Centro Universitário de Brasília - UniCEUB
Faculdade de Ciências Jurídicas e Sociais - FAJS
Curso de Bacharelado em Direito

LETICIA SOARES SOUTO

OPEN BANKING E A LEI GERAL DE PROTEÇÃO DE DADOS – LGPD: SEGURANÇA JURÍDICA E TRANSPARÊNCIA DAS INFORMAÇÕES

BRASÍLIA
2020

LETÍCIA SOARES SOUTO

OPEN BANKING E A LEI GERAL DE PROTEÇÃO DE DADOS – LGPD: SEGURANÇA JURÍDICA E TRANSPARÊNCIA DAS INFORMAÇÕES

Monografia apresentada como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (UniCEUB).

Orientadora: Professora Lucinéia Possar

BRASÍLIA
2020

LETÍCIA SOARES SOUTO

OPEN BANKING E A LEI GERAL DE PROTEÇÃO DE DADOS – LGPD: SEGURANÇA JURÍDICA E TRANSPARÊNCIA DAS INFORMAÇÕES

Monografia apresentada como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (UniCEUB).

Orientadora: Professora Lucinéia Possar

BRASÍLIA, 23 DE OUTUBRO DE 2020

BANCA AVALIADORA

_____

Professor(a) Orientador(a)

_____

Professor(a) Avaliador(a)

AGRADECIMENTOS

Sou muito grata a Deus acima de tudo, pela saúde e oportunidade de realizar mais esse sonho. À minha mãe, Maria de Fátima, pelo amor incondicional, paciência e apoio durante toda a minha vida. À toda a minha família pelo carinho e presença, mesmo que distante pela pandemia. Aos amigos que o UniCEUB me presenteou no decorrer do curso, em especial àqueles que sempre me ajudaram e foram fonte de inspiração para que eu não desistisse: Jaime, Wemerson, Caetano, Rafael, Luana, Ana Rachel, Waleska, Elon e tantos outros que marcaram minha jornada nesses anos de curso. Ao Banco do Brasil por acreditar e investir nos seus talentos, pelo suporte financeiro da bolsa de estudos que tanto me ajudou a permanecer no curso. Ao Alan, que coordena a frente da LGPD no BB, pelo conhecimento compartilhado e pelas valorosas contribuições e estímulo constantes. À Marina, minha grade amiga, pelo apoio e carinho diários e que, além de perguntar insistentemente sobre a monografia, me indicou a escolha mais que acertada da minha orientadora. Agradeço imensamente à minha orientadora, Prof.ª Lucinéia Possar, por não desistir de mim e deste trabalho, pelas palavras de motivação e apoio, por ser fonte de inspiração profissional, pelas observações tão relevantes e por sempre me fazer pensar e questionar sobre o tema do meu trabalho de pesquisa. Por fim agradeço aos funcionários do Núcleo de Pesquisa da FAJS pelo valioso auxílio na questão do prazo de depósito do presente trabalho. Sem cada um de vocês não seria possível a conclusão dessa etapa. Por isso o meu muito obrigada!

Ao futuro ou ao passado, a um tempo em que o pensamento seja livre, em que os homens sejam diferentes uns dos outros, em que não vivam sós - a um tempo em que a verdade exista e em que o que for feito não possa ser desfeito:
da era da uniformidade, da era da solidão, da era do Grande Irmão, da era do duplipensamento - Saudações!
(George Orwell)

RESUMO

O objetivo do presente trabalho é apresentar um breve histórico e a importância da proteção de dados no direito brasileiro, tomando como exemplo o *open banking* e sua relação com a Lei Geral de Proteção de Dados – LGPD. Para melhor ilustrar as consequências jurídicas da violação da privacidade e da proteção de dados, traz diversos exemplos de casos reais que incitaram a manifestação do poder judiciário para decidir acerca do tema, antes e depois da entrada em vigor da Lei. Explica a hipossuficiência do titular de dados em relação ao controlador e operador, chamada aqui de hipervulnerabilidade. Fala sobre o funcionamento do *open banking* como modelo de negócios que pode servir de exemplo bem sucedido no tratamento de dados de acordo com a legislação vigente e traz, por fim, o exemplo do Pix, novo sistema de pagamentos implementado pelo Banco Central do Brasil para demonstrar outra hipótese de consequência do desrespeito à proteção de dados e à livre manifestação do titular. Não possui o condão de exaurir as discussões, tamanha atualidade do tema, mas sim trazer reflexões acerca da complexidade envolvida ao se relacionar tecnologia e direito.

Palavras-chave: Proteção de dados. Privacidade. LGPD. GDPR. Consentimento. Dados pessoais. Titular de dados. ANPD. *Open banking. API.* Pix.

SUMÁRIO

INTRODUÇÃO

A preocupação do Estado com a regulamentação da proteção dos dados pessoais começou a se intensificar ao longo dos últimos vinte anos em virtude, principalmente, da evolução tecnológica e, de acordo com Pinheiro (2018), do quanto a sociedade digital tornou a economia global integrada e, de certa forma, dependente de fluxos internacionais de bases de dados.

Por sua vez, Bioni (2020) pontua que o estágio atual da sociedade demonstra que ela está desenhada sob uma nova forma de organização, onde a informação é o centro e o motor de desenvolvimento da economia.

Não há como compreender a importância do referido tema no mundo jurídico sem contextualizar o patamar atual da forma de ser da sociedade e os impactos dessa transformação, impulsionada principalmente pela expansão da internet.

O avanço tecnológico relacionado à internet, ocorrido especialmente nos últimos vinte anos, fez nascer novas formas mercado, consumo, produção, divulgação e distribuição de bens, serviços, conhecimentos, e até mesmo novos formatos de relacionamentos e interação social.

O que por um lado ampliou o acesso, reduzindo as distâncias, e de certa forma democratizou e tornou possível que a informação chegasse aos mais diversos confins do planeta, com uma velocidade sem precedentes, por outro lado fez com que surgissem novas demandas para o direito, até então impensadas e não previstas em legislação, doutrina e jurisprudência.

Em termos de volume, nenhuma época do passado remoto produziu e disseminou tantas informações em uma velocidade tão rápida quanto os últimos anos. Um estudo feito em 2015 demonstrou que 90% dos dados disponíveis para consumo naquele ano haviam sido produzidos nos dois anos anteriores e que, além disso, a cada biênio esse índice se duplica.[1]

[1] BSA. The Software Alliance. Qual é o “x” da questão com relação a dados? Disponível em: https://data.bsa.org/wp-content/uploads/2015/10/BSADataStudy_br.pdf. Acessado em: 20 de setembro de 2020.

É possível observar grande movimento da doutrina com diversas publicações a respeito do assunto, desde paralelos com outras áreas do direito, como o direito do consumidor até a complexa questão da autenticidade de provas processuais obtidas por meios digitais.

Já no âmbito legislativo, com exceção da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD), poucas leis esparsas tratam de maneira pontual da proteção de dados. E atualmente tramita no Congresso Nacional a proposta de Emenda Constitucional nº 17/2019 para a inclusão do tema de forma expressa e inequívoca sob o manto dos direitos e garantias fundamentais.

