de interferir na decisão final, tomada pelo agente humano.

Para o enfrentamento de tal celeuma, sobressaem a abordagem subsidiária, para qual a análise do grau de automatização deve recair sob o último ponto da árvore de decisão, ou seja, apenas a decisão final deve ser escrutinada quanto ao seu nível de participação humana, e, por outro lado, a abordagem contrafactual, na qual todos os pontos da árvore de decisão que afetam significativamente a decisão final devem ser verificados sob o espectro de sua automatização[145].

A primeira abordagem implica retirar do espectro de atuação da proteção de dados pessoais decisões automatizadas intermediárias que repercutem, de maneira relevante, na tomada da decisão final, com potencial de eventuais violações permanecerem à sombra, inalcançáveis pela tutela jurídica.

---

direito de, pelo menos, obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão.

As decisões a que se refere o n.o 2 não se baseiam nas categorias especiais de dados pessoais a que se refere o artigo 9.o, n.o 1, a não ser que o n.o 2, alínea a) ou g), do mesmo artigo sejam aplicáveis e sejam aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular. (Versão em português de Portugal. Disponível em: https://gdprinfo.eu/pt-pt. Acesso em 27 de dezembro de 2022).

[143] Órgão consultivo criado pela Diretiva 95/46/CE responsável pelas questões referentes à proteção de privacidade e dados pessoais. Extinto em 25 de maio de 2018, com a entrada em vigor da GPDR, que criou o European Data Protection Board.

[144] Disponível em: https://ec.europa.eu/newsroom/article29/items/612053/en. Acesso em 27 de dezembro de 2022.

[145] VEALE. Michael. Governing machine learning that matters. 2019. Tese de Doutorado em Science, Tecnhology, Engineering and Public Policy. University College London. Londres. 2019.

Já a abordagem contrafactual tem o condão de expandir as cautelas aplicáveis à tomada de decisão para todo e qualquer tratamento de dados, majorando a carga protetiva incidente neste último, com provável elevação dos custos de transação e comprometimento dos avanços tecnológicos impulsionados, sobretudo, pelo uso da *big data*. Especificamente na seara do *open finance*, tal entendimento resultaria na redução do potencial de criação de novos modelos de negócios, ante o cerceamento no tratamento dos dados.

Diante das fragilidades de ambas as abordagens, a doutrina pátria, à luz da expressão "*que afetem seus interesses*" contida no artigo 20 da LGPD, propõe que a decisão automatizada, intermediária ou final, seja sopesada conforme o seu grau de repercussão nos direitos do titular dos dados.

> "O exercício de direitos não pode se condicionar ao critério de automação total ou parcial, mas sim de afetação de interesses dos titulares. Decisões intermediárias que visam unicamente a automatizar processos de gestão podem contar com uma regulação mais flexível. Por outro lado, decisões intermediárias usadas para prever ou avaliar o comportamento de sujeitos mostram-se especialmente relevantes pelo critério do risco. Caso essa previsão e avaliação condicione o acesso desse sujeito a bens, direitos ou serviços (como a avaliação de crédito), o grau de risco mostra-se ainda mais elevado"[146]
>
> "Portanto, a partir da interpretação da redação do art. 20, caput, há o reconhecimento de que as proteções concedidas pela LGPD às decisões automatizadas incluem as decisões intermediárias. Isso porque, conforme argumentado, decisões intermediárias que aconteçam de forma automatizada e que ofereçam riscos aos direitos e liberdades fundamentais dos titulares (ou seja, afetem os seus interesses) devem atrair garantias legais".[147]

Nessa perspectiva, embora a proteção ao crédito figure como uma base legal para o tratamento de dados pessoais, o caráter decisório relevante do *profiling*, sobretudo nas metodologias de análise de crédito como o *credit scoring* (ainda que normalmente figurem como decisões intermediárias), enseja o direito ao titular dos dados de solicitar a revisão das decisões lastreadas em tais perfilamentos, consoante interpretação dada ao artigo 20 da LGPD.

Para além do direito à revisão das decisões automatizadas, sobretudo, na seara do *credit scoring*, defende-se o desenvolvimento de um sistema capitaneado pelo órgão regulador para aferição de eventual potencial discriminatório, resguardado o segredo comercial (códigos e fórmulas matemáticas utilizados), bem como uma ferramenta aberta para estudos públicos sobre correlações e inferências das metodologias de crédito, aspectos até o presente momento

[146] Martins, Pedro Bastos Lobo. Op.cit. p. 51-52.
[147] Martins. Pedro Bastos Lobo. Op. cit. p. 104.

não incorporados na legislação protetiva de dados pessoais e tampouco presentes na regulamentação do *open finance*[148].

Sedimentado os limites das decisões automatizadas, do uso do perfilamento de clientes, especificamente quanto as metodologias de análise de crédito, sob a ótica da proteção de dados pessoais, o próximo passo recai sobre suas implicações no *open finance*.

Com vistas a dimensionar a potencialidade de violação dos direitos a proteção de dados no *open finance*, necessário reforçar a visão contemporânea sobre o direito à autodeterminação informativa, que abrange o papel de protagonista do titular dos dados também na construção de sua subjetividade (e, portanto, não restrito ao controle do fluxo de seus dados, ou seja, não apenas como zelador de sua privacidade, resguardando ou consentindo com o tratamento).

Nessa dimensão, o direito à autodeterminação informativa é indevidamente impactado pela governança algorítmica promovida por instrumentos como as decisões automatizadas e o *profiling*, a despeito do prévio consentimento do titular quando do compartilhamento de seus dados.

> "Por esse motivo, abordagens que buscam empoderar o sujeito apenas quanto à capacidade de compartilhar ou não determinados dados encontram limitações. Os possíveis usos secundários para o mesmo conjunto de dados, especialmente por meio de técnicas de aprendizagem de máquina, são virtualmente ilimitados e possuem impactos reais na identidade do sujeito. (...) parece haver algo ainda mais fundamental, ligado a como o sujeito consegue (ou deixa de conseguir) participar nos processos de afirmação de sua identidade, de como terceiros irão determinar elementos de sua identidade de forma unilateral, criando uma assimetria ainda mais forte entre as partes"[149].

Repise-se que a regulamentação do *open finance* está adstrita aos tempos e movimentos praticados no compartilhamento de dados entre as instituições participantes, para os quais são medidas imperiosas a obtenção do prévio consentimento e adoção das cautelas no uso de ferramentas de *profiling*, fortemente difundidas e estimuladas para a concretização dos objetivos do sistema financeiro aberto, sobretudo o desenvolvimento de novos modelos de negócios e fomento a competitividade.

Outrossim, após a internalização dos dados cadastrais e transacionais pela instituição receptora, o entendimento majoritário converge para a incidência das regras de proteção de dados preconizadas pela Lei Geral de Proteção de Dados, permanecendo a autorização e os limites para o tratamento de dados para fins de proteção ao crédito.

---

[148] Citron, Danielle Keats e Pasquale, Frank A., The Scored Society: Due Process for Automated Predictions (2014). Washington Law Review, Vol. 89, 2014, p. 1-, U of Maryland Legal Studies Research Paper No. 2014-8. Disponível em SSRN: https://ssrn.com/abstract=2376209. Acesso em 07 de janeiro de 2023.

[149] Martins. Pedro Bastos Lobo. Op. Cit. p. 69-70.

Sob a ótica do debate a respeito do alcance do consentimento no *open finance* e a possibilidade do uso dos dados para fins diversos daqueles pretendidos quando consentido o compartilhamento, em eventual afronta ao princípio da finalidade, possível argumentar que a redação da Lei nº 12.414/2011, dada pela Lei Complementar 166/2019, limita eventual objeção do usuário ao uso de seus dados para fins eminentemente de análise de crédito.

Isto porque, referida alteração legislativa revogou o modelo *opt-in*, aquele que exige o consentimento formalizado para a inclusão dos dados no cadastro positivo, vigendo hodiernamente a dispensa de autorização do avaliado para fins de abertura de seu cadastro de crédito.

Desse modo, conquanto os debates sobre a matéria ainda estejam em estágio embrionário, o regime jurídico de proteção aos dados pessoais, em interpretação sistemática a todo o arcabouço jurídico, permite antever a viabilidade do tratamento de dados compartilhados no *open finance* para fins de proteção do crédito. E, nesse espectro, em modelos de avaliação de crédito, independentemente do consentimento para tanto e da vinculação à finalidade do compartilhamento, ressalvado o direito à revisão das decisões automatizadas, inclusive àquelas afetas ao perfilamento.

Outrossim, tal assertiva não afasta a crescente preocupação sobre o intenso fluxo de dados pessoais e a seleção daqueles que alimentam o modelo estatístico, pois "para além do acesso à informação e boa-fé, o que está em jogo é a justificação de decisões automatizadas, os limites da utilização de dados pessoais e os potenciais discriminatórios desses sistemas"[150].

Nesse sentido, note-se que o caso jurisprudencial paradigmático também apresenta fundamentos hábeis a nortear o estudo:

> "Devem ser prestadas também as informações pessoais do consumidor avaliado que foram consideradas para que ele possa exercer o seu direito de controle acerca das informações excessivas ou sensíveis, que foram expressamente vedadas pelo art. 3o, § 3o, I e II, da própria Lei no 12.414/2011. Não podem ser valoradas pelo fornecedor do serviço de "creditscoring" informações sensíveis, como as relativas à cor, à opção sexual ou à orientação religiosa do consumidor avaliado, ou excessivas, como as referentes a gostos pessoais, clube de futebol de que é torcedor etc". (STJ – Resp. 1419697 RS 2013-0386285-0. Relator Ministro Paulo de Tarso Sanseverino. Data do julgamento 12.11.2014. Segunda seção. Data de Publicação 17.11.2014).

Para ilustrar os riscos do uso de dados no setor financeiro, salutar a publicação do *The Center for Investigative Reporting (CIR)*, organização de jornalismo investigativo sem fins

---

[150] DONEDA. Danilo. ZANATTA. Rafael. O que há de novo no debate "credit score" no Brasil? Direitos são conhecidos e efetivamente exercidos pelos consumidores? Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/o-que-ha-de-novo-no-debate-credit-score-no-brasil-09022017. Acesso em 20 de agosto de 2022.

lucrativos, sobre o maior índice de negativa de concessão de crédito para financiamento da casa própria à latinos e negros pelos bancos norte-americanos, evidenciando a sensibilidade no uso de dados para a tomada de decisões automatizadas na concessão de crédito, notadamente pela replicação exponencial de preconceitos estruturais da sociedade por meio da parametrização algorítmica[151].

No cenário nacional, similar viés discriminatório foi identificado pela pesquisa elaborada por Ramon Vilarino e Renato Vicente, na qual os três primeiros dígitos do Código de Endereçamento Postal (CEP) foram alterados, promovendo a mudança de endereço dos avaliados do estado de São Paulo (onde 36% da população se autodeclara não branca) para a Bahia (onde 78% da população se autodeclara não branca), mantendo-se todas as demais variáveis. Referida alteração demonstrou viés racial discriminatório por meio da localização geográfica, evidenciado pela redução da pontuação de crédito em 99,8% dos casos analisados[152].

Note-se que o tema atrai a potencialidade de que dados pessoais sejam qualificados como dados sensíveis em face dos efeitos do tratamento a que foram submetidos, caso infirmada a tese do rol taxativo, o que tem o condão de impactar na forma de operacionalização do *open finance*, ante os riscos de eventual tratamento sem o adequado consentimento do titular dos dados.

Contudo, ainda que sob a ótica do uso de dados anonimizados, mantém-se os contornos delicados, tornando necessária a perquirição, de forma cautelosa, sobre o conceito expansionista de dados pessoais e seu tratamento, com vistas a construir limites objetivos, claros e rígidos na adoção da inteligência analítica no tratamento de dados anonimizados, com análise minuciosa de eventual potencial discriminatório do algoritmo elaborado, além de pautar-se pelas exigências legais de razoabilidade, sob o prisma da tecnologia existente à época, bem como custo e tempo para sua reversão.

Considerando a regulamentação de dados sensíveis pela nova malha normativa de proteção de dados, em sentido sinérgico ao quanto decidido no acórdão paradigma, notadamente à luz do maior rigor ao tratamento de dados desta espécie, imperioso destacar que quando se aborda o uso de dados pessoais nos modelos de avaliação de crédito passa-se ao largo

---

[151] Disponível em: https://revealnews.org/podcast/the-red-line-racial-disparities-in-lending-2/. Acesso em 26 de junho de 2022.

[152] VILARINO, Ramon; VICENTE, Renato. Dissecting racial bias in a Credit Scoring System experimentally developed for the Brazilian population. arXivLabs. Nova Iorque. 2020. Disponível em: https://arxiv.org/abs/2011.09865. Acesso em 28 de dezembro de 2022.

de eventual autorização para tratamento de dados identificáveis sensíveis na parametrização das análises de crédito.

O uso de *big data* atrelado à maior facilidade de compartilhamento de dados traz novas preocupações sob a ótica do perfilamento dos usuários bancários para os mais diversos fins (tendo em vista a atual abrangência do *open finance*) e, mais especificamente, quanto ao *credit scoring,* tanto sob a ótica do potencial discriminatório como pela violação ao princípio da autodeterminação informativa.