A LGPD trouxe para o mundo jurídico as premissas para o tratamento de dados pessoais, princípios que devem orientar a conduta dos agentes de tratamento, além de dez possíveis bases legais para justificar o tratamento de dados por empresas e entidades.

A verdade é que a revolução digital trouxe inúmeras mudanças de paradigma para as relações contratuais e de consumo. E as instituições financeiras não ficaram de fora dessas transformações.

O tema *open banking* tem tido grande relevância no mundo no que diz respeito à inovação no mercado financeiro. Nesse contexto, a Europa foi uma das precursoras no *start* da regulamentação do assunto com a edição, em maio de 2016, do documento "*Understanding the business relevance of Open APIs and Open banking for banks*", pela *Euro Banking Association*[2].

O documento trouxe diretrizes relativas ao uso de interfaces de aplicações para a troca de informações entre bancos e entre bancos e empresas de outro segmento, a fim de proporcionar o acesso aos serviços bancários por meio de outras plataformas pelos usuários.

Outra frente importante para a regulação das novas tecnologias agregadas aos serviços financeiros foi o relatório elaborado pela Comissão de Assuntos Econômicos e Monetários e votado no Parlamento Europeu sobre *FinTech*, em abril de 2017.

---

[2] Fórum do setor de pagamentos europeu, composto por cerca de duzentos bancos e organizações membros da União Europeia e de todo o mundo, que tem por objetivo promover e impulsionar inovações nos meios de pagamento.

O documento destacou como um dos motivos da inclusão do assunto na pauta a transformação no mercado proporcionada pelo “desenvolvimento de novos serviços financeiros e a digitalização dos serviços existentes (...) através da introdução de novas formas de concorrência, inovação, parcerias e externalização.” Quanto à segurança, especialmente em relação a ataques cibernéticos, a referida Comissão chamou a atenção para o especial risco ao qual o mercado financeiro está sujeito e que, portanto, a segurança, a confiabilidade e a continuidade na prestação dos serviços são condições *sine qua non* de existência e perenidade na prestação de serviços para os consumidores. Estes que, de acordo com o mesmo documento, estão em situação de extrema vulnerabilidade quanto à possibilidade de ataques *hackers* e sequestro de dados pessoais.

O pioneirismo das instituições bancárias e financeiras no uso de tecnologias de segurança da informação e o alto nível de regulação que é inerente a esse nicho de mercado são fatores que sugerem que o modelo de negócios proposto pelo *open banking* possa servir de referência no uso e tratamento de dados pessoais, sem prejudicar os direitos individuais envolvidos.

Nesse sentido, será abordado no presente trabalho de que forma o *open banking* se relaciona com a LGPD e como essa relação pode ser vista sob a ótica da segurança jurídica e da transparência.

O objetivo é analisar de que forma se construiu a proteção aos dados pessoais no Brasil e de que maneira isso se relaciona com o *open banking*. Para tentar estabelecer esse paralelo, optou-se por dividi-lo em seis capítulos.

No primeiro, serão trazidos alguns marcos históricos importantes, do Brasil e do mundo, sobre a privacidade e a proteção de dados enquanto direitos fundamentais.

Já no capítulo subsequente, falaremos especificamente sobre a LGPD, seus princípios, conceitos, a inspiração no regulamento europeu, uma análise comparativa entre ambos, sua repercussão no mundo jurídico, mesmo antes de sua vigência, além de seu longo processo legislativo e seus percalços.

No terceiro capítulo, será trazido à baila o tema da hipervulnerabilidade do titular de dados, processos que podem auxiliar na proteção dos dados pessoais, consequências e exemplos práticos de eventos de vazamentos de dados.

A judicialização da proteção de dados será abordada no capítulo quatro, que conta com diversos exemplos de situações em que o judiciário foi chamado a decidir sobre práticas abusivas, antes e depois da entrada em vigor da Lei.

Por fim, o capítulo cinco aborda o *open banking* em si, como funciona o modelo, em que base legal da LGPD se apoia, além de trazer aspectos sobre o exemplo mais notável na esteira dessa iniciativa no Brasil: o Pix.

Para compreender melhor o conteúdo do presente trabalho, a consulta do leitor ao glossário (disponível na página 46) poderá ser necessária. O glossário contém as expressões e conceitos específicos das áreas de conhecimento abrangidas aqui, bem como os termos e palavras estrangeiras, com seus respectivos significados.

Por fim, não é demais lembrar que o presente trabalho não tem a pretensão de exaurir a discussão, mas apenas a expectativa de que este estudo seja um ponto de partida para o debate permanente sobre o tema, o qual deverá ser revisitado e atualizado permanentemente.

1. PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS: DIREITOS FUNDAMENTAIS

O reconhecimento da privacidade e da proteção de dados enquanto direitos aconteceu em momentos e de maneiras distintas em cada continente, de acordo com as concepções relacionadas ao papel do Estado em cada país, seu grau de abertura à internacionalização e, em todos os casos, atrelada à evolução tecnológica ocorrida em especial a partir da década de 60.

Este capítulo não possui o condão de exaurir todas as nuances relativas ao tema, mas propõe uma breve síntese histórica desses institutos a título exemplificativo.

Sendo o dado atrelado à esfera de uma pessoa, dá-se a ele a conceituação de dado pessoal. O dado pessoal na atual sociedade da informação representa a projeção, extensão e dimensão da própria pessoa. A proteção destes dados, portanto, faz parte da família de direitos da personalidade, que começaram a ter sua garantia chancelada nas constituições das nações a partir do período pós Segunda Guerra mundial (PINHEIRO, 2018).

Importante pontuar que, não obstante se tratar de conceitos distintos, privacidade e proteção de dados estão intimamente ligados, uma vez que as informações e os dados pessoais são desdobramentos naturais da privacidade dos indivíduos.

Sem adentrar às minúcias da diferenciação técnica dos conceitos de dado e informação, o denominador comum de todo o processo nos últimos quarenta anos é a proteção de dados vista como uma espécie de herdeira da privacidade. Esse entendimento foi trazido à baila pelo Conselho Europeu, na Convenção de Strasbourg, em 1981, ao definir que informação pessoal é qualquer informação referente a uma pessoa identificada ou suscetível de identificação. (SDE/DPDC, 2010).

Nas palavras de Costa (2018), privacidade se refere à possibilidade de o indivíduo dominar as informações pertencentes a si e sobre elas exercer controle, de acordo com seus valores e interesses. Refere-se a:

> [...] um conjunto de informações acerca de um indivíduo, que, por sua vez, pode decidir mantê-las sob o seu controle exclusivamente ou, se quiser, comunicar a outrem nas condições que desejar. É uma

> faculdade que cada pessoa tem de impedir a intromissão de estranhos na sua vida privada e familiar.

Já a concepção embrionária da proteção de dados enquanto bem jurídico a ser tutelado remonta ao ano de 1890 a partir da publicação do artigo *The Right to Privacy* pelos norte-americanos Samuel Warren e Louis D. Brandeis, que defendiam a ideia de um direito básico do indivíduo a estar sozinho. A partir desse estudo começou-se a destrinchar a ideia de que a decisão sobre publicar ou não informações pessoais pertenceria ao próprio indivíduo (RUARO; RODRIGUEZ; FINGER, 2011).

O artigo de Warren e Brandeis teve ampla repercussão nos debates que se seguiram acerca do tema e, muito embora a privacidade seja um componente essencial à própria identidade de formação dos Estados Unidos, pela ideia muito forte e arraigada da garantia das liberdades individuais frente à intervenção estatal, foi na Europa que o tema ganhou espaço e relevância no âmbito legislativo em primeiro lugar (WIMMER, 2020).

De acordo com Mayer-Schonberger *apud* Wimmer (2020), datam da década de 70 as primeiras leis europeias sobre proteção de dados: *Hessisches Datenschutzgesetz,* de Hesse, na Alemanha (1970), *Datalag*, na Suécia (1974), além dos Estatutos de Proteção de Dados da França e da Áustria (1978), os dois últimos inaugurando a chamada segunda geração de leis de proteção aos dados pessoais.

Quase cem anos depois da publicação do artigo *The Right to Privacy* nos Estados Unidos, foi na Alemanha em 1983 que o Tribunal Constitucional Federal positivou o chamado direito à autodeterminação informativa (SCHAAR *apud* RUARO; RODRIGUEZ; FINGER, 2011).

No ano 2000 a proteção de dados foi então alçada ao status de direito fundamental em âmbito continental, conforme o art. 8º da Carta de Direitos Fundamentais da União Europeia:

> Protecção de Dados Pessoais
>
> 1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal, que lhes digam respeito.
> 2. Esses dados devem ser objecto de tratamento leal, para fins específicos e com **consentimento** da pessoa interessada **ou com outro fundamento legítimo previsto por lei**. Todas as pessoas têm o direito de aceder aos dados coligidos que lhe digam respeito e de obter a respectiva rectificação.

> 3. O cumprimento destas regras fica sujeito a **fiscalização por parte de uma autoridade independente**. (grifo nosso)

Já no direito brasileiro, de acordo com Zanatta (2020), a base para a concepção da proteção de dados enquanto valor jurídico reconhecido remonta ao início da década de 90, quando o país começou um movimento mais consistente de abertura ao mercado internacional, intensificando-se, por consequência, a preocupação com os direitos do consumidor.

A Constituição Federal de 1988 materializou a importância deste tema enquanto direito fundamental, prevendo no rol do consagrado art. 5º:

> XXXII - o Estado promoverá, na forma da lei, a defesa do consumidor.

Ademais, reforçou a relevância da pauta ao prever a defesa do consumidor como princípio balizador da ordem econômica e financeira, conforme disposto no art. 170 da Carta Magna:

> Art. 170. A ordem econômica, fundada na valorização do trabalho humano e na livre iniciativa, tem por fim assegurar a todos existência digna, conforme os ditames da justiça social, observados os seguintes princípios: [...]
> V - defesa do consumidor;

Foi nessa mesma época que surgiram as primeiras versões do anteprojeto da Lei Geral de Proteção de Dados sob a condução do Departamento de Proteção e Defesa do Consumidor. À época estava em pleno vapor um movimento político:

> (...) de afirmação da defesa do consumidor como objetivo constitucional em 1988 e de definição das estruturas regulatórias de defesa do consumidor no Código de Defesa do Consumidor (Zanatta, 2020).

Não obstante o constituinte originário não ter previsto explicitamente a proteção aos dados pessoais no texto da Carta Magna, já se reconhecia a relevância do assunto, uma vez que foi contemplado como objeto de um dos principais remédios constitucionais previstos no art. 5º:

> LXXII - conceder-se-á habeas data:
> a) para **assegurar o conhecimento de informações relativas à pessoa do impetrante**, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
> b) para a **retificação de dados**, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo. (grifo nosso)

Já a privacidade foi expressamente arrolada como um direito fundamental e cláusula pétrea, porquanto prevista no inciso X do art. 5º:

> [...] são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

A preocupação do Estado brasileiro em legislar e estabelecer políticas públicas voltadas à proteção de dados ganhou um reforço nos anos seguintes com a promulgação do Código de Defesa do Consumidor, de 1990, que previu em seu artigo 43 a garantia de acesso aos dados pessoais e de consumo em bancos de dados mantidos por fornecedores:

> O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

A ideia do legislador à época foi, principalmente, estabelecer uma garantia mínima contra eventuais abusos no tratamento de dados relativos à concessão de crédito. No entanto, com a expansão da internet e o aumento exponencial do tratamento de dados dos consumidores pelo mercado para a definição de perfil de consumo, oferta direcionada, ações de marketing, entre outras estratégias, o que foi previsto até então já não se mostrava suficiente para a proteção adequada dos direitos relativos à proteção de dados, à privacidade dos indivíduos e à própria relação de consumo. Esta se tornou mais dinâmica e de certa forma aumentou a hipossuficiência dos consumidores frente ao domínio e ao investimento massivo em tecnologia por parte dos fornecedores (SDE/DPDC, 2010).

Com a adoção do novo Código Civil em 2002, o direito à privacidade foi contemplado no rol dos direitos relativos à personalidade, no art. 21, fortalecendo o

estabelecido na Constituição no que se refere à previsão de indenização e outras sanções em caso de violação ou ameaça de lesão a esse bem jurídico:

> [...] A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

Muito embora a relevância da tutela jurídica ao referido tema seja dotada de certa obviedade, o Supremo Tribunal Federal enfrentou em 2015 o embate entre o direito à privacidade e à intimidade e o direito à informação, na apreciação da Ação Direta de Inconstitucionalidade nº 4815/DF. Na ocasião discutiu-se a aplicação e o sopesamento dos princípios dispostos na CF/88 relativos à intimidade versus o disposto também na Carta Magna sobre transparência no acesso e divulgação de informações, tendo em vista a proibição constitucional a qualquer tipo de censura.

O caso concreto referia-se à necessidade ou não de prévia autorização dos indivíduos para a produção de biografias a respeito de sua história e de sua vida privada. Decidiu o STF, por unanimidade, nesse caso, pela prevalência da transparência das informações sobre o direito à intimidade:

> Ação direta julgada procedente para dar interpretação conforme à Constituição aos arts. 20 e 21 do Código Civil, sem redução de texto, para, em consonância com os direitos fundamentais à liberdade de pensamento e de sua expressão, de criação artística, produção científica, declarar **inexigível autorização de pessoa biografada relativamente a obras biográficas literárias ou audiovisuais, sendo também desnecessária autorização de pessoas retratadas como coadjuvantes** (ou de seus familiares, em caso de pessoas falecidas ou ausentes).