Nesse ponto, o retro transcrito acórdão resguardou o direito do titular dos dados de controlar suas informações excessivas ou sensíveis. Embora seja uma decisão anterior à LGPD, nota-se um alinhamento entre seus ditames, notadamente o direito de acesso aos dados (artigo 18, II da LGPD), como de revisão das decisões automatizadas.

Desse modo, por quaisquer dos prismas, resta o dever das Instituições de informar os dados brutos que compõem o cadastro e de formular eventual revisitação das decisões (o que será melhor detalhado adiante), resguardado o sigilo empresarial, na forma preconizada na predita decisão e no artigo 18, V da LGPD, de tal sorte que os parâmetros das decisões e a valoração dos dados não estão abrangidos no dever de informação ao titular dos dados pessoais.

> "A exposição dos dados pessoais a pedido do titular não pode, por exemplo, implicar a revelação de fórmulas relativa aos cálcuos de avaliações de crédito dos clientes ou outros elementos intrinsecamente vinculados a seu modelo de negócios. Aliás, a mesma proteção aos segredos comercial e industrial é garantida também na LGPD aos critérios utilizados em decisões automatizadas, mesmo quando solicitados pelo titular dos dados."[153]

Agrega-se ao tema as pressuposições empíricas da sociedade e, especialmente, do Poder Judiciário, quanto aos Bancos terem capacidade técnica e elevado potencial econômico para investimento em eficiência na área de tecnologia da informação, o que tangencia uma expectativa pela infalibilidade, atrelada aos riscos advindos, sobretudo, da legislação consumerista quanto a inversão do ônus probatório, também previsto na própria LGPD, em seu artigo 42 §2º, bem como, em alguns casos, agravados pela competência atribuída aos juizados especiais e o dogma da inadmissibilidade do procedimento de produção de prova pericial em referido juízo.

---

[153] GOETTENAUER. Carlos. Open Banking e proteção de dados pessoais: convergências e divergências entre a LGPD e a regulação. In: Direito Público e Tecnologia. Coord. CRAVO. Daniela Copetti. JOBIM. Eduardo. JUNIOR. José Luiz de Moura Faleiros. Indaiatuba. Editora Foco. 2022. p. 89-90.

Outro aspecto da atual inteleção do direito à proteção de dados pessoais ante o perfilamento que exige atenção no *open finance* é a superação do modelo individualista e a evolução para um direito de caráter coletivo.

A coletivização do direito à proteção de dados tem o condão de mitigar o parâmetro de identificabilidade dos dados (inclusive em sua concepção expansionista) e trazer maior rigor para as atividades de tratamento de dados anonimizados e, sobretudo, de perfilamento. Isto porque, a visão coletiva do direito à proteção de dados pessoais atrai a preocupação para "os interesses coletivos das pessoas cujos dados estão sendo analisados e agrupados. A natureza distinta desses grupos de indivíduos exige uma abordagem que não pode ser exclusivamente baseada em direitos individuais"[154].

Tal preocupação coaduna-se ao crescimento vertiginoso do uso de Big Data e tratamento massivo de dados e suas potenciais interferências, ainda que veladas e silenciosas, na construção da subjetividade do titular de dados, sobretudo pelas atividades de perfilamento.

> "Se a premissa da causa regulatória da proteção de dados pessoais é tutelar o cidadão, que é cada vez mais exposto a tais tipos de práticas que afetam sua vida, então, uma compartimentalização dura entre dados pessoais e dados anonimizados deixaria de fazer sentido. Em especial, quando está em questão a formação de perfis comportamentais que tem por objetivo precípuo influenciar de alguma forma a vida de uma pessoa, que está atrás de um dispositivo e pouco importa ser ela identificável ou não"[155].

A superação da dicotomia entre dado pessoal e dado anonimizado é apresentada por Bruno Bioni por meio da adoção de uma abordagem consequencialista, pela qual deve-se aferir a interferência do tratamento nos interesses do titular, independentemente de sua identificação ou não durante tal tratamento[156]. Trata-se de interpretação similar àquela proposta ao artigo 20 da LGPD, ainda que no presente caso elaborada sem amparo no texto legal e com aplicação não restrita ao exercício de um direito individual.

No cenário pátrio, destaca-se, ainda, o histórico de uma estrutura jurídica de prestígio à tutela dos interesses difusos, denominada microssistema de tutela dos interesses transindividuais[157], formada pela Lei das Ações Civis Públicas (Lei nº 7.447/1985) e pelo Código de Defesa do Consumidor (Lei nº 8.078/1990), em aderência aos preceitos constitucionais que também versam sobre o tema.

---

[154] MANTELERO, Alessandro. Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. Computer Law & Security Review, v. 32, n. 2, p. 246.

[155] BIONI. Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro. Forense. 2019. p.76.

[156] BIONI. Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites de consentimento. 2 ed. Rio de Janeiro. Forense. 2019.

[157] Denominação adotada pelo Ministro Luiz Fux.

Aliada a tal tradição, a própria LGPD sinaliza, ainda que de modo tímido, com a possibilidade do exercício da tutela coletiva dos direitos dos titulares dos dados, em seus artigos 20, 22 e 42 §3º.

Esse arcabouço jurídico voltado à tutela coletiva mostra-se hábil à articulação das ferramentas em prol da proteção dos dados pessoais e, sobretudo, da sedimentação de seu caráter coletivo, o que tende a impulsionar a adoção dos procedimentos administrativos e judiciais voltados a proteção coletiva, notadamente por meio de entidades representativas e institucionais, reduzindo a assimetria informacional e de poder existente entre controladores/operadores de dados e seus titulares.

> "Em síntese, a partir da leitura conjunta do art. 22 com o art. 42 da LGPD, bem como os dispositivos da Lei da Ação Civil Pública e do Código de Defesa do Consumidor, pode-se afirmar com segurança que a legislação brasileira (i) permitirá uma atuação repressiva, em nível administrativo, para a tutela da proteção de dados pessoais, valendo-se do microssistema de proteção dos direitos difusos, (ii) fomentará a atuação de entidades civis especializadas e do Ministério Público na tutela dos direitos difusos de proteção de dados pessoais, por meio do poder judiciário, e (iii) possibilitará o uso de um ferramental do processo civil brasileiro para interrupção de violações de direitos assegurados na LGPD, tornando a dinâmica regulatória mais complexa. De fato, o *enforcement* se dará não só pela Autoridade Nacional de Proteção de Dados, mas também por meio de desse arranjo de atores institucionais dedicados à tutela coletiva da proteção de dados pessoais"[158].

A coletivização do direito à proteção de dados pessoais atrelado ao prognóstico de um arsenal jurídico nacional voltado a tutela difusa de tal direito carece, até o presente momento, de um sopesamento pela regulamentação do open finance, ainda fortemente arraigado à base legal do consentimento, "sendo papel dos reguladores observarem a transparência e o provimento de informações contratuais aos consumidores para adotarmos uma concepção fundada na integridade contextual"[159].

---

[158] ZANATTA. Rafael. SOUZA. Michel R. A tutela coletiva na proteção de dados pessoais: tendências e desafios. In: DE LUCCA, Newton; ROSA, Cíntia. Direito & Internet IV: Proteção de Dados Pessoais. São Paulo. Quartier Latin. 2019. Disponível em: https://www.researchgate.net/publication/344495215_A_Tutela_Coletiva_em_Protecao_de_Dados_Pessoais_tendencias_e_desafios/link/5f7c85dd458515b7cf6a54bc/download. Acesso em 02 de janeiro de 2023.

[159] ZANATTA. Rafael. SOUZA. Michel R. A tutela coletiva na proteção de dados pessoais: tendências e desafios. In: DE LUCCA, Newton; ROSA, Cíntia. Direito & Internet IV: Proteção de Dados Pessoais. São Paulo. Quartier Latin. 2019. Disponível em: https://www.researchgate.net/publication/344495215_A_Tutela_Coletiva_em_Protecao_de_Dados_Pessoais_tendencias_e_desafios/link/5f7c85dd458515b7cf6a54bc/download. Acesso em 02 de janeiro de 2023

Em que pese a lacuna normativa, não se pode fechar os olhos diante do potencial de judicialização, em seara coletiva, do tratamento de dados pessoais a ser realizado no open finance para a concretização de seus valorosos objetivos.

Desse modo, mostra-se, de todo recomendável, que o Relatório de Impacto à Proteção de Dados Pessoais do *open finance* abranja todas as atividades de perfilamento (inclusive metodologias de análise de crédito e perfis de consumo para novos modelos de negócios), ainda que desenvolvidas com dados anonimizados, ressalvadas as devidas cautelas afetas ao segredo comercial, para fins de demonstração da licitude das atividades, com vistas a defesa das instituições participantes e, especialmente, para resguardar a credibilidade e confiabilidade do sistema aberto.

Ainda que os debates sobre o perfilamento e os riscos de afronta aos preceitos da autodeterminação informativa (dada sua potencialidade de comprometer o livre desenvolvimento da personalidade humana) tenham destaque, sobretudo, na seara da publicidade comportamental, os riscos quanto ao *open finance* são latentes, especialmente ante o potencial de judicialização da matéria e, portanto, exigem mapeamento para salvaguarda dos direitos individual e coletivos e atuação regulatória.

Os potenciais riscos do open finance, à luz da proteção de dados pessoais, mapeados no presente capítulo são sintetizados no quadro abaixo, com vistas a estruturar a propositura de ações mitigadoras de tais riscos, a serem desenvolvidas a seguir.

Tabela 2 – Fatores de risco no open finance

Risco	Fatores de risco
Risco exógeno	Estrutura técnica – interface de interoperabilidade
Risco exógeno	Fraudes via engenharia social
Risco endógeno	Jornada do consentimento
Risco endógeno	Decisões automatizadas e *profiling*

Fonte: Elaboração própria.

4 RECOMENDAÇÕES DE BOAS PRÁTICAS PARA A PROTEÇÃO DOS DADOS PESSOAIS NO OPEN FINANCE

O caráter inovador do *open finance* atrelado à recente positivação do direito à proteção de dados pessoais obsta o mapeamento integral dos riscos que permeiam esse novo ecossistema, sendo certo que novos desafios e complexidades serão evidenciados na medida em que o acesso à ferramenta ganhe maior engajamento junto a sociedade.

Balizado em tal premissa, o presente estudo buscou identificar os principais riscos e desafios do *open finance*, na seara da proteção de dados pessoais, sem a pretensão de esgotá-los.

Não obstante, entende-se que os riscos aqui mapeados exigem monitoramento e ações propositivas, sob pena de entraves operacionais e jurídicos hábeis a inviabilizar o atingimento dos objetivos almejados pelo *open finance*.

Desse modo, propõe-se, de forma não exaustiva, as diretrizes interpretativas à regulação do *open finance*, em aderência ao arcabouço jurídico de proteção aos dados pessoais, bem como medidas estruturantes para mitigar os riscos advindos de eventual caracterização de tratamento indevido dos dados pelas instituições participantes do *open finance*, sintetizados no quadro abaixo e detalhados a seguir.

Tabela 3 – Riscos, fatores de riscos e ações mitigadoras dos riscos

Risco	Fatores de risco	Mitigadores de risco
Risco exógeno	Estrutura técnica – interface de interoperabilidade	API's seguras; estrutura de Governança e definicação regulatória das responsabilidades.
Risco exógeno	Fraudes via engenharia social	API's seguras e ações educativas.
Risco endógeno	Jornada do consentimento / Fadiga do consentimento	Adoção da teoria da integridade contextual, *Privacy by design e Privacy Enhancing Technologies (PETs), bem como e*conomia comportamental na arquitetura de escolha.
Risco endógeno	Decisões automatizadas e *profiling*	*Accountability*, uso de dados anonimizados e elaboração de Relatório de Impacto à Proteção de Dados Pessoais.

Fonte: Elaboração própria

4.1 RISCOS EXÓGENOS – SEGURANÇA DA INFORMAÇÃO

Conforme descrito no capítulo anterior, os principais desafios envolvendo segurança da informação no *open finance* dizem respeito ao desenvolvimento da interface tecnológica para a interoperabilidade e padronização mínima, de forma segura e confiável e, ao mesmo tempo, sem gerar custos demasiados, considerando a heterogeneidade das instituições participantes.

O aparato regulatório sobre segurança da informação e normas de segurança cibernética no setor financeiro ampara-se na Lei Complementar nº 105/01 (Lei do Sigilo Bancário)[160], Resolução nº 4.893/21[161], que trata da política de segurança cibernética e requisitos para contratação de serviços de processamento e armazenamento de dados em nuvem, bem como a Circular nº 3.909/18 (Normas de Segurança Cibernética)[162], núcleo que, numa perspectiva empírica, e atrelado ao contexto histórico de evolução do sistema financeiro nacional, forjou uma maturidade do segmento no uso da tecnologia e no enfrentamento de investidas fraudulentas.

Da mesma sorte, a adoção pela regulação do *open finance* de *Application Programming Interface (API)* como interface para estruturar o fluxo de dados entre as instituições mostra-se uma escolha regulatória acertada, posto que permite a interoperabilidade de forma simples, controlada e segura[163].