No entendimento da Corte, em especial no voto da relatora, ministra Carmen Lúcia, a preponderância do direito à informação sobre o direito à intimidade no caso em questão não causaria prejuízos ao indivíduo, uma vez que este está resguardado pelo amparo legal que prevê possibilidade de indenização para o caso de eventuais excessos. E que, do contrário, deixar a critério do biografado a decisão por publicar ou não determinada obra caracterizaria sim violação à liberdade de expressão:

> [...] Há o risco de abusos. Não apenas no dizer, mas também no escrever. Vida é experiência de riscos. Riscos há sempre e em tudo e para tudo. Mas o direito preconiza formas de serem reparados os

> abusos, por indenização a ser fixada segundo o que se tenha demonstrado como dano. O mais é censura. E censura é forma de "calar a boca". Pior: calar a Constituição, amordaçar a liberdade, para se viver o faz de conta, deixar-se de ver o que ocorreu. [...]

Tangenciando o tema, porém sob outra perspectiva, o Senado Federal já havia aprovado em 2011 o projeto de lei que deu origem à LAI – Lei de Acesso à Informação. A Lei de nº 12.527 foi concebida com o objetivo primordial de garantir aos cidadãos o acesso facilitado a informações de seu interesse ou de interesse coletivo constantes de bancos de dados e registros mantidos por órgãos e entidades estatais. Trata-se de uma ótica de empoderamento do cidadão no exercício de exigir mais transparência e participação na atuação do Estado (JARDIM, 2012).

Seguiu-se à lei o Decreto nº 7.724/2012, que regulamentou a forma como se dariam as solicitações e o fornecimento dos dados pelos órgãos e entes estatais, bem como os prazos, grau de sigilo das informações, instâncias recursais, entre outras particularidades.

Na linha temporal da proteção legal à privacidade e aos dados, muito embora não seja escopo deste trabalho explorar a esfera criminal, houve também a publicação da Lei nº 12.737/2012, conhecida popularmente como Lei Carolina Dieckmann (atriz brasileira que teve seu computador invadido e suas fotos íntimas expostas na internet).

O diploma legal alterou o Código Penal, incluindo o art. 154-A, que passou a prever o crime de invasão de equipamento de informática com o objetivo de obter, alterar ou destruir dados e informações, sem o consentimento do proprietário do equipamento. Esse é mais um marco normativo motivado pela hipervulnerabilidade dos indivíduos e de seus dados frente aos riscos de violação e abuso, tema que será explorado com mais detalhes no capítulo 3 do presente trabalho.

Ainda sobre os "ensaios" ao surgimento da LGPD, foi em 2009 que se deu a principal iniciativa anterior no que se refere à privacidade e à proteção de dados no Brasil: a elaboração do projeto de lei do que veio a se tornar o Marco Civil da Internet, materializado na Lei nº 12.965/2014.

Os debates que resultaram no projeto de lei do Marco Civil da Internet tiveram início em 2006, observando como ponto de partida a quantidade cada vez maior de usuários da rede mundial de computadores e a expansão do comércio eletrônico (LEONARDI, 2020).

Foram realizadas duas fases de consultas públicas ao anteprojeto, em 2009 e em 2010, e no ano seguinte o documento foi enviado à Câmara dos Deputados.

O trâmite do projeto seguia o ritmo comum às demais iniciativas legais quando, em setembro de 2013, documentos divulgados na mídia e trazidos à tona pelo ex-agente da Agência Central de Inteligência (CIA) e da Agência de Segurança Nacional dos Estados Unidos (NSA), Edward Snowden, revelaram que órgãos e empresas integrantes do Estado brasileiro, como a Presidência da República e a Petrobras, além de pessoas residentes ou em trânsito no Brasil, vinham sendo alvo de espionagem nos últimos quatro anos pela NSA (BESSA, 2017).

O escândalo fez com que o Marco Civil da Internet entrasse em votação em regime de urgência na Câmara dos Deputados, porém sem consenso naquele ano, o que fez com que a pauta da casa legislativa fosse trancada por diversas vezes até ser enfim aprovado o projeto e convertido em lei em abril de 2014.

Ainda que carente de algumas definições de conceitos importantes, a Lei nº 12.965/2014 (Marco Civil da Internet) foi o primeiro diploma legal brasileiro a trazer como premissas para o uso da internet a proteção à privacidade, além de prever, especialmente em seu art. 7º, incisos VIII, IX e X, garantias quanto à coleta, uso, tratamento, armazenamento e exclusão de dados pessoais dos usuários. Nesse contexto, importante para a presente monografia transcrever parte de sua exposição de motivos:

> [...] No panorama normativo, o anteprojeto representa um primeiro passo no caminho legislativo, sob a premissa de que uma proposta legislativa transversal e convergente possibilitará um posicionamento futuro mais adequado sobre outros importantes temas relacionados à internet que ainda carecem de harmonização, como a proteção de dados pessoais, o comércio eletrônico, os crimes cibernéticos, o direito autoral, a governança da internet e a regulação da atividade dos centros públicos de acesso à internet, entre outros. A despeito das mencionadas lacunas normativas, a solução que se submete à avaliação de Vossa Excelência faz jus ao potencial criativo e inovador característico do povo brasileiro, alçando o país à posição de protagonista mundial na garantia das novas liberdades da cultura digital.[3]

3 BRASIL. Casa Civil. EMI Nº 00086 - MJ/MP/MCT/MC. Disponível em: http://www.planalto.gov.br/ccivil_03/Projetos/ExpMotiv/EMI/2011/86-MJ%20MP%20MCT%20MC.htm. Acessado em: 10 de outubro de 2020

De acordo com Leonardi (2020), pode-se extrair do trecho em destaque, e observa-se na leitura dos artigos da Lei, que o Marco Civil da Internet não se propôs a esgotar o assunto e sim a ser o instrumento balizador de princípios gerais a serem observados na ausência de uma lei específica para tratar sobre os temas ali abrangidos.

Pode-se depreender essa conclusão a partir do exemplo do inciso III do art. 3º da Lei nº 12.965/2014:

> [...] a disciplina do uso da internet no Brasil tem os seguintes princípios: proteção dos dados pessoais, **na forma da lei**. (grifo nosso).

Há, no momento, uma Proposta de Emenda à Constituição de nº 17/2019, em tramitação no Congresso Nacional, que propõe a inclusão da proteção dos dados pessoais entre os direitos e garantias fundamentais do art. 5º da Carta Magna e insere como competência privativa da União a regulamentação do assunto no art. 22. A proposta já tramitou nas comissões e atualmente aguarda apreciação pelo Plenário.

Nesse contexto, e como tema central do presente trabalho, imperiosa a análise sobre a Lei nº 13.709/2018 (LGPD), que instituiu as normas específicas sobre proteção de dados no país.

2. A LEI 13.709/2018: LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

A necessidade de uma lei específica sobre proteção de dados pessoais, de acordo com Pinheiro (2018), decorre, em essência, da forma como está sustentado o atual modelo de negócios da sociedade digital, onde a informação passou a ser a principal e mais valiosa moeda de troca do mercado.