Não por outra razão, seu uso foi preconizado nas Diretrizes sobre o Direito à Portabilidade de Dados[164], é fortemente difundido nas empresas globais de tecnologia[165] e foi adotado como a estrutura técnica em diversos modelos de *open banking*, a exemplo de Singapura[166] e Reino Unido[167], ressalvadas as diferentes abordagens do órgão regulador de cada país quanto a forma orientativa (*supportive jurisdiction*) ou impositiva (*mandatory jurisdiction*) de construção e desenvolvimento de API's padronizadas.

---

[160] BRASIL, 2001.

[161] BANCO CENTRAL DO BRASIL, 2021.

[162] BANCO CENTRAL DO BRASIL, 2018.

[163] PREMCHAND, Anshu; CHOUDHRY, Anurag. Open Banking & APIs for Transformation in Banking. 2018 International Conference on Communication, Computing and Internet of Things (IC3IoT), IEEE, 2018, p. 25–29.

[164] ARTICLE 29. DATA PROTECTION WORKING PARTY, Guidelines on the right to data portability, October, p. 1–20, abr. 2017.

[165] MILANESI, Diana. A New Banking Paradigm: The State of Open Banking in Europe, the United Kingdom, and the United States. TTLF Working Papers, n. 29, 2017. Disponível em: http://ttlf.stanford.edu. Acesso em: 21 de janeiro de 2023.

[166] *Association of Banks in Singapore* – ABS. *Finance-as-a-service: API Playbook*.

[167] OPEN BANKING LIMITED, Open Banking Guidelines for Open Data Participantes. 2018

Portanto, sob a ótica regulatória, a estrutura técnica de segurança da informação adotada pelo *open finance* brasileiro está em harmonia com a experiência internacional e alinhada ao atual estado da técnica.

No mesmo sentido, a segurança e privacidade de dados e informações sobre os serviços compartilhados estão expressamente previstos como princípios do *open finance*[168], devendo, portanto, balizar a interpretação das normas e a definição de suas diretrizes técnicas.

Todo o arcabouço jurídico-regulatório aplicável às instituições integrantes do Sistema Financeiro Nacional, agregado às especificidades do *open finance* delineadas na Resolução Conjunta nº 32[169] e no Manual de API's, constantemente atualizado, mostram-se aptos a garantir a observância dos pilares da segurança da informação, a saber, integridade (impedir a alteração dos dados, preservando os dados em seu formato e conteúdo originais), confidencialidade (obstar o acesso das informações por pessoas não autorizadas) e disponibilidade (possibilidade de acesso aos dados sempre que solicitado/necessário).

Outrossim, a determinação regulatória de que os critérios técnicos das *API's* padronizadas sejam construídos pelas Instituições Participantes, por meio de Convenção, exigem iniciativas que impeçam que padrões tecnológicos de segurança da informação sejam utilizados como cláusula de barreira aos entrantes, costumeiramente com menor potencial aquisitivo para fazer frente aos custos de implementação do aparato técnico eventualmente exigido na Convenção. Assim, resta a necessidade de compatibilizar os padrões mínimos de segurança da informação com a possibilidade de ingresso de novos agentes, a exemplo de Fintechs.

Para o enfrentamento de tal risco, salutar a determinação de que a Convenção seja submetida à aprovação do órgão regulador[170], em que pese o caráter híbrido de tal modelo de regulação, afastando-se da preconizada autorregulação.

Da mesma sorte, a Estrutura de Governança do processo de implementação do *open banking*, denominação vigente à época, preocupou-se em zelar pela representatividade dos diferentes segmentos envolvidos no sistema financeiro aberto e no acesso não discriminatório, além de instrumentalizar mecanismos para mitigar e tratar eventuais conflitos de interesse,

---

[168] Art. 4º da Resolução Conjunta nº 1/2020. As instituições de que trata o art. 1º, para fins do cumprimento dos objetivos de que trata o art. 3º, devem conduzir suas atividades com ética e responsabilidade, com observância da legislação e regulamentação em vigor, bem como dos seguintes princípios: (...) II - segurança e privacidade de dados e de informações sobre serviços compartilhados no âmbito desta Resolução Conjunta.

[169] Resolução Conjunta n° 32. Banco Central do Brasil. Art. 2º. Para os fins do disposto nesta Resolução, considera-se: (...) III - Application Programming Interface (API): interface dedicada ao compartilhamento entre instituições participantes de dados e serviços do escopo do Open Banking

[170] Artigo 47 da Resolução Conjunta Bacen/CVM nº 1. O conteúdo da convenção de que trata o art. 44 deve ser submetido à aprovação do Banco Central do Brasil, respeitados os seguintes prazos.

mediante adoção de quóruns qualificados para deliberação, previsão do Conselheiro Independente, com direito ao voto de minerva, bem como possibilidade de o órgão regulador acompanhar as discussões do Conselho Deliberativo, conforme depreende-se da Circular 4.032 de 23 de junho de 2020.[171]

Nota-se, assim, uma estrutura regulatória apta a consubstanciar o princípio da não discriminação dos participantes, atenta e precavida em face de potenciais ações de reserva de mercado pelas principais instituições participantes, inclusive ante àquelas travestidas de precauções quanto a segurança da informação, aspectos que merecem estrita cautela quando da definição das diretrizes técnicas e supervisão do órgão regulador pautado em tal premissa.

Por outro lado, isso não significa que se pode minimizar a importância das medidas de segurança da informação, tanto pelo dever de cumprimento dos ditames legais, sobretudo da Lei do Sigilo Bancário e da LGPD, como pelo próprio sucesso do projeto, pois um ecossistema que garanta a segurança da informação é essencial para que os clientes bancários e/ou usuários sejam incentivados a aderir.

Nesse cenário, emerge a preocupação quanto às entidades não reguladas pelo Banco Central do Brasil e, portanto, não sujeitas às regras da Resolução nº 4.893/21[172], embora envolvidas no tratamento de dados via *open finance*, a exemplo de *marketplaces* ou plataformas de *banking-as-a-service.*

Ademais, a Resolução Conjunta nº 01/2020[173] não individualiza as condutas e respectivas responsabilidades das instituições participantes e demais envolvidos, configurando uma sensível lacuna regulatória.

Eventuais violações à proteção de dados pessoais nesse contexto demandam análise casuística via mapeamento do fluxo de dados, a serem submetidas às responsabilizações previstas na LGPD, identificando-se o papel desempenhado por cada ator envolvido (controlador ou operador de dados), bem como aos preceitos do Código de Defesa do Consumidor, sendo forçoso evidenciar a responsabilidade objetiva preconizada em ambos os diplomas legais.

Tal situação mostra a importância do mapeamento e rastreamento do fluxo de dados, com vistas a adequada individualização das condutas e respectivas responsabilidades (com o escopo de infirmar o pressuposto da conduta e/ou nexo causal na configuração da responsabilidade civil), sem prejuízo de eventual ação de regresso, se o caso.

---

[171] BANCO CENTRAL DO BRASIL. 2020.
[172] BANCO CENTRAL DO BRASIL, 2021.
[173] BANCO CENTRAL DO BRASIL, 2020.

Para além das cautelas por ora recomendáveis às instituições participantes do *open finance*, é prudente que a regulação trate de forma mais aprofundada sobre as responsabilidades das instituições participantes e entidades não autorizadas pelo Banco Central, definindo-se os limites de atuação, ainda que essas não estejam sob a jurisdição regulatória.

Esse aprofundamento da regulação nas responsabilidades de cada um dos envolvidos, proposta no parágrafo acima, não tem por escopo alcançar entidades não submetidas ao crivo do órgão regulador. Objetiva-se, tão somente, definir aspectos técnicos e operacionais do ecossistema, inclusive por meio da Convenção prevista no artigo 44 da Resolução Conjunta nº 1/2020, para delimitar a seara de atuação e, por conseguinte, viabilizar a individualização dos deveres e respectivas responsabilidades de cada um dos envolvidos.

Esclarece-se que, em caso de contrato de parceria nos moldes do artigo 36 da Resolução Conjunta nº 1/2020, firmado entre instituição autorizada pelo Banco Central do Brasil com entidade não autorizada, a responsabilidade é atribuída à instituição participante, respondendo pelos atos da entidade não autorizada, ainda que os atos de supervisão determinados na regulação tenham sido adequadamente implementados, sem prejuízo de eventual ação de regresso.

Outro aspecto salutar da segurança da informação remonta às precauções necessárias para o enfrentamento da crescente criminalidade cibernética, realidade que pode afetar todo o Sistema Financeiro Nacional, não restrito ao *open finance*.

À guisa de exemplo, em 2021, o investimento dos bancos em tecnologia alcançou o patamar de R$ 30,1 bilhões, incremento de 13% em comparação ao ano anterior. Os dados de 2022 ainda não foram divulgados, porém, a estimativa era de R$ 35,5 bilhões, com prioridade de destinação de tais recursos para as áreas de segurança cibernética, inteligência artificial, 5G, computação em nuvem, e *big data*.[174]

Necessário pontuar que, no levantamento realizado pela Delloite, sob encomenda da Febraban, o *open finance* é apontado como um dos propulsores desse aumento dos recursos investidos em tecnologia, no ano de 2021, em virtude de o compartilhamento de dados demandar aprimoramento em inteligência artificial, computação em nuvem e segurança cibernética, bem como construção de interfaces que propiciem uma melhor experiência do usuário[175].

---

[174] https://cmsarquivos.febraban.org.br/Arquivos/documentos/PDF/pesquisa-febraban-2022-vol-2.pdf. Acesso em 02 de janeiro de 2023.

[175] https://cmsarquivos.febraban.org.br/Arquivos/documentos/PDF/pesquisa-febraban-2022-vol-2.pdf. Acesso em 02 de janeiro de 2023.

Conquanto os massivos investimentos, a Febraban aponta que o Brasil responde por 18% das investidas criminosas por engenharia social da América Latina, ocupando o segundo lugar nesse malfadado ranking[176].

Nesse aspecto, evidencia-se que 70% dos ataques cibernéticos valem-se da engenharia social, que envolve a manipulação ou indução do usuário pelo criminoso para o fornecimento de informações confidenciais, e não de fragilidades do sistema em si[177], o que evidencia a necessidade de ações educativas mais robustas para que a sociedade seja instruída sobre como bem se proteger.

Conquanto não se ignore as boas práticas já promovidas pela Febraban em prol da conscientização da população, como a Semana da Segurança Digital[178], a campanha intitulada "Pare & Pense #pode ser golpe"[179] e a cartilha sobre engenharia social[180], além de ações destinadas a coibir as práticas delituosas, como o Acordo de Cooperação Técnica firmado junto a Polícia Federal (Convênio Tentáculos) e apoio à Lei nº 14.155/21[181], que fixou penas mais severas para crimes praticados por meios digitais[182], tais ações ainda são tímidas ante a dimensão do desafio a ser enfrentado e merecem serem estruturadas de forma a atingirem uma maior penetração junto a sociedade em geral.

Assim, com a expansão dos novos modelos de negócios digitais e a almejada majoração do engajamento dos clientes bancários/usuários no *open finance*, recomenda-se que as ações educativas ganhem maior propulsão e apelo massificado, sendo certo que os próprios bancos, em ações individuais, podem assumir tal protagonismo, ensejando, inclusive, ganhos de imagem mediante o fortalecimento de sua credibilidade, confiabilidade e responsabilidade para com seus clientes.

---

[176] https://tiinside.com.br/05/09/2022/o-aumento-do-crime-financeiro-no-brasil-a-inteligencia-artificial-do-lado-do-banco-e-do-consumidor/. Acesso em 02 de janeiro de 2023.

[177] https://tiinside.com.br/05/09/2022/o-aumento-do-crime-financeiro-no-brasil-a-inteligencia-artificial-do-lado-do-banco-e-do-consumidor/. Acesso em 02 de janeiro de 2023.

[178] https://febrabantech.febraban.org.br/temas/seguranca/febraban-e-26-bancos-promovem-semana-da-seguranca-digital-e-orientam-populacao-sobre-golpes. Acesso em 02 de janeiro de 2023.

[179] https://antifraudes.febraban.org.br/. Acesso em 02 de janeiro de 2023.

[180] https://cmsarquivos.febraban.org.br/Arquivos/documentos/PDF/cartilha_eng_social_atualizada_20.pdf. Acesso em 02 de janeiro de 2023.

[181] BRASIL. 2021.

[182] https://exame.com/future-of-money/cybersecurity/com-apoio-de-bancos-governo-endurece-pena-para-crimes-ciberneticos/. Acesso em 02 de janeiro de 2023.

4.2 RISCOS ENDÓGENOS

Os riscos endógenos (ainda que possam se consubstanciar em diversas facetas, conforme detalhado no capítulo anterior do presente trabalho) têm por cerne a legitimidade do consentimento a ser obtido junto ao titular dos dados e os limites de tal consentimento.

Em que pesem os riscos advindos da base legal do consentimento, sobretudo ante ao contexto social que evidencia a famigerada *fadiga do consentimento*, levando a desvalorização do instituto, consigna-se, de antemão, o acerto da regulação em prestigiar o consentimento para o tratamento de dados pessoais no *open finance*, especificamente no que tange à relação entre titulares de dados pessoais e as Instituições participantes do ecossistema.

Assente o entendimento de que o tratamento de dados pessoais em sede de *open finance* deve observar, obrigatoriamente, uma das bases legais previstas na LGPD, a imersão nas demais hipóteses potencialmente elegíveis corrobora a escolha feita pelo órgão regulador.

Isto porque, todas as demais bases legais para tratamento de dados pessoais prescindem do consentimento do titular e, se adotadas, alterariam, sensivelmente, as condições de confidencialidade vigentes por ocasião do fornecimento dos dados pelo titular à Instituição Financeira.

Apenas o consentimento prestigia a autodeterminação informativa do titular dos dados e resguarda os interesses daqueles titulares que outorgaram seus dados às Instituições Financeiras sob a batuta da confidencialidade inerente ao sigilo bancário e não desejam alterar esse cenário, sobretudo mediante compartilhamento de seus dados com demais instituições com as quais o titular não pretenda construir uma relação negocial.

Conquanto o compartilhamento forçado dos dados seja uma ação pró-fomento da concorrência, seu enquadramento na doutrina de infraestrutura essencial é controvertido diante da dificuldade de uma precificação assertiva e elevados custos de implementação e operacionalização. E, sob a ótica da proteção dos dados pessoais, tanto o legítimo interesse como o cumprimento de obrigação regulatória não devem ignorar a necessidade de um alinhamento com os interesses dos próprios titulares dos dados de verem seus dados utilizados como insumos para medidas concorrenciais[183].

[183] MOURAO. Carlos. Novaes. Leandro. A proteção de dados pessoais à luz do Direito Concorrencial: Portabilidade de dados, Infra estruturas essenciais e Open Banking in Revista de Direito à Concorrência. Cade. Volume 8. Nº2. Dezembro de 2020. Disponível em: https://revista.cade.gov.br/index.php/revistadedefesadaconcorrencia/issue/download/26/59. Acesso em 03 de setembro de 2023.

Não menos importante, o consentimento guarda aderência ao arcabouço jurídico aplicável aos dados bancários, em especial os ditames do sigilo bancário, sobretudo ao artigo 1º, §3º, V, da Lei Complementar 105/01, que exige o consentimento expresso do titular para que as Instituições Financeiras possam revelar os seus dados. Assim, mantém-se a coerência do sistema jurídico-normativo e evitando-se eventuais debates e judicializações da regulação em virtude de suposta inobservância da Lei do Sigilo Bancário.

Reforce-se aqui, apenas, o entendimento pela viabilidade de maior incentivo pela regulação ao tratamento de dados anonimizados no *open finance*, especialmente nos contratos de parceria, o que se mostra potencialmente mais eficiente no desenvolvimento de novos modelos de negócios, afastando-se das celeumas do consentimento, sem prejuízo, por óbvio, da rigorosa regulação técnica dos requisitos da (in) reversibilidade.

Adentrando-se aos meandros da estruturação do consentimento, compreende-se a acerto da regulação, sob a ótica concorrencial em preconizar o início do compartilhamento de dados no *open finance* mediante consentimento a ser outorgado à instituição receptora dos dados, que realizará a chamada de interface para requisitar os dados, desenho regulatório que mitiga os conflitos de interesses e incentivos negativos da instituição transmissora de dados em acolher tais adesões.

A regulação ainda exige que a jornada do consentimento, que abrange as etapas do consentimento do cliente, autenticação e confirmação, aconteça pelos canais digitais das instituições participantes, previsão que, à primeira vista, mostra-se coerente à ideia de facilitar o acesso e a experiência do cliente no *open finance*.

Outrossim, identificou-se a externalidade de maiores dificuldades no compartilhamento de dados em duas relevantes situações: (i) por clientes novos, ou seja, aqueles que pretendem compartilhar seus dados com instituições receptoras com as quais ainda não possuem relacionamento, com entraves na etapa do consentimento; e (ii) ex-clientes, ou seja, aqueles que pretendem compartilhar seus dados que estão com instituições transmissoras com as quais já não possuem relacionamento, na qual destacam-se os percalços das etapas de autenticação e confirmação.

As instituições participantes buscaram suprir a dificuldade de novos clientes mediante adequação de seus portais na internet e aplicativos para dispositivos móveis, as quais, contudo, estão aquém de ofertar uma satisfatória experiência ao usuário.

Quanto aos ex-clientes, as dificuldades são ainda maiores e sem perspectivas de soluções eficientes a serem implementadas pelas instituições participantes.

As externalidades explicitadas, ainda que decorrentes do modelo regulatório adotado, denotam a possibilidade de superação mediante adequações de *design* nos portais e aplicativos das instituições participantes, com maior atenção à facilitação de acesso dos usuários enquadrados em tais situações.

Conquanto tais externalidades não demandem mudanças na estrutura regulatória, imperioso que o órgão regulador e os órgãos de governança do *open finance* exijam aprimoramento dos leiautes para a melhor experiência do usuário, tendo em vista a importância de incrementar a quantidade de adesões, fortalecendo o ecossistema e tornando-o cada vez mais atrativo.

Ademais, os pontos mais sensíveis referem-se a observância dos requisitos regulatórios a serem observados para a obtenção válida do consentimento.

Enquadram-se, nesse ponto, os aspectos objetivos quanto aos prazos do consentimento, identificação das instituições participantes, transmissora e receptora; identificação da finalidade do compartilhamento e dos dados ou serviços que serão compartilhados; identificação do cliente titular dos dados; além do óbice à obtenção do consentimento por meio de contrato de adesão, formulário previamente preenchido com a adesão ou sem a manifestação ativa do titular dos dados.

É um desafio para as instituições participantes evidenciarem sua aderência ao arcabouço jurídico e, sobretudo, validade do consentimento, em caso de sua contestação.

Nesse aspecto, ganha relevo a adoção de preceitos de *privacy by design* na construção dos portais do *open finance* pelas instituições participantes, com adoção de leiaute simplificado e linguagem clara e objetiva que facilite a compreensão do usuário, bem como restrita ao escopo de dados prevista na Resolução Conjunta nº 1/20.

Aliás, todas as informações indicadas como requisitos ao consentimento (prazo, finalidade, instituições participantes e dados) devem ser evidenciadas no *design*, com acesso obrigatório do usuário pelos campos respectivos para que conclua o seu consentimento.

Destaca-se, nessa senda, a importância de evidenciar a finalidade do compartilhamento dos dados e, mostra-se, de todo recomendável, o esclarecimento de que os dados, após internalizados na instituição receptora, poderão ser tratados sob a ótica de outras bases legais, a exemplo da proteção de crédito e legítimo interesse para o desenvolvimento de novos modelos de negócios e/ou ofertas direcionadas cliente. Nesse sentido, cita-se o aviso constante no portal do *open finance* do Banco Itaú:

Seus dados, sua privacidade

> Ao trazer suas informações, também poderemos usar os seus dados para outras finalidades ou com base em outras hipóteses legais, como para fins de cadastro; prevenção a fraudes; avaliações de risco, inclusive de crédito; proteção do crédito; fornecimento de serviços e produtos; cumprimento de obrigações legais e regulatórias, inclusive relacionadas ao Open Banking; além da criação e melhoria de serviços, processos e produtos das empresas e marcas do Itaú[184].

Ressalte-se a importância de que tanto a finalidade do compartilhamento de dados como avisos como o supratranscrito sejam disponibilizados de forma direta ao titular de dados. No caso citado, o acesso ao aviso dá-se somente mediante clique não obrigatório no campo "confira os detalhes da finalidade", o que fragiliza o consentimento sobre a ótica da ciência da finalidade ao usuário.

Outra sugestão cabível ao tema, é a obtenção do consentimento de forma granular, obtendo-se o consentimento para cada uma das finalidades pretendidas, inclusive aquelas a serem exercidas após a internalização dos dados, ainda que passíveis de amparo em outras bases legais de tratamento. Nesse ponto, pretende-se evitar a nulidade do consentimento na origem, o que pode implicar no enquadramento de tratamento indevido de quaisquer ações dele decorrentes.

Sob tal aspecto, recomenda-se fortemente que a regulação do *open finance* vá além do consentimento informado e contemple, expressamente, o consentimento granular, de forma a incorporar as melhores práticas atualmente defendidas sobre o consentimento, sem a necessidade de atrair para a regulação os debates sobre o alcance das qualificadoras atualmente adotadas.

A previsão expressa do consentimento granular, além de bem resguardar os direitos dos titulares dos dados pessoais, alinhando-se com a melhor doutrina sobre o tema, evita que instituições participantes adotem fluxos diferentes para a obtenção do consentimento, uma valendo-se do consentimento centrado na qualificadora "informado" e outro prestigiando a fragmentação do consentimento, mediante interpretação restritiva e outra extensiva dos termos qualificadores atualmente adotados na regulação, respectivamente.

Da mesma sorte, recomenda-se que todo tratamento a ser realizado com dados obtidos via compartilhamento no *open finance* observe a compatibilidade com o contexto no qual se deu a obtenção do consentimento, respeitada a legítima expectativa do titular dos dados.

Nesse espectro, o teste de proporcionalidade[185] desenvolvido por Bruno Bioni para fundamentar a base legal do legítimo interesse e com fulcro no artigo 10 da LGPD apresenta-

---

[184] https://www.itau.com.br/open-finance/consentimento. Acesso em 25 de janeiro de 2023.
[185] BIONI. Bruno Ricardo. op.cit. p. 252-253

se como uma salutar ferramenta passível de adoção pelo *open finance*, embora o cerne do ecossistema seja o consentimento.

O teste é composto por quatro etapas, nos seguintes moldes: a) verificação da legitimidade do interesse: situação concreta e finalidade legítima (art. 10, caput e I da LGPD); b) necessidade: minimização e outras bases legais (art. 10 §1º da LGPD); c) Balanceamento: impactos sobre o titular dos dados e legítimas expectativas (art. 10, II da LGPD); d) salvaguardas: transparência e minimização dos riscos ao titular do dado (art. 10 § 2º e 3º da LGPD)[186], cuja devida estruturação tem o condão de amparar a atuação das instituições participantes do *open finance*.

Embora não exista determinação normativa expressa, outro aspecto que merece ser objeto de recomendação é a arquitetura de escolha dos dados a serem compartilhados.

Assim, além da incontestável necessidade de que o escopo dos dados seja observado, ou seja, que os dados a serem compartilhados fiquem restritos àqueles definidos na regulação, bem como o prazo máximo do compartilhamento, sugere-se, valendo-se dos estudos sobre economia comportamental[187], que os dados a serem compartilhados e o respectivo prazo de compartilhamento não sejam objeto de opção-padrão, mas sim selecionados pelo próprio usuário, de modo a atrair a atenção do titular dos dados e induzi-lo a necessária reflexão. Nesse ponto, tomando como exemplo o mesmo portal acima citado, tem-se a prévia seleção de todos os dados[188].

Conquanto as boas práticas para a coleta da consentimento supra expostas possam ser voluntariamente adotadas pelas Instituições Participantes, não se olvida que os custos de transação impostos para a execução pertinente e o déficit informacional sobre o tema (que pode ensejar o não reconhecimento pela sociedade quanto aos boas práticas adotadas, mitigando eventuais benefícios de ganho de imagem), têm o condão de incentivar as Instituições Participantes a adotarem os requisitos mínimos regulatórios, nivelando o sistema para o cumprimento raso e superficial do consentimento.

---

[186] BIONI. Bruno Ricardo. op.cit. p. 252-253

[187] "Muitas pessoas aceitam a opção que exige o menor esforço – seja ela qual for – ou o caminho de menor resistência. Lembre-se do que foi dito sobre a inércia, o viés do status quo e a heurística do "ah, tanto faz". Todas essas forças nos levam a crer que, se há uma opção-padrão – uma opção que prevalecerá caso nenhuma outra seja escolhida -, podemos esperar um grande número de pessoas acabará por mantê-la, mesmo que não seja boa. E como também já enfatizamos, essas tendências à falta de ação são reforçadas quando, de forma implícita ou até explícita, se sugere que a opção-padrão representa a ação normal ou mesmo a ação recomendada. SUNSTEIN. Cass R; THALER. Richard H. Nudge: Como tomar melhores decisões sobre saúde, dinheiro e felicidade. Tradução Angelo Lessa. 1ª edição. Rio de Janeiro. Objetiva. 2019. p.101.

[188] https://www.itau.com.br/open-finance/consentimento. Acesso em 25 de janeiro de 2023.

Especificamente quanto ao consentimento granular, some-se que sua estruturação é, por vezes, criticada por agravar a experiência de fadiga do consentimento, de tal sorte que ante a ausência de norma cogente para a sua adoção, não se vislumbram incentivos aos participantes do *open finance* para estruturar o consentimento de forma fragmentada.

Nesse cenário, recomenda-se que as boas práticas para a outorga do consentimento sejam incorporadas à regulação, tanto para resguardar a efetiva observância aos preceitos de proteção de dados pessoais como para evitar vantagens competitivas indevidas por aqueles que estruturem o consentimento de forma restrita aos requisitos regulatórios, sem acrescer qualquer camada de proteção, a despeito da evolução doutrinária sobre o tema.