A Lei Geral de Proteção de Dados, chamada neste trabalho apenas de LGPD ou Lei, originou-se do Projeto de Lei nº 53/2018 e foi promulgada com o objetivo de regulamentar, em um nível mais pormenorizado que o Marco Civil da Internet, os direitos e obrigações referentes ao uso, armazenamento e tratamento de dados pessoais dos cidadãos por pessoas naturais ou jurídicas, de direito público ou privado.

De forma resumida, conforme Paludetto e Barbieri (2019), o principal objetivo da LGPD é garantir a privacidade dos dados pessoais e viabilizar um controle maior dos indivíduos sobre esses dados.

A Lei brasileira teve como inspiração e modelo o regulamento europeu de proteção de dados, *General Data Protection Regulation* – GDPR, marco de referência mundial aprovado em 2016, que instituiu as normas relativas à proteção de dados dos cidadãos dos países da União Europeia e do Espaço Econômico Europeu (CALABRICH, 2019).

A ideia do legislador, ao estabelecer um diploma seguindo as diretrizes do regulamento europeu, conforme trazido por Silva (2020), foi elevar a reputação brasileira a um nível adequado a ponto de oferecer segurança jurídica aos demais países no estabelecimento de relações que envolvam o fluxo de dados internacional.

Conforme pontuado por Pinheiro (2018), o pioneirismo europeu nas discussões e no estabelecimento de normas a esse respeito de certa forma “obrigou” os demais países a elaborarem sua própria legislação a respeito do tema. Especialmente porque as relações comerciais da União Europeia com outras nações estariam condicionadas a estas observarem os mesmos cuidados com a proteção de dados pessoais de seus cidadãos. Dessa maneira, o regulamento europeu não se tornaria inócuo com a globalização das interações econômicas.

Tal qual a legislação brasileira, o GDPR também previu um período de *vacatio legis* de dois anos. E as penalidades começaram, no caso do regulamento europeu, a

serem aplicadas apenas a partir de 2018. Detalhes sobre as sanções na legislação brasileira serão discorridos no capítulo 4 deste trabalho.

Na esteira até a sua entrada em vigor, em 18 de setembro de 2020, a LGPD passou, ao longo desses dois anos, por um processo legislativo um tanto quanto conturbado e marcado pela intensa participação da sociedade, incertezas e pressão política de diferentes setores (ALMEIDA, 2020).

Originalmente, a LGPD estaria em plena vigência a partir de fevereiro de 2020. No entanto, em julho de 2019 foi aprovada a Lei nº 13.853/2019 que, dentre outros assuntos, previu a criação da Autoridade Nacional de Proteção de Dados[4] e alterou a entrada em vigor da LGPD para agosto de 2020.

Em abril de 2020 foi aprovado no Senado Federal o Projeto de Lei nº 1179, que, entre outras questões, propôs mais uma alteração da *vacatio legis*, com seu início postergado para janeiro de 2021, com a possibilidade de aplicação de penalidades apenas a partir de agosto do mesmo ano. Na justificativa do projeto, a casa legislativa argumentou que a crise de saúde mundial decorrente da pandemia do Covid-19 seria motivo suficiente para adiar por mais dezoito meses a possibilidade de aplicação de penalidades, com o objetivo de não onerar ainda mais as empresas em face das enormes dificuldades econômicas advindas da crise do coronavírus.[5]

Ainda em abril de 2020, foi editada a Medida Provisória nº 959 alterando a eficácia da LGPD, inclusive em relação aos aspectos sancionatórios, para maio de 2021.

O PL nº 1179 foi então aprovado pela Câmara dos Deputados, em maio de 2020, com alteração proposta pela casa legislativa para que a LGPD entrasse em vigor conforme o previsto na MP Nº 959, porém prevendo a possibilidade de sanções administrativas somente a partir de agosto de 2021, mantendo sua proposta original nesse ponto.

Em junho de 2020, foi publicada a Lei nº 14.010/2020 que alterou a previsão da aplicação de sanções administrativas decorrentes da LGPD para agosto de 2021. E no final de agosto, o Senado Federal aprovou a MP nº 959 com o detalhe da

---

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

[5] BRASIL. Senado Federal. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/141306. Acessado em: 20 de setembro de 2020.

prejudicialidade do artigo que previa o adiamento da vigência da LGPD para o fim do período de calamidade pública.

O resultado, em síntese, foi a entrada em vigor da LGPD em 18 de setembro de 2020, em relação às normas e às disposições acerca da proteção de dados e, no tocante à aplicação das sanções administrativas, a partir de 1º de agosto de 2021.

O fato é que, mesmo no período de *vacatio legis*, e, não obstante o adiamento da aplicabilidade de penalidades administrativas, as disposições da LGPD já repercutem no mundo jurídico. Antes mesmo de sua entrada em vigor, a lei foi usada como fundamento para o deferimento de medida cautelar pelo Supremo Tribunal Federal à Ação Direta de Inconstitucionalidade de nº 6387/DF, ajuizada pelo Conselho Federal da OAB, que pedia a suspensão da eficácia da Medida Provisória nº 954, publicada pelo Poder Executivo em 17 de abril de 2020.

O normativo previa o amplo compartilhamento de dados pessoais entre as operadoras de telefonia e o Instituto Brasileiro de Geografia Estatística/IBGE, implicitamente justificado pela pandemia do coronavírus.

No entender da Ministra Rosa Weber, relatora da medida cautelar no STF, não restou comprovado o legítimo interesse público na obtenção dos dados e tampouco evidenciado o benefício na elaboração de políticas voltadas para o combate à crise sanitária. Conforme a decisão:

> [..] Nessa ordem de ideias, não emerge da Medida Provisória nº 954/2020 [...] interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia, considerados a necessidade, a adequação e a proporcionalidade da medida. [...] a MP nº 954/2020 não apresenta mecanismo técnico ou administrativo apto a proteger os dados pessoais de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na sua transmissão, seja no seu tratamento. [...] Não bastasse, a ausência de garantias de tratamento adequado e seguro dos dados compartilhados parece-me **agravada pela circunstância de que, embora aprovada, não está em vigor a Lei Geral de Proteção de Dados Pessoais** (Lei nº 13.709/2018) [...] Não se subestima a gravidade do cenário de urgência decorrente da crise sanitária [...] o seu combate, todavia, não pode legitimar o atropelo de garantias fundamentais consagradas na Constituição. Reforço, em cumprimento ao dever de justificação decisória, no âmbito de medida liminar, que a adequada tutela do direito à intimidade, privacidade e proteção de dados pessoais é estruturada pela característica da inviolabilidade. Vale dizer, uma vez afrontada a norma de proteção de tais direitos, o ressarcimento se apresenta como tutela insuficiente aos deveres de proteção. (grifo nosso)

Superadas as reviravoltas normativas, é importante compreender a estrutura formal da Lei n. 13.709/2018, cujo texto legal está assim dividido:

> Capítulo I – Disposições Preliminares
> Arts. 1º ao 6º
>
> Capítulo II – Do Tratamento de Dados Pessoais
> Arts. 7º ao 16
>
> Capítulo III – Dos Direitos do Titular
> Arts. 17 ao 22
>
> Capítulo IV – Do Tratamento de Dados Pessoais pelo Poder Público
> Arts. 23 ao 32
>
> Capítulo V – Da Transferência Internacional de Dados
> Arts. 33 ao 36
>
> Capítulo VI – Dos Agentes de Tratamento de Dados Pessoais
> Arts. 37 ao 45
>
> Capítulo VII – Da Segurança e das Boas Práticas
> Arts. 46 ao 51
>
> Capítulo VIII – Da Fiscalização
> Arts. 52 ao 54
>
> Capítulo IX – Da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade
> Arts. 55-A ao 58-B
>
> Capítulo X – Disposições Finais e Transitórias
> Arts. 60 ao 65

A par disso, cabe destacar os princípios orientadores das atividades de tratamento de dados trazidos pela LGPD.

Em um panorama geral, a Lei definiu os principais atores do processo de gestão, troca e consumo de dados e informações, categorizou os dados de acordo com a criticidade de seu conteúdo, enumerou os princípios que devem ser seguidos pelas pessoas que fazem uso dos dados, definiu as bases legais possíveis para o tratamento de dados, estabeleceu sanções pelo descumprimento da norma e propôs a criação da Autoridade Nacional de Proteção de Dados, que é uma espécie de órgão de controle responsável por fiscalizar e aplicar sanções pelo descumprimento da lei, além de estabelecer normas técnicas específicas.

Alguns conceitos trazidos pela LGPD precisam estar claros para o melhor entendimento do presente trabalho. Os principais são os previstos no art. 5º da Lei nº 13.709/2018:

> [...] I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 13.853, de 2019) Vigência
> IX - agentes de tratamento: o controlador e o operador;
> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
> XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
> [...]
> XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

O fundamento principiológico da LGPD permeia diversas searas do mundo jurídico, mas está voltado especialmente ao direito à liberdade, à privacidade e à dignidade da pessoa humana. Nas palavras de Blum (2018):

> O homem não é uma coisa ou um objeto cujos dados possam ser tratados simplesmente como meio por eventuais fornecedores despreocupados com o respeito à sua privacidade, mas, sim, deve ser tratado com o devido respeito ao ser humano que é, ou seja, deve ser respeitado como fim em si mesmo.

De acordo com o estabelecido na LGPD, toda atividade realizada por pessoa física (para fins econômicos) ou jurídica que envolva o uso, o armazenamento e a disponibilização de dados deve observar os princípios da finalidade, da adequação, da necessidade, do livre acesso, da transparência, da segurança, da responsabilização e da prestação de contas, além da boa-fé objetiva.

E todos esses princípios que possibilitam o tratamento dos dados pessoais permeiam as dez bases legais[6], elencadas no art. 7º da Lei, a saber: consentimento, legítimo interesse, cumprimento de obrigação legal ou regulatória, execução de políticas públicas previstas em lei, realização de estudos por órgãos de pesquisa[7], execução de contrato, proteção do crédito, exercício regular de diretos em litígios judiciais, administrativos ou arbitrais, proteção da vida ou incolumidade física e tutela da saúde.

Apesar de declaradamente inspirada na norma europeia, Pinheiro (2018) ressalta que a Lei brasileira veio mais concisa e deixou certa margem para insegurança jurídica em alguns pontos. Um exemplo disso ocorre na determinação de prazos. Enquanto o regulamento europeu estabelece com exatidão (ex.: as empresas estão obrigadas a notificar os usuários e as autoridades em até 72 horas após uma ocorrência de vazamento de dados), a LGPD usa termos como “prazo razoável”.

Mais exemplos podem ser observados na tabela abaixo:

Tabela 1 – Comparativo GDPR x LGPD

Tema	GDPR	LGPD
Prazo para que as empresas respondam às solicitações dos usuários (portabilidade,	30 dias	15 dias

[6] Hipóteses jurídico-legais de tratamento de dados disciplinadas na Lei nº 13.709/2018.
[7] Garantida, sempre que possível, a anonimização dos dados pessoais, conforme versa o inciso IV do art. 7º da lei nº 13.709/2018.

correção ou exclusão de informações)		
Prazo para notificação de incidente de vazamento de dados à autoridade competente	Até 72 horas	Fala em “prazo razoável”
Tratamento de dados sensíveis	A regra é o NÃO tratamento. Admite-se exceções em situações específicas, como: dados tornados públicos pelo titular, cumprimento de obrigação legal ou exercício de funções do interesse público	Pode ocorrer com a autorização do titular em situações específicas ou, ainda, para de cumprimento de obrigação legal pelo controlador, exercício regular de direitos e até mesmo a proteção da vida do titular ou de terceiros
Tratamento de dados de menores de idade	O consentimento pode ser dado pelo titular, a partir de 16 anos. Abaixo disso, somente pelos responsáveis legais.	O consentimento para tratamento de dados de menores de 18 anos deve ser concedido pelos responsáveis legais
Boas práticas e governança	Obriga os controladores de dados a adotar medidas que assegurem que o tratamento de dados está de acordo com o regulamento	Faculta aos controladores a criação de boas práticas para o tratamento de dados
Relação entre operador e controlador de dados	Prevê a exigência de contrato ou outro ato jurídico que vincule o	Não especifica que tipo de vínculo deve haver, limitando-se a

	operador e o controlador, caso sejam pessoas distintas	dispor que o operador deve seguir instruções do controlador
Procedimentos para o processamento de dados pessoais para fins de marketing direto	Definiu requisitos e etapas específicos a serem seguidos	Não há referência direta ao assunto

Fonte: PINHEIRO, Patricia Peck. 2018. Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.
MACHADO, José Mauro Decossau. SANTOS, Matheus Chucri dos. PARANHOS, Mário Cosac Oliveira. LGPD e GDPR: Uma análise comparativa entre as legislações. Disponível em: http://www.pinheironeto.com.br/publicacoes/lgpd-e-gdpr-uma-analise-comparativa-entre-as-legislacoes. Acessado em 05 de agosto de 2020.

Além disso, diferentemente da legislação europeia, de acordo com Bioni (2020), a LGPD não fez uma sistematização adequada ao discorrer sobre a pseudoanonimização, instituto que será explicado no próximo Capítulo.

Enquanto o GDPR enumerou até mesmo incentivos para o uso desse recurso, com a flexibilização de algumas obrigações legais, a lei brasileira limitou-se a citar o processo como sendo algo a ser aplicado de maneira pontual. Perder-se-ia, dessa forma, uma oportunidade de reduzir de modo significativo os riscos de um eventual incidente de segurança relacionado a vazamento de dados, uma vez que a pseudoanonimização dificultaria sobremaneira a reversão por terceiros, pois os dados que permitiriam a identificação pessoal estariam em base separada, mantida pela própria organização (BIONI, 2020).