Forçoso, ainda, reconhecer que os pedidos de revogação do consentimento, garantidos tanto pela LGPD como pela regulação do *open finance*, não estão disponibilizados de forma explícita nos portal dos grandes bancos, ao reverso do que lecionam os preceitos do *privacy by design*, cenário que demanda a atuação do órgão regulador e dos órgãos de governança do *open finance* em busca do devido alinhamento.

Ainda sobre os dados a serem compartilhados, recomenda-se fortemente apenas o compartilhamento de dados brutos, ou seja, não abarquem aspectos de *profiling*, inclusive pontuação de *credit scoring*, e tampouco quaisquer dados sintéticos decorrentes de tratamentos e inferências realizados pela própria Instituição, considerando todas as celeumas que envolvem a matéria e seus potenciais impactos na autodeterminação informativa do titular dos dados, em sua atual concepção, sugerindo-se, assim, uma interpretação extensiva ao artigo 5º, §4º, I, "b" da Resolução Conjunta nº 1º.[189]

Estima-se que tal recomendação não encontre óbice junto às Instituições Financeiras quando da solicitação formulada pelo titular dos dados para compartilhamento com instituições receptoras não integrantes do mesmo conglomerado ou não parceiras, na medida em que tal posicionamento converge com a proteção do segredo empresarial.

Outrossim, nos contratos de parceria envolvendo o *open finance*, notadamente com escopo de desenvolvimento de novos modelos de negócios e aprimoramento da experiência do usuário, a recomendação pelo não compartilhamento de dados de perfilamento tem o potencial de impactar negativamente os objetivos pretendidos na parceira, ante a menor assertividade dos dados para a modelagem em desenvolvimento.

[189] Artigo 5º § 4º. O compartilhamento de dados de cadastro de que trata o inciso I, alínea "c", do caput, deve abranger: I - os dados fornecidos diretamente pelo cliente ou obtidos por meio de consulta a bancos de dados de caráter público ou privado, exceto: b) as notas ou pontuações de crédito.

Ciente das eventuais repercussões prejudiciais ao desenvolvimento de novos modelos de negócios, propõe-se, subsidiariamente, a preferência por adoção de dados anonimizados e elaboração, com especial atenção, de Relatório de Impacto à Proteção de Dados Pessoais específico aos contratos de parceria (com as devidas cautelas quanto ao segredo empresarial).

Como forma de estruturar as propostas supra, recomenda-se a adoção de ferramentas pautadas em *Privacy Enhancing Technologies,* que se destinam ao desenvolvimento de ferramentas com enfoque prioritário na proteção da privacidade, como parte instrumental da metodologia do *privacy by design.*

Caracterizam-se pela preocupação com a proteção de dados pessoais, sobretudo, pela busca por utilizar, o mínimo possível, o tratamento de dados pessoais identificados ou identificáveis e priorizar a anonimização, sem comprometer a funcionalidade dos serviços.[190]

Há um conjunto de estratégias e atribuições das PETs destinadas a preservar a privacidade do usuário, cujos aspectos pormenorizados e desafios ensejam intensos debates que escapam ao cerne do presente trabalho. Desse modo, apresenta-se, a seguir, uma compilação daqueles de maior destaque, sob a denominação de mecanismos:

Tabela 4 – Mecanismos de preservação da privacidade do usuário

MECANISMO	DESCRIÇÃO
Limitação da coleta de dados	Os dados coletados devem estar adstritos àqueles necessários ao sistema ou atividade a ser desenvolvida.
Propósito específico	O uso dos dados coletados tem que ser específico, informado de forma clara e sua finalidade não pode ser alterada ou aplicada de modo diverso àquela apresentada na autorização concedida pelo titular dos dados.
Autenticação e Autorização	Nem todos os dados disponibilizados pelo titular podem ser livremente acessados por todos os intervenientes, mas apenas aqueles necessários ao processamento a ser realizado. A contratação de um seguro, por exemplo,

[190] https://www.insper.edu.br/noticias/tecnologias-de-aprimoramento-da-privacidade-ganham-relevancia/. Acesso em 13 de agosto de 2023.

	prescinde do acesso aos dados afetos à investimentos.
Anonimização	Adoção de técnicas para inviabilizar a identificação do titular dos dados. Há uma modalidade menos efetiva que é a desidentificação, pela qual se exclui os dados que permitem a identificação, como nome e documentos pessoais. Pauta-se em dois princípios: *data masking*, que cria uma versão diferente do dado original, mediante versão alterada ou resumida, com a exclusão de determinados dados; ou *data synthesis*, que produz uma síntese dos dados originais, mantendo os seus atributos. Outra estratégia é criar óbices para que os dados isolados possam, de forma combinada, permitir a identificação do titular.
Pseudo-identidade	Criação de referências que substituam os dados hábeis a identificar o usuário.
Criptografia	Codificar os dados por meio de uma chave, de modo que apenas o receptor, portador da chave, possa recompor o conteúdo original. A criptografia é uma técnica relevante, sobretudo, para as etapas de armazenamento, transferência e acesso.
Biometria	Adoção da biometria para acesso a senhas e demais informações que se pretenda proteger. Para fins de controle de acesso, trata-se de técnica segura e eficiente. Contudo, apresenta riscos quanto ao controle dos dados biométricos em si.

Possibilidade de auditagem	Auditagem dos dados por um terceiro, seja uma autoridade regulatória ou um ente privado a quem se autorize tal atribuição.
Desagregação	As atividades de coleta e processamento de dados devem ser exercidas de forma descentralizada, competindo a entes diferentes ou, se os mesmos, em sistemas distintos.
Controle pelo usuário	O usuário deve ter o controle de seus dados em todas as etapas, tanto quanto à sua disponibilização como ao seu processamento, inclusive para desautorizar o acesso à algum dado, seu uso específico ou até o seu apagamento. Tal controle deve ocorrer de forma fácil, com interfaces amigáveis e com informações claras.

Fonte: Elaboração própria[191]

Sob a ótica do *profiling*, os diversos mecanismos destinados a resguardar a identificação do titular permitem preservar a esfera de privacidade do usuário e, por outro lado, garantem interfaces amigáveis para a compreensão de eventuais inferências equivocadas que resultem em perfilamento inadequado e, diante de tais situações, viabilizam as ferramentas hábeis e de fácil acesso para as devidas correções.

À guisa de exemplos de outros meios de empregabilidade da *Privacy Enhancing Technologies (PETs) têm-se o "Do not Track – DNT"*[192] – Não me rastreie e a *"Platform for Privacy Preferences – P3P"*[193] – massificação das preferências de privacidade, ambas ferramentas construídas para simplificar o consentimento, sem comprometer o nível informacional.

A principal dificuldade enfrentada para a execução das duas ferramentas foi a necessidade de padronização dos sistemas dos diversos intervenientes, dos quais uma parcela

[191] Elaborado com base no estudo do Instituto de Tecnologia e Sociedade (ITS). Disponível em: https://itsrio.org/wp-content/uploads/2018/06/Privacidade-em-perspectivas_DTP.pdf. Acesso em 13 de agosto de 2023.

[192] Mecanismo pelo qual o usuário vale-se de um com

ando para escolher entre permitir ou bloquear a coleta de dados pessoais, replicada pelo navegador em todos os acessos seguintes.

[193] Mecanismo pelo qual o usuário pode configurar suas preferências de privacidade e o próprio browser realiza uma análise automatizada de compatibilidade com as políticas de privacidade doravante acessadas.

considerável apresentou resistência, inexistindo norma cogente que lhes impusesse a necessária uniformização.

Note-se que no caso do *open finance*, a principal dificuldade estaria, de pronto, afastada, uma vez que a padronização via plataforma única é a base do ecossistema, competindo ao regulador os devidos ajustes para inclusão dos aspectos tecnológicos que se fizerem necessários.

No que concerne a identificação das instituições participantes, seja receptora ou transmissora, mostra-se salutar esclarecer ao usuário os aspectos que envolvem os conglomerados das instituições participantes e a necessidade de consentimento ou autenticação/confirmação individualizada.

Isto porque, dados do Bradesco Financiamento, por exemplo, serão compartilhados por referida instituição e não pelo Banco Bradesco[194], o que não é facilmente depreendido pelo homem médio, além dos riscos de responsabilização, em sede judicial, das instituições participantes pelo não cumprimento das obrigações do *open finance* perante o titular dos dados, sob o fundamento da teoria da aparência.

Transpondo a temática para a seara judicial, os riscos mostram-se potencialmente agravados ante os elevados índices nacionais de judicialização, a tradição histórica e o aparato jurídico que viabiliza o ajuizamento de ações coletivas que versem sobre o tratamento de dados pessoais e a convergência entre os dispositivos da LGPD e do CDC, conforme síntese abaixo:

> Não é demais lembrar que a LGPD e o Código de Defesa do Consumidor (CDC) mesclam-se em química volátil e explosiva. Isso porque, entre os diplomas, há vários dispositivos em comum, alguns, inclusive, transcritos *ipsis litteris* de uma legislação para a outra (LGPD, art. 22 e 42), repetindo contingências velhas e revelhas, como inversão do ônus da prova, solidariedade, responsabilidade objetiva e uma generosa possibilidade de desconsideração da personalidade jurídica[195].

O cenário exige que as instituições participantes estejam cientes de sua obrigação de *accountability* quanto ao tratamento de dados pessoais. E, sob tal premissa, devem balizar suas respostas às potenciais demandas judiciais, demonstrando, na fase de instrução, quando o caso, todo o racional que subsidia as ações adotadas, comprovando-as mediante documentações cabíveis, a exemplo do testes de proporcionalidade e Relatórios de Impacto à Proteção de Dados

---

[194] https://openfinancebrasil.org.br/quem-participa/?. Acesso em 25 de janeiro de 2023.

[195] BECKER, Daniel; WOLKART, Erik Navarro; BRUZZI. Eduardo. Estamos trancados num paiol de pólvora: LGDP, ANPD e demandismo. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/regulacao-e-novas-tecnologias/estamos-trancados-num-paiol-de-polvora-lgpd-anpd-e-demandismo-20072019. Acesso em 25 de janeiro de 2023

Pessoais (RIPDP), resguardado o segredo empresarial, proteção expressamente conferida pela LGPD.

Quanto ao Relatório de Impacto à Proteção de Dados Pessoais, passível de solicitação apenas pela ANPD, nos termos da lei, a doutrina jurídica elenca ações passíveis de conferir maior credibilidade ao balanceamento de interesses consubstanciado no relatório, a saber, revisão por um agente externo, publicização do relatório e chamamento coletivo para que diferentes atores sociais participem da elaboração do relatório, o que envolve a fase da definição da metodologia[196].

Cabe aqui uma ressalva, a obrigação de *accountability* sobre o tratamento de dados pessoais preconizada no presente trabalho não significa o total escrutínio da tomada de decisão e riscos do tratamento de dados, mediante imersão no código fonte, modelo estatístico ou linha de programação, dentre outros.

Isto porque, indubitável a complexidade técnica de todo o processo, notadamente quando envolve uso de algoritmos e inteligência artificial no tratamento de dados pessoais, aspectos cuja necessidade de imersão publicizada resultariam num elevado custo de transação. Registre-se, nesse contexto, que desde a concepção da LGPD até o presente momento, padece-se de uma análise oficial de seu impacto regulatório.

Da mesma sorte, não se defende a elaboração de normas do *open finance* capazes de impor um custo regulatório desnecessário ou desproporcional. A intervenção regulatória deve pautar-se pela proporcionalidade entre os fundamentos e interesses que ensejaram a atuação do regulador[197], sendo certo que no *open finance* eventual desequilíbrio dessa espécie coloca em xeque os próprios objetivos do ecossistema.

> "Qualquer entendimento extensivo agravará as externalidades da lei, produzindo resultados temerários para a economia, sobretudo para os setores que utilizam, em suas atividades, decisões automatizadas como é o caso dos setores bancários e financeiros."[198]

A prestação de contas proposta deve zelar pela informação de quais dados foram objeto de tratamento e a finalidade do tratamento, demonstrando a necessária adequação ao contexto no qual o consentimento foi obtido, resguardando-se o direito à sua revogação e a possibilidade de revisão das decisões automatizadas.

---

[196] BIONI. Bruno Ricardo. Regulação e Proteção de Dados Pessoais: o princípio da accountability. 1ª ed. Rio de Janeiro. Foresen. 2022. P.104-109.

[197] MORENO, Natália de Almeida. Análise de impacto regulatório. Revista dos Tribunais, vol. 951/2015.

[198] BECKER. Daniel; CAVALHEIRO. Gabriela; ROMMEL. Roberto. All Data is credit data: apontamento sobre a regulação do credit score. In: Banking 4.0: Desafios jurídicos e regulatórios do novo paradigma bancário e de pagamentos. Coord. Bruzzi, Eduardo; Feigelson. Bruno. 1ª ed. Thomson Reuters. São Paulo. 2020. p.58.

Portanto, as recomendações pautam-se em diretrizes que têm por cerne a demonstração do acautelamento das instituições participantes quanto ao tratamento dos dados pessoais, com vistas e evidenciar o cumprimento do arcabouço jurídico, a estrita observância à boa-fé, dever de transparência e informação, bem como a finalidade do tratamento em prol de melhorias na experiência do usuário e não adstritos aos interesses das instituições participantes.

5 CONCLUSÃO

O *open finance*, também denominado de sistema financeiro aberto, é um ecossistema que permite o compartilhamento de dados entre as instituições participantes, mediante prévio consentimento de seus titulares, e de forma padronizada, sistematizada e segura, via APIs, que são interfaces que permitem a comunicação e a integração dos diferentes sistemas.

A possibilidade de compartilhamento dos dados por decisão do seu titular configura uma substancial alteração em um segmento tão arraigado à concepção do sigilo bancário e suas inerentes preocupações e ações para preservá-lo, esvaziando a supremacia das instituições no controle dos dados submetidos à sua guarda.

Em paralelo, o incremento no fluxo de informações e o crescente agregamento de valor nas mais diferentes atividades econômicas, culminando no quadro de sua mercantilização, alçou os dados pessoais a condição de ativo econômico, com elevada carga de monetização.

Esse contexto exigiu, tanto sob a ótica do direito como da economia, a construção de uma perspectiva jurídico-regulatória para este novo e tão relevante bem jurídico, o dado pessoal.

Destacam-se, no espectro internacional, o Regulamento Geral de Proteção de Dados da União Europeia (GDPR*)*, e a Lei nº 13.709/18 – Lei Geral de Proteção de Dados Pessoais (LGPD), em âmbito nacional, bem como a positivação do direito à proteção de dados pessoais como direito fundamental, arcabouço jurídico cuja interpretação ainda pende de maior sedimentação doutrinária e posições jurisprudenciais são escassas.

A construção da intelecção da proteção de dados pessoais e do seu liame com a regulação do *open finance* (que versa sobre o tratamento de dados no segmento financeiro) exige a conciliação de critérios interpretativos adaptáveis ao desenvolvimento tecnológico, e, concomitantemente, claros e rígidos no sentido de resguardar e conferir segurança jurídica aos titulares dos dados.

Assim, a superação da aparente dicotomia entre o movimento protetivo dos dados pessoais e a festejada construção de um ecossistema que fomenta o compartilhamento dos dados é o cerne do presente trabalho.

De pronto, cabe esclarecer que, apesar de pontos temáticos convergentes, a regulação do *open finance* não se destina a regulamentar a LGPD no segmento financeiro. Seu escopo é destinado ao sistema financeiro aberto e, por respeito à hierarquia das normas, observa (ou deveria observar) todo o arcabouço jurídico de proteção aos dados pessoais, assim como às regras de sigilo bancário.

O estudo do texto regulatório do *open finance* evidencia a especial atenção e o seu alinhamento principiológico à LGPD, com destaque aos princípios da transparência, segurança e privacidade de dados, qualidade e tratamento não discriminatório, e, sobretudo, aos preceitos da autodeterminação informativa, consubstanciado, em especial, na estruturação do consentimento a ser outorgado pelo titular e passível de revogação a qualquer momento, observando-se, ainda, os requisitos da LGPD necessários à validade de tal consentimento.

Contudo, as potenciais afrontas à proteção de dados pessoais transcendem ao texto e exigem uma imersão no contexto fático, notadamente na sistematização e operacionalização do *open finance*.

Para tanto e com vistas a facilitar a compreensão, o presente trabalho classificou os riscos em exógenos, aqueles decorrentes da atuação de terceiros não participantes, direta ou indiretamente, do *open finance*, ainda que se valham de eventual fragilidade operacional do sistema, e envolvem, sobretudo, aspectos de segurança da informação; e riscos endógenos, aqueles riscos internos, advindos da própria atuação dos participantes do *open finance* em face dos titulares dos dados.

As precauções afetas à segurança da informação estão longe de serem uma novidade para o sistema financeiro, cuja expertise e pioneirismo tecnológico são reconhecidos pela sociedade e foram devidamente incorporados ao *open finance*. Não por outra razão, os aspectos de padrões e critérios técnicos foram, acertadamente, delegados à autorregulação, sob supervisão do Banco Central.

Da mesma sorte, a escolha regulatória pelas APIs como ferramentas de interface de comunicação e integração do sistema está coadunada com o atual estado da técnica, adotada por diferentes projetos de *open banking* ao redor do mundo.

O cenário, porém, não esgota os riscos incidentes e tampouco as medidas de enfretamento a serem adotadas, com especial destaque para as ameaças lastreadas em engenharia social, principal vetor de ataques cibernéticos e fraudes impetradas em face do setor financeiro.

Assim, além das medidas técnicas de segurança informacional e cibernética, as quais, numa perspectiva empírica, concentram os esforçam dos órgãos de governança do *open finance* e de todas as instituições participantes, mister atrelar ações educativas junto a sociedade para coibir a ocorrência de fraudes perpetradas mediante engenharia social.

No contexto dos riscos endógenos, as novas interpretações e ressalvas quanto ao uso do consentimento na seara da proteção de dados pessoais colocam em xeque a visão de que o

compartilhamento de dados escorado, única e exclusivamente, em tal base legal resguarda os ditames da LGPD, garantindo, assim, a aderência da regulação do *open finance*.

Rememore-se que o crescente fluxo de dados e os cruzamentos em escala exponencial pelo *Big Data* e ferramentas de *analytics* dificultam e, por vezes, tangenciam a inviabilidade do exercício do controle individual pelo titular dos dados, agravados pela assimetria técnico-informacional, desejo de conformação social ou acesso à benefícios (a exemplo de melhores condições de crédito no *open finance*), além de vieses e heurísticas na tomada de decisão, conjunto que infirma a gênese do princípio da autodeterminação informativa.

Nesse cenário, emerge a principal proposta de boas práticas a serem adotadas pelas instituições participantes, centrada na cautela na adoção indiscriminada do consentimento, recomendando-se o agregamento dos ditames da teoria da integridade contextual, a qual preconiza a aferição da adequada relação do tratamento dos dados ao contexto no qual o consentimento foi outorgado e as legítimas expectativas depreendidas desse contexto.

Para amparar tal interpretação, sugere-se, ainda, maior apego à clareza das informações a serem prestadas nos portais e plataformas de adesão ao *open finance*, com desenvolvimento lastreado em *privacy by design* e, sua parte instrumental, com ferramentas pautadas em *Privacy Enhancing Technologies*, os quais devem zelar para que as informações indicadas como requisitos ao consentimento (prazo, finalidade, instituições participantes e dados) sejam estruturadas com acesso obrigatório do usuário pelos campos respectivos antes da conclusão do consentimento, destaque à finalidade do tratamento dos dados, inclusive eventuais tratamentos a serem realizados após a internalização dos dados na instituição receptora, sem prejuízo das cautelas quanto as jornadas de consentimento exaustivas (fadiga do consentimento).

No mesmo sentido, a despeito da ausência de previsão normativa a respeito, mostra-se salutar que sejam agregados preceitos da economia comportamental no desenvolvimento da arquitetura da escolha, com o escopo de propiciar a máxima reflexão do titular dos dados no momento da outorga do consentimento, evitando-se o emprego de opções-padrão que atendam, eminentemente, os interesses das instituições participantes.

O atual direcionamento da proteção de dados pessoais sobre as atividades de perfilamento e decisões automatizadas, entendidos como potenciais violadores do livre desenvolvimento da personalidade, também tem o condão de impactar a intelecção das normas do *open finance*, restringido o compartilhamento de dados de tais espécies, além de implicar no debate sobre os limites do segredo empresarial, devidamente protegido pela LGPD.

Por tais razões, recomenda-se maior incentivo regulatório ao uso de dados anonimizados, valendo-se dos parâmetros de reversibilidade definidos pela LGPD.

Entende-se, ainda, pela interpretação extensiva do artigo 5º §4º, I, "b", de modo que a restrição ao compartilhamento não fique adstrita às notas e pontuações de crédito, mas alcance quaisquer espécies de perfilamento.

Por derradeiro, merece destaque o elevado patamar de judicialização das demandas bancárias, bem como a viabilidade jurídica de busca por provimento jurisdicional referente aos dados pessoais pelas vias da tutela coletiva, o que torna recomendável a apresentação de documentos hábeis à demonstrar a aderência legal e regulatória, a exemplo do teste de proporcionalidade e relatórios de impacto à proteção de dados e, preferencialmente, elaborados sob a ótica da obrigação de *accountability*.

Imperioso consignar que, a despeito da convergência principiológica entre a LGPD e a regulação do *open finance*, bem como da autorregulação supervisionada do ecossistema, além da adoção das melhores práticas pelas instituições participantes, a exemplo das expostas no presente trabalho, não se descarta a ocorrência de conflitos regulatórios advindos de violações porventura identificadas pela Autoridade Nacional de Proteção de Dados (ANPD), o que exigirá a harmonização entre os posicionamentos e orientações das autarquias envolvidas, para a construção de um contexto jurídico pautado na segurança jurídica.

Nesse contexto, salutar a abertura de um diálogo interinstitucional, com vistas a construção da exegese sobre proteção de dados pessoais no setor financeiro, sobretudo no *open finance*, à exemplo dos Termos de Cooperação já firmados pela ANPD junto ao Cade e a Senacom.

Há um longo caminho para o *open finance* a ser pavimentado, cujas primeiras iniciativas foram adotadas pelo órgão regulador e merecem o reconhecimento de toda a sociedade pela iniciativa e protagonismo.

A busca pelo ótimo de pareto entre a proteção dos dados pessoais e o incentivo à inovação, com todas as vantagens dela advindas é um desafio da sociedade da informação, amplificado no setor financeiro, tão arraigado à ideia de sigilo dos dados e, no contexto nacional, com elevados índices de monopólio informacional.

Almeja-se que o presente trabalho possa contribuir para os próximos passos a serem dados nesse longo caminho, norteados por diretrizes que evidenciem o acautelamento das instituições participantes quanto ao tratamento dos dados pessoais, em estrita observância à boa-fé, dever de transparência e informação, e, sobretudo, tratamento de dados cujo escopo seja o desenvolvimento de novos modelos de negócios que propiciem melhoria na experiência do usuário, promovendo inclusão bancária e competitividade no setor, com todas as benesses sociais advindas do atingimento de tais objetivos.

REFERÊNCIAS

ANAQUIM. Ludmilla. LIMA. Marcello.Open Banking e portabilidade de dados – uma análise supranacional. In: Banking 4.0: Desafios jurídicos e regulatórios do novo paradigma bancário e de pagamentos. Coord. Bruzzi, Eduardo; Feigelson. Bruno. 1ª ed. Thomson Reuters. São Paulo. 2020. p.195-211.

ARNER. Douglas. BARBERIS. Janos Nathan. BUCKELY. Ross. Fintech, Regtech, and the Reconceptualization of Financial Regulation. Northwestern Journal of International Law & Business. v.37. n. 3. 2017.

AUTORIDADE Nacional de Proteção de Dados. Planejamento Estratégico 2021-2023. Brasília. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/planejamento-estrategico/planejamento-estrategico-2021-2023.pdf. Acesso em 27 de janeiro de 2023.

BAGNOLI, Vicente; RIBEIRO, Alexandre Ogêda Ribeiro. Open Banking: Impactos e desafios no mercado financeiro. In: Constituição, Economia e Desenvolvimento: Revista da Academia Brasileira de Direito Constitucional. Curitiba. 2020. Vol. 13. Disponível em: https://abdconst.com.br/revista24/Artigo%208%20-%20Alexandre%20Ogeda%20Ribeiro%20e%20Vicente%20Bagnoli.pdf. Acesso em 17 de setembro de 2022.

BANCO Itaú. Open Finance – Consentimento. Disponível em: https://www.itau.com.br/open-finance/consentimento. Acesso em 25 de janeiro de 2023.

BARRETO, Wanderlei de Paula. In: ALVIM, Arruda e ALVIM, Thereza. Comentários ao código civil brasileiro. Rio de Janeiro: Forense, 2005, v. 1.

BECKER, Daniel; WOLKART, Erik Navarro; BRUZZI. Eduardo. Estamos trancados num paiol de pólvora: LGDP, ANPD e demandismo. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/regulacao-e-novas-tecnologias/estamos-trancados-num-paiol-de-polvora-lgpd-anpd-e-demandismo-20072019. Acesso em 25 de janeiro de 2023.

BECKER. Daniel; CAVALHEIRO. Gabriela; ROMMEL. Roberto. *All Data is credit data*: apontamento sobre a regulação do credit score. In: Banking 4.0: Desafios jurídicos e regulatórios do novo paradigma bancário e de pagamentos. Coord. Bruzzi, Eduardo; Feigelson. Bruno. 1ª ed. Thomson Reuters. São Paulo. 2020.

BIONI. Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2ª ed. Rio de Janeiro. Forense. 2019.

BIONI. Bruno Ricardo. Regulação e proteção de dados pessoais: o princípio da accountability. 1ª ed. Rio de Janeiro. Forense. 2022.

BIONI. Bruno Ricardo. Xeque-Mate: O tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasi. GpoPai/USP – Grupo de Pesquisa em Políticas Públicas

para acesso à informação. São Paulo. 02.07.2015. Disponível em: http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf. Acesso em 17 de dezembro de 2022.