3. HIPERVULNERABILIDADE DO TITULAR DE DADOS

Em diversos ramos do direito, pode-se observar um esforço do Estado na tentativa de minimizar as assimetrias decorrentes da própria dinâmica social inerente ao contexto em que as relações se estabelecem e de trazer mais equilíbrio entre as partes. Nas palavras de Bioni (2020), é quando entra em cena:

> O paradigma protetivo que reconhece a posição de vulnerabilidade de certos grupos, dedicando-lhes normas especiais para tutelá-los na exata medida de suas fraquezas.

Isso pode ser facilmente percebido nas normas de direito do trabalho e do direito do consumidor. E deve balizar também os aspectos do direito digital, onde se faz necessário o cuidado do legislador na percepção da vulnerabilidade do indivíduo frente ao mercado, que usa as informações como ativos de grande valor, e também em relação a indivíduos mal intencionados, que atuam à margem ética e legal em nome de interesses escusos diversos.

Conforme trazido por Sarlet e Ferreira Neto *apud* Facchini Neto e Demoliner (2019), há na sociedade atual:

> um absoluto descontrole no manuseio, na armazenagem e no acesso dos dados pessoais que estão pulverizados na Internet, o que acaba por fragmentar o nosso senso de privacidade e de personalidade, tornando-nos vulneráveis em relação ao que os demais pensam e falam sobre nossa esfera individual e sobre o nosso passado.

Diante da assimetria nas relações entre os titulares e os controladores de dados e da vulnerabilidade daqueles, cunhou-se a expressão “consumidor de vidro”, de acordo com Lace *apud* Cruvinel (2019). Segundo a autora, a vulnerabilidade do indivíduo nesse tipo de relação se dá em diferentes dimensões: informacional (dificuldade do titular dos dados em identificar a real finalidade do tratamento de dados), técnica (limitação intelectiva para decidir sobre o tratamento de seus dados) e econômica (hipossuficiência de recursos em relação às empresas).

Há também o desconhecimento generalizado da amplitude do uso de dados pelas organizações a partir da rede mundial de computadores. Grande parte dos indivíduos ainda ignora o fato de que ao navegar na internet, seja para conferir as notícias locais, seja para buscar informações acerca de um determinado assunto ou

para comprar determinado item em um site qualquer, existe um mecanismo tecnológico por trás que acompanha toda a navegação, monitora os passos e cliques virtuais, bem como o tempo usado em cada página visitada (PALHARES, 2020).

Para além disso, adentrando ao viés subjetivo da conduta humana, destacam Facchini Neto e Demoliner (2019) que a maior parte dos indivíduos:

> Não tem paciência (até porque desconhece os riscos) para ler as "políticas de privacidade". Simplesmente 'clica' no botão da 'aceitação' porque de outra forma não conseguiria "criar sua conta" e/ou "perfil" nas redes sociais. E tudo o que mais quer é "participar desse mundo virtual", onde a imagem vale mais do que a realidade. Tudo é urgente, tudo é feito em instantes e ler os "termos de aceitação" – através do qual vende (ou melhor, doa) "sua alma", abrindo mão da sua valiosa privacidade – pode tomar muito tempo e energia, que seriam mais bem utilizados, sob a ânsia do momento, se destinados para postar a próxima selfie ou compartilhar o próximo 'meme'.

Um exemplo de repercussão mundial que demonstra a vulnerabilidade do titular de dados e os riscos atrelados ao uso de informações obtidas por meio de redes sociais foi o caso envolvendo as empresas Cambridge Analytica e Facebook em 2015 que, porém, só veio à tona em meados de 2018.

No episódio, dados pessoais de mais de oitenta e sete milhões de usuários da rede social foram usados, sem o prévio consentimento dos titulares, por analistas de dados da Cambridge Analytica para construir perfis e modelos de comportamento a fim de influenciar eleitores e direcionar a campanha de determinado candidato à presidência dos Estados Unidos, nas eleições que ocorreram no ano de 2016 (LAPAIRE, 2018).

Dentre esses milhões de usuários que tiveram expostos seus dados, cerca de quatrocentos mil eram brasileiros, o que fez com que o Departamento de Proteção e Defesa do Consumidor – DPDC multasse o Facebook em mais de seis milhões de reais.[8]

Nos Estados Unidos, a empresa fechou acordo com a *Federal Trade Commission – FTC* para encerrar as investigações do caso sob a condição de pagar

[8] EL PAÍS. Disponível em: https://brasil.elpais.com/tecnologia/2019-12-30/brasil-multa-facebook-em-66-milhoes-de-reais-pelo-vazamento-de-dados-no-caso-cambridge-analytica.html. Acessado em: 1º de outubro de 2020.

uma multa equivalente a US$ 5 bilhões de dólares, contabilizando a maior penalidade já aplicada na história da *FTC*.[9]

A consequência desse tipo de uso indevido dos dados das pessoas, notadamente quanto à finalidade de modificar resultados eleitorais, de acordo com a visão de Martins e Tateoki (2019):

> obscurece a transparência em torno da pessoa do candidato, notadamente suas ideias e propostas. Com efeito, a transparência em torno do candidato é pedra angular do sistema, visto que é ela que permite ao eleitor fazer sua escolha de forma livre e, sobretudo, consciente. Assim, em um cenário de manipulação do eleitor por propaganda eleitoral direcionada a grupos ou perfis pré-selecionados, a qualidade do voto, como expressão do exercício da cidadania, é severamente prejudicada.

Tudo o que até aqui foi trazido são elementos diversos que acentuam mais ainda a distância entre o titular dos dados e o real controle pelas decisões do que deve ser feito em relação às suas informações. Não é a pretensão deste trabalho, no entanto, explorar profundamente cada um desses vieses, mas concentrar esforços para compreender o papel da LGPD na concretização da segurança jurídica necessária à harmonia das relações que envolvam a proteção de dados entre o indivíduo e a sociedade.

Referenciando a perspectiva trazida por Blum (2018), nota-se que o respeito à privacidade do indivíduo tem se distanciado da perspectiva restrita da ótica do segredo e se aproximado cada vez mais da ideia de controle dos dados pelo seu titular:

> A preocupação que antes era voltada para a tutela do direito a ser deixado só e do direito ao recato, agora está menos voltada à privacidade de certos dados (porque as pessoas sabem que há um certo grau de publicidade) e mais focada no uso destes dados, no fato de o indivíduo poder controlar a forma de coleta, organização e uso das informações.

Retomando a análise normativa: se, por um lado, a ausência de dispositivo constitucional a respeito da proteção de dados no ambiente digital favorece a democratização da informação, conforme observado no julgamento da Arguição de

---

[9] MUNDO CONECTADO. Disponível em: https://mundoconectado.com.br/noticias/v/9883/facebook-vai-pagar-us5-bilhoes-para-encerrar-investigacao-sobre-o-caso-cambridge-analytica.