BISELLI. Esther Collet Janny Teixeira. Inovação e abertura no setor bancário: desafios concorrenciais. In: Revista do Instituto Brasileiro de Estudos Concorrenciais, Consumo e Comércio Internacional. Volume 24. 2018. Disponível em: https://ibrac.org.br/UPLOADS/PDF/RevistadoIBRAC/Revista_do_IBRAC_24_N._2-2018.pdf. Acesso em 26 de janeiro de 2022.

BNDES. Transparência, Open Finance. Disponível em: https://www.bndes.gov.br/wps/portal/site/home/transparencia/open-finance/open-finance-perguntas-frequentes#:~:text=Por%20meio%20de%20quais%20canais,financeiras%20ou%20de%20pagamentos%20participantes. Acesso em 25 de janeiro de 2023.

BONSERE. Silvana Fátima Mezaroba; GIBRAN. Sandro Mansur; VEIGA. Fábio da Silva. Open Banking: Expectativas e desafios para o mercado financeiro no Brasil. Disponível em: http://revista.unicuritiba.edu.br/index.php/admrevista/article/view/4087. Acesso em 17 de setembro de 2022.

BOSCO. Franscesca et al. Proling Technologies in Pratice: Applications and Impacto on Fundamental Rights and Values. 2017.

BOUVIER. Pascal. EZRACHI. Ariel. MORTON. Fiona Scott; et al. Committee for the study of digital platforms: Market structure and antitruste subcommittee report. Chicago. Stigler Center for the study of the Economy and the State. University of Chicago Booth School of Business. 2019.

CARLETTI. Elena. SMOLENSKA. Agnieska. 10 years on from the financial crisis: co-operaion between competition agencies and regulators in the financial sector. OECD, 2017. Disponível em: https://one.oecd.org/document/DAF/COMP/WP2(2017)8/en.pdf. Acesso em 07 de janeiro de 2024.

CARVALHO. Laura Brodsky Liz. Data sharing and open baking. 05 de setembro de 2017. Disponível em: https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking. Acesso em 26 de janeiro de 2022.

CHOI, Hanbyul; PARK, Jonghwa; JUNG, Yoonhyuk. The role of privacy fatigue in online privacy behavior. **Computers in Human Behavior**, v. 81, 2018.

CITRON, Danielle Keats e PASQUALE, Frank A., The Scored Society: Due Process for Automated Predictions (2014). Washington Law Review, Vol. 89, 2014, p. 1-, U of Maryland Legal Studies Research Paper No. 2014-8. Disponível em SSRN: https://ssrn.com/abstract=2376209. Acesso em 07 de janeiro de 2023.

COLAÇO. Hian Silva; SAMPAIO. Carolina Vasques. Direito à autodeterminação informativa no mercado de créditos: análise econômica do cadastro positivo de dados no Resp. 1419697/RS. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/1493-3489-1-sm.pdf. Acesso em 26 de junho de 2022.

COMISSÃO EUROPEIA. Proteção de dados. Disponível em: https://ec.europa.eu/newsroom/article29/items/612053/en. Acesso em 27 de dezembro de 2022.

COMISSÃO EUROPEIA. Proteção de dados. Fintech Action Plan: For a more competitive and innvotive European financial sector. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0109. Acesso em 25 de janeiro de 2023.

COMITÊ Europeu para Proteção de Dados. Diretrizes 06/2020 sobre a interação entre a Segunda Diretiva Serviços de Pagamento e o RGPD. 2020. Disponível em: https://edpb.europa.eu/system/files/2021-06/edpb_guidelines_202006_psd2_afterpublicconsultation_pt.pdf. Acesso em 18 de dezembro de 2022.

COMITÊ Europeu para Proteção de Dados. Guidelines on data protection in EU financial services regulation. 2014. Disponível em: https://edps.europa.eu/sites/edp/files/publication/14-11-25_financial_guidelines_en.pdf. Acesso em 18 de dezembro de 2022.

CONSULTOR JURÍDICO. Com dois anos de atraso, governo cria estrutura da agência de proteção de dados. Conjur. 27 de agosto de 2020. Disponível em: https://www.conjur.com.br/2020-ago-27/dois-anos-atraso-governo-cria-estrutura-anpd. Acesso em em 19 de junho de 2022.

CRESPO. Marcelo Xavier de Freitas. SANTOS. Coriolano Aurélio de Almeida Camargo. Como será o futuro dos negócios com a vigência do Regulamento Geral de Proteção de Dados Europeu? In Direito Digital Aplicado 3.0. Coordenadora Patrícia Peck Pinheiro. 1ª ed. São Paulo. Thomson Reuters Brasil. 2018.

CUPIS. Adriano de. Os direitos da personalidade. Tradutor Afonso Celso Furtado de Rezende. São Paulo. Quorum. 2ª edição. 2008.

DELLOITE. Pesquisa Febraban de Tecnologia Bancária 2022. Disponível em: https://www2.deloitte.com/br/pt/pages/financial-services/articles/pesquisa-febraban-tecnologia-bancaria.html. Acesso em 25 de janeiro de 2023.

DOLABELLA. Gabriel. RAGAZZO. Carlos. Open Banking ao redor do mundo: EUA, UE e Austrália – Panorama Econômico #18. Realização Instituto Propague. 2020. Disponível em: https://www.youtube.com/watch?v=NeWNkamyXL8. Acesso em 20 de abril de 2023.

DONEDA. Danilo. A proteção dos dados pessoais como um direito fundamental in Espaço Jurídico. V.12. nº 2. Julho/Dezembro 2011.

DONEDA, Danilo. Da Privacidade à Proteção de dados pessoais: Fundamentos da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters, 2020.

DONEDA. Danilo. Privacidade e transparência no acesso à informação pública. Zaragoza. Prensas Universitárias de Zaragoza. 2010. Disponível em:

http://www.egov.ufsc.br/portal/sites/default/files/lefis11-09.pdf. Acesso em: 16 de novembro de 2022.

DONEDA. Danilo. Privacidade, vida privada e intimidade no ordenamento jurídico brasileiro. Da emergência de uma revisão conceitual e da tutela de dados pessoais. Disponível em http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=2460. Acesso em 05 de janeiro de 2023.

DONEDA. Danilo. ZANATTA. Rafael. O que há de novo no debate "credit score" no Brasil? Direitos são conhecidos e efetivamente exercidos pelos consumidores? Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/o-que-ha-de-novo-no-debate-credit-score-no-brasil-09022017. Acesso em 20 de agosto de 2022.

EROLES. Pedro. Breves comentários sobre os desafios para a governança da autorregulação do Open Banking no Brasil. In: Fintechs, Bancos Digitais e Meios de Pagamento: Aspectos Regulatórios das novas tecnologias financeiras. Eroles. Pedro coordenador. São Paulo. Quartier Latin. 2019.

ESTRELA. Márcio Antonio. Moeda, Sistema Financeiro e Banco Central – Uma abordagem teórica e prática sobre o funcionamento de uma autoridade monetária no mundo e no Brasil. Rio de Janeiro: Fundação Cesgranrio, 2011.

EURO BANKING ASSOCIATION. Understanding the business relavance of Open APIs and Open Banking for Banks. Euro Banking Association. v.1.0. 2016.

FARHAT. Raymond. Le Secret Bancaire: étude de droit comparé. France. Suisse, Liban. Paris. Librairie Genérale de Droit et de Jurisprudence.1980.

FARO. Priscila Pinheiro Ribeiro. Open Banking no Brasil como iniciativa de modernização do sistema financeiro e mecanismo de incentivo à concorrência. In: Banking 4.0: Desafios jurídicos e regulatórios do novo paradigma bancário e de pagamentos. Coord. Bruzzi, Eduardo; Feigelson. Bruno. 1ª ed. Thomson Reuters. São Paulo. 2020.

FEDERAÇÃO BRASILEIRA DE BANCOS. Prevenção à Fraudes Febraban. Disponível em: https://antifraudes.febraban.org.br/. Acesso em 02 de janeiro de 2023.

FEDERAÇÃO BRASILEIRA DE BANCOS. Prevenção à Fraudes Febraban. Disponível em: https://cmsarquivos.febraban.org.br/Arquivos/documentos/PDF/cartilha_eng_social_atualizada_20.pdf. Acesso em 02 de janeiro de 2023.

FEDERAÇÃO BRASILEIRA DE BANCOS. Prevenção à Fraudes Febraban. Disponível em: https://cmsarquivos.febraban.org.br/Arquivos/documentos/PDF/pesquisa-febraban-2022-vol-2.pdf. Acesso em 02 de janeiro de 2023.

FEDERAÇÃO BRASILEIRA DE BANCOS. Febrabantech. Disponível em: https://febrabantech.febraban.org.br/temas/seguranca/febraban-e-26-bancos-promovem-semana-da-seguranca-digital-e-orientam-populacao-sobre-golpes. Acesso em 02 de janeiro de 2023.

FERREIRA. Rafael Freire. Desafios em sede de tutela da Personalidade: a autodeterminação informativa e a privacidade na sociedade da informação. Dissertação (Mestrado em Ciências Jurídicas) – Universidade Autónoma de Lisboa Luís de Camões, Lisboa.2016.

FIUZA, Cesar. Por uma redefinição da contratualidade. Março/2017. Âmbito Jurídico. Disponível em: https://ambitojuridico.com.br/cadernos/direitocivil/por-uma-redefinicao-da-contratualidade/. Acesso em 27 de novembro de 2022.

FIUZA. Cesar. Direito Civil – curso completo. 11 ed. Belo Horizonte. Del Rey. 2008.

FIUZA. Cesar. Direitos da personalidade. Disponível em: http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=7340&revista_caderno=7. Acesso em 20 de dezembro de 2022.

FONSECA. Gabriel C. Soares da. MENDES. Laura Schertel. Proteção de Dados para além do consentimento: tendências contemporâneas de materialização. In: Revista Estudos Institucionais. V. 6. nº 2, p. 515/516. Disponível em: https://www.estudosinstitucionais.com/REI/article/view/521/510. Acesso em 07 de janeiro de 2023.

FRAZÃO. Ana. A nova Lei Geral de Proteção de Dados. Repercussões para a atividade empresarial: o alcance da LGPD. Parte II. Disponível em: http://anafrazao.com.br/files/publicacoes/2018-09-05-A_nova_Lei_Geral_de_Protecao_de_Dados_Repercussoes_para_a_atividade_empresarial_o_alcance_da_LGPD_Parte_II.pdf. Acesso em 25 de novembro de 2022.

FRAZÃO. ANA. Nova LGPD: A importância do consentimento para o tratamento de dados pessoais. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-a-importancia-do-consentimento-para-o-tratamento-dos-dados-pessoais-12092018. Acesso em 26 de junho de 2022.

FRAZÃO. Ana. Nova LGPD: o tratamento dos dados pessoais sensíveis. A quinta parte de uma série sobre as repercussões para a atividade empresarial. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018. Acesso em 25 de novembro de 2022.

GARCIA. Larissa. Quatro bancos concentraram 59% do mercado de crédito em 2022, com operações pressionadas pela Selic. Valor Investe. 06 de junho de 2023. Disponível em: https://valorinveste.globo.com/produtos/credito/noticia/2023/06/06/quatro-bancos-concetraram-59percent-do-mercado-de-credito-em-2022-com-operacoes-pressionadas-pela-selic.ghtml. Acesso em 07 de janeiro de 2024.

GOETTENAUER. Carlos. Algoritmos de credit score, dados pessoais: um mapa regulatório para o compliance na análise de crédito. In Compliance e políticas de proteçao de dados. Ana Frazão e Ricardo Villas Boas Cueva – coordenação. São Paulo. Thomson Reuters Brasil. 2021.

GOETTENAUER. Carlos. Open Banking e proteção de dados pessoais: convergências e divergências entre a LGPD e a regulação. In: Direito Público e Tecnologia. Coord. CRAVO. Daniela Copetti. JOBIM. Eduardo. JUNIOR. José Luiz de Moura Faleiros. Indaiatuba. Editora Foco. 2022.

HILDEBRANDT. Mireille. Defining Profiling: A New Type of Knowledge? In: Profiling the European Citizen: Cross Disciplinary Perspectives. Cham: Springer Science, 2008.

ITSRIO. Convergindo visões: meios de pagamento, LGPD e impactos regulatórios. 2022. Disponível em: https://itsrio.org/pt/varandas/convergindo-visoes-meios-de-pagamento-lgpd-e-impactos-regulatorios/. Acesso em 19 de junho de 2022.

ITSRIO. Privacidade em perspectivas. 2018. Disponível em https://itsrio.org/wp-content/uploads/2018/06/Privacidade-em-perspectivas_DTP.pdf. Acesso em 13 de agosto de 2023.

JABUR. Gilberto Haddad. Liberdade de pensamento e direito à vida privada. São Paulo: Revista dos Tribunais. 2000.

JUNIOR. Ivo Gico. Introdução ao Direito e Economia. In. Direito e economia no Brasil. Organizador Luciano Benetti Timm. 2ª ed. São Paulo. Atlas. 2018.

JUNIOR. José Luiz de Moura Faleiros. Open Banking, Governança de Dados e Responsabilidade Civil no Brasil: Algumas Reflexões. In: Revista de Dreito da Responsabilidade. 2021. Disponível em: https://revistadireitoresponsabilidade.pt/2021/open-banking-governanca-de-dados-e-responsabilidade-civil-no-brasil-algumas-reflexoes-jose-luiz-de-moura-faleiros-junior/. Acesso em 07 de setembro de 2022.

KAHNEMAN. Daniel. Rápido e Devagar: Duas formas de pensar. Tradução Cássio de Arantes Leite. 1ª edição. Rio de Janeiro. Objetiva. 2012

LACE, Susane. The Glass Consumer: life in a surveillance society. Bristol. Policy Press. 2005.

LINHARES. Edurdo. O aumento do crime financeiro no Brasil: a inteligência artificial do lado do banco e do consumidor. Tiinside. 05 de setembro de 2022. Disponívell em: https://tiinside.com.br/05/09/2022/o-aumento-do-crime-financeiro-no-brasil-a-inteligencia-artificial-do-lado-do-banco-e-do-consumidor/. Acesso em 02 de janeiro de 2023.

MALDONADO. Viviane Nóbrega; GUTIERREZ, Andriei. A estratégia brasileira para a transformação digital e as questões que dela emergem no que se refere à proteção de dados pessoais. Revista dos Tribunais. v. 993. 2018.

MANTELERO, Alessandro. Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. Computer Law & Security Review, v. 32, n. 2.

MARTINS. Pedro Bastos Lobo. Profiling na Lei Geral de Proteção de Dados: o livre desenvolvimento da personalidade em face da governamentalidade algorítmica. Coord. Brunello Souza Stancioli. Indaiatuba – SP. Editora Foco. 2022.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor. 1ª ed. Brasília: Saraiva, 2014.

MENDES. Felipe. Open Banking: a inovação do sistema financeiro na palma da mão. Revista Veja. Publicado em 31 de julho de 2020. Versão digital. Disponível em: https://veja.abril.com.br/economia/open-banking-a-inovacao-do-sistema-financeiro-na-palma-da-mao/

MILANESI, Diana. A New Banking Paradigm: The State of Open Banking in Europe, the United Kingdom, and the United States. TTLF Working Papers, n. 29, 2017. Disponível em: http://ttlf.stanford.edu. Acesso em: 21 de janeiro de 2023.

MORAES. Maria Celina Bodin. Ampliando os direitos da personalidade. In: José Ribas Vieira (org.), 20 anos da Constituição cidadã de 1988: efetivação ou impasse institucional?. Rio de Janeiro. Forense. 2008.

MORENO, Natália de Almeida. Análise de impacto regulatório. Revista dos Tribunais, vol. 951. 2015.

MULHOLLAND. Caitlin. Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (lei 13.709/2018). Disponível em: https://www.jur.puc-rio.br/wp-content/uploads/2021/07/IBERC_Responsabilidade-civil-e-dados-sensi%CC%81veis.pdf. Acesso em 03 de setembro de 2023.

NASCIMENTO. Loise C. Era Open Banking: a tecnologia na revolução do sistema financeiro. In: Fintechs, Bancos Digitais e Meios de Pagamento: Aspectos Regulatórios das novas tecnologias financeiras. Eroles. Pedro coordenador. São Paulo. Quartier Latin. 2019.

NETO. Roberto Campos. Apontamentos do Presidente do Banco Central do Brasil, Roberto Campos Neto. Workshop sobre Open banking. Maio/19. Disponível em https://www.bcb.gov.br/conteudo/home-ptbr/TextosApresentacoes/Apontamentos%20do%20Presidente_Open%20Banking%20v1.pdf. Acesso em 20 de outubro de 2022.

NISSENBAUM, Helen. Privacy in Context. Technology, Policy, and the Integrity of Social Life. Stanford, EUA: Stanford University Press, 2009.

OLIVEIRA. Lis Arrais e VERBICARO. Dennis. A vulnerabilidade algorítimica do consumidor: a extração e o compartillhamento de dados pessoais nas relações de consumo digitais. In: Direito do Consumidor e Novas Tecnologias. Coord. Marcos Ehrhardt Júnior, Marcos Catalan, Pablo Malheiros. Belo Horizonte. Editora Foco. 2021.

OLIVEIRA. Marco Aurélio Bellizze. LOPES. Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. In: Lei Geral

de Proteção de Dados Pessoais e suas repercussões no Direit Brasileiro. TEPEDINO. Gustavo. FRAZÃO. Ana. OLIVA. Milena Donato. São Paulo. Thomson Reuters. 2018.

OPEN BANKING: Banco Central adia para setembro de 2022 funcionameno completo. 1BILHAO. 2021. Disponível em: https://1bilhao.com.br/economia/open-banking-banco-central-adia-para-setembro-de-2022-funcionamento-completo/. Acesso em 26 de janeiro de 2023.

OPEN FINANCE. Conheça o open banking. Disponível em: https://openbankingbrasil.org.br/conheca-o-open-banking/. Acesso em 22 de junho de 2022.

OPEN FINANCE. Open Finance Brasil. Página inicial. Disponível em: https://openfinancebrasil.org.br/. Acesso em 10 de janeiro de 2023.

PACHECO. Thaise Maria Neves Duarte. PASQUAL. Cristina Stringari. Open Banking como instrumento para o desenvolvimento tecnológico a serviço do consumidor. In: Direito do Consumidor e Novas Tecnologias. Coord. Marcos Ehrhardt Júnior, Marcos Catalan, Pablo Malheiros. Belo Horizonte. Editora Foco. 2021.

PEREZ. Rafaella Di Palermo; STROHL. Juliana. Open Banking: Contexto cultural e experiência internacional. In: Fintechs, Bancos Digitais e Meios de Pagamento: Aspectos Regulatórios das novas tecnologias financeiras. Eroles. Pedro coordenador. São Paulo. Quartier Latin. 2019.

PINHEIRO. Patrícia Peck Garrido; SANTOS. Coriolano Aurélio de Almeida Camargo. Livre fluxo de dados é caminho sustentável para a economia digital. In Direito Digital Aplicado 3.0. Coordenadora Patrícia Peck Pinheiro. 1ª ed. São Paulo. Thomson Reuters Brasil. 2018.

POLIDO. Fabricio B. Pasquot Polido e outros. *GDPR e suas repercussões no direito brasileiro. Primeiras impressões de análise comparativa.* Instituto de Referência em Internet e Sociedade. 2018. Disponível em: http://irisbh.com.br/wp-content/uploads/2018/06/GDPR-e-suas-repercuss%C3%B5es-no-direito-brasileiro-Primeiras-impress%C3%B5es-de-an%C3%A1lise-comparativa-PT.pdf. Acesso em 16 de novembro de 2022.

PREMCHAND, Anshu; CHOUDHRY, Anurag. Open Banking & APIs for Transformation in Banking. 2018. International Conference on Communication, Computing and Internet of Things (IC3IoT). IEEE. 2018.

RAGAZZO. Carlos; Leite. Douglas. Desafios do compliance de dados para o setor financeiro: PIX, open Banking e a LGPD. In Compliance e políticas de proteçao de dados. Ana Frazão e Ricardo Villas Boas Cueva. coordenação. São Paulo. Thomson Reuters Brasil. 2021.

RAMOS. Cesar Augusto. Aristóteles e o sentido político da comunidade ante o liberalismo. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-512X2014000100004#_ftn3. Acesso em 21 novembro de 2022.

REALE. Miguel. O estado democrático de direito e o conflito das ideologias. São Paulo. Saraiva. 2005.

REVEAL. A linha vermelha: disparidades raciais nos empréstimos. 2018. Disponível em: https://revealnews.org/podcast/the-red-line-racial-disparities-in-lending-2/. Acesso em 26 de junho de 2022.

RIBARCZYK, Bruna Gabriela; CÉSAR DE OLIVEIRA, Júlio. Análise da Concentração Bancária Brasileira entre 2000-2011: o impacto da fusão do Itaú com o Unibanco. Revista Estudos do CEPE, n. 37. 2013.

RUBINSTEINN. Gabriel. Com apoio de bancos, governo endurece pena para crimes cibernéticos. Exame. 28 de maio de 2021. Disponível em: https://exame.com/future-of-money/cybersecurity/com-apoio-de-bancos-governo-endurece-pena-para-crimes-ciberneticos/. Acesso em 02 de janeiro de 2023.

RUSSI. Ana. Banco Central atrasa primeira fase do open banking. CNN. 27 de novembro de 2020. Disponível em: https://www.cnnbrasil.com.br/business/bc-atrasa-primeira-fase-do-open-banking-para-1-de-fevereiro-de-2021/. Acesso em 26 de janeiro de 2023.

SANTOS. Marcel Mascarenhas dos. Revolução Regulatória no Sistema Financeiro Nacional. In: Banking 4.0: Desafios jurídicos e regulatórios do novo paradigma bancário e de pagamentos. Coord. Bruzzi, Eduardo; Feigelson. Bruno. 1ª ed. Thomson Reuters. São Paulo. 2020.

SCHERMER, Bart et al. The Crisis of Consent: how stronger legal protection may lead to weaker consent in data protection. Ethics and Information Technology, 2014, vol. 16: 171-182. Disponível em: Disponível em: https://ssrn.com/abstract=2412418 ou http://dx.doi.org/10.2139/ssrn.2412418. Acesso em 30 de julho de 2023.SCHWARTZ. Paul M. SOLOVE. Daniel J. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1909366. Acesso em 18 de dezembro de 2022.

SILVA. Alberto Luis Camilier da. Palestra "O Direito e o ambiente digital – temas atuais". Proferida na OAB-SP em 14/11/2018. Disponível em: https://www.youtube.com/watch?v=SEQbQ4joQeg. Acesso em 07 de janeiro de 2024.

SILVA. Glacus Bedeschi da Silveira e Silva. Open Banking no Brasil: uma análise das normas relativas às APIs sob o prisma do direito concorrencial regulatório (Mestrado em Direito). Universidade Federal de Minas Gerais – UFMG. Belo Horizonte. 2021.

Skinner.Chris. Is Open Banking all it's craked up to be? Disponível em: https://thefinanser.com/2023/09/is-open-banking-all-its-cracked-up-to-be. Acesso em 19 de novembro de 2023.

SOUSA**.** CAPELO DE. O Direito Geral de Personalidade. Coimbra: Coimbra Editora. 2011.

STRAHILEVITZ. Lior; Kugler.Matthew B. Is privacy policy language irrelevante to consumers? Coase-Sandor Working Paper Series in Law and Economics, nº 776 (2016). Disponível em: https://chicagounbound.uchicago.edu/law_and_economics/796/. Acesso em 26 de junho de 2022.

SUNSTEIN. Cass R; THALER. Richard H. Nudge: Como tomar melhores decisões sobre saúde, dinheiro e felicidade. Tradução Angelo Lessa. 1ª edição. Rio de Janeiro. Objetiva. 2019.

SUTTO. Giovanna. De urubu do pix ao sequestro-relâmpago: veja em quais casos é possível recuperar o dinheiro perdido em golpes.. Infomoney. 11 de julho de 2022. Disponível em: https://www.infomoney.com.br/minhas-financas/de-urubu-do-pix-ao-sequestro-relampago-veja-em-quais-casos-e-possivel-recuperar-dinheiro-perdido-em-golpes. Acesso em 13 de janeiro de 2023.

TARTUCE. Flávio. Direito Civil. Lei de Introdução e Parte Geral. v.1. 13ª ed. Rio de Janeiro. Forense. 2017.

TEPEDINO. Gustavo. A tutela da personalidade no ordenamento civil-constitucional brasileiro. In: Temas de Direito Civil. 3ª ed. Renovar.

VEALE. Michael. Governing machine learning that matters. 2019. Tese de Doutorado em Science, Tecnhology, Engineering and Public Policy. University College London. Londres. 2019.

VIEIRA. Tatiana Malta. O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. (Mestrado em Direito, Estado e Sociedade: Políticas Públicas e Democracia) – Universidade de Brasília (UnB), Brasília.2007.

VILARINO, Ramon; VICENTE, Renato. Dissecting racial bias in a Credit Scoring System experimentally developed for the Brazilian population. arXivLabs. Nova Iorque. 2020. Disponível em: https://arxiv.org/abs/2011.09865. Acesso em 28 de dezembro de 2022.

ZANATTA. Rafael. SOUZA. Michel R. A tutela coletiva na proteção de dados pessoais: tendências e desafios. In: DE LUCCA, Newton; ROSA, Cíntia. Direito & Internet IV: Proteção de Dados Pessoais. São Paulo. Quartier Latin. 2019. Disponível em: https://www.researchgate.net/publication/344495215_A_Tutela_Coletiva_em_Protecao_de_Dados_Pessoais_tendencias_e_desafios/link/5f7c85dd458515b7cf6a54bc/download. Acesso em 02 de janeiro de 2023.

ZANOBIA. Luana. Bancos tradicionais se rendem às fintechs. Veja. 07 de setembro de 2022. Disponível em: https://veja.abril.com.br/economia/bancos-tradicionais-se-rendem-as-fintechs/ Acesso em 05 de janeiro de 2023.