Descumprimento de Preceito Fundamental nº 130 pelo Supremo Tribunal Federal, que derrubou a Lei de Imprensa em 2009:

> Silenciando a Constituição quanto ao regime da internet (rede mundial de computadores), não há como se lhe recusar a qualificação de território virtual livremente veiculador de ideias e opiniões, debates, notícias e tudo o mais que signifique **plenitude de comunicação**. (STF - ADPF: 130 DF, Relator: Min. CARLOS BRITTO, Data de Julgamento: 30/04/2009, Tribunal Pleno, Data de Publicação: DJe-208 DIVULG 05-11-2009 PUBLIC 06-11-2009 EMENT VOL-02381-01 PP-00001) (grifo nosso)

Por outro lado, conforme Denardis *apud* Borges (2019):

> ao mesmo tempo em que é possível assegurar tais direitos, **a internet também apresenta-se como solo fértil para a violação de valores como proteção da propriedade intelectual (...) ciberataques e ameaças à segurança dos próprios**. Diante disso, a capacidade de proteger o ciberespaço passa a ser requisito para que qualquer país possa proteger direitos, executar operações de comércio internacional e desenvolver funções públicas essenciais. (grifo nosso)

Consolidado o entendimento de que os dados pessoais devem ser protegidos como extensão natural do direito à privacidade, e, considerando o expressivo aumento do volume da troca de informações, da quantidade de dados publicados especialmente nas redes sociais e do interesse econômico na obtenção desses dados pelas empresas, fez-se necessário o estabelecimento de alguns meios de mitigação da vulnerabilidade e dos riscos para os indivíduos que são titulares dessas informações.

Um desses mecanismos, previsto na LGPD, é a anonimização de dados, que consiste em um processo onde o vínculo entre o dado e seu respectivo titular é quebrado, de maneira que não seja possível realizar a associação entre um e outro. E isso pode ser feito basicamente por meio de quatro espécies possíveis: supressão, generalização, randomização e pseudonimização (BIONI, 2020).

Foge ao escopo deste trabalho explorar as formas de anonimização de dados, bastando para o objetivo proposto apenas explicar que a pseudonimização, a exemplo do GDPR, também é trazida pela LGPD como uma forma de mascarar os dados, onde o controlador teria a capacidade de recombinar esse conjunto de dados e novamente identificar o indivíduo. No entanto, conforme versa o §4º do art. 13 da Lei nº 13.709/2018, essa informação adicional capaz de reunir os elementos e montar o

“quebra-cabeças” entre o dado e seu titular deverá ser mantida pelo controlador em ambiente e seguro, onde somente este teria acesso.

Para compreender melhor essas estruturas, é relevante mencionar Machado e Doneda (2018) que argumentam que, do ponto de vista da técnica legislativa e da política de proteção de dados, há duas principais abordagens para a definição de dado pessoal: reducionista e expansionista. Na primeira abordagem, o dado pessoal é tido como:

> a representação de fatos sobre pessoa identificada, isto é, representação referente a alguém que se conhece e individualiza em meio a certo grupo ou coletividade. O processo de identificação aí operado é possível a partir de elementos informativos chamados identificadores.

Já o caráter expansionista considera dado pessoal qualquer informação relativa à pessoa identificável, ou seja, um dado que tenha potencial de conduzir à descoberta da identidade do indivíduo também deve ser considerado pessoal (MACHADO; DONEDA, 2018).

O legislador adotou o critério expansionista na edição da LGPD, o que representa na prática uma maior segurança para os titulares de dados, conforme se depreende do inciso I do art. 5º da Lei nº 13.709/2018:

> I - dado pessoal: informação relacionada a pessoa natural **identificada ou identificável** (grifo nosso)

Os dados acima evidenciam a persistência de uma conduta inadequada de algumas empresas e o engajamento da sociedade ao buscar a proteção legal no tratamento de seus dados, mas imediatamente também trazem uma reflexão necessária à realidade brasileira: uma vez que o país conta com quase oitenta milhões de processos judiciais em tramitação[10], quais serão as consequências das lacunas e conceitos indeterminados presentes na LGPD para o judiciário brasileiro?

[10] Relatório Justiça em Números 2019 – Conselho Nacional de Justiça.

4. JUDICIALIZAÇÃO DA PROTEÇÃO DE DADOS PESSOAIS

É fato que as demandas sociais possuem uma dinâmica mais célere do que a resposta legal e judicial, que costuma vir a posteriori. No caso específico de proteção de dados, por se tratar de temática altamente entrelaçada com recursos tecnológicos cada vez mais avançados, a ausência de parâmetros legais robustos e compatíveis com a complexidade envolvida traz inúmeros impactos, não só para os indivíduos como para a própria justiça.

No primeiro semestre de 2019, a Comissão Europeia divulgou um documento com os resultados do primeiro ano de vigência do GDPR. De acordo com análise feita por Reis (2019), só nesse período foram realizadas quase cento e cinquenta mil denúncias de cidadãos junto às autoridades europeias em relação à violação no uso de seus dados pessoais. Os assuntos mais recorrentes foram os relacionados a ações de *marketing* abusivas, ao envio de e-mails promocionais e a circuitos de vídeo de vigilância.

No contexto europeu, de acordo com Zanatta (2020), faz parte da cultura utilizar-se em larga escala da esfera administrativa para a apreciação de demandas relativas aos interesses difusos na proteção de dados, com fundamento no art. 80 do GDPR:

> O titular dos dados tem o direito de mandatar um organismo, organização ou associação sem fins lucrativos, que esteja devidamente constituído ao abrigo do direito de um Estado-Membro, cujos objetivos estatutários sejam do interesse público e cuja atividade abranja a defesa dos direitos e liberdades do titular dos dados no que respeita à proteção dos seus dados pessoais, para, em seu nome, apresentar reclamação, exercer os direitos previstos nos artigos 77.o, 78.o e 79.o, e exercer o direito de receber uma indemnização referido no artigo 82.o, se tal estiver previsto no direito do Estado-Membro.

No Brasil, antes mesmo da sanção e publicação da LGPD, o Ministério Público já vinha realizando ao longo dos últimos anos o ajuizamento de ações civis públicas para a defesa da proteção de dados e da privacidade, no âmbito dos direitos difusos e coletivos.

Zanatta (2020) destaca, ainda, em seu artigo alguns exemplos de grande repercussão:

Tabela 2 – Exemplos de casos que foram judicializados no Brasil em temas de proteção de dados

Ano	Autor(es)	Réu	Fundamentação	Danos morais coletivos	Resultado
2016	MPF/PI	Google	Coleta de dados (Gmail) sem consentimento informado, violando Marco Civil da Internet e CDC	R$ 1.000.000,00 (um milhão de reais)	Improcedente (1ª Instância)
2017	MP/RJ e Defensoria Pública	Fetranspor	Cessão ilegal (sem licitação) do serviço público de Bilhete Único a empresa privada. Comercialização indevida de dados pessoais dos usuários de transporte público	R$ 260.000.000,00 (duzentos e sessenta milhões de reais)	Liminar concedida ao autor
2018	MPDFT	Banco Inter	Incidente de segurança e exposição ilegal de informações financeiras de clientes	R$ 10.000.000,00 (dez milhões de reais)	ACP encerrada após assinatura de Termo de Ajuste de Conduta e repasse de recursos ao Fundo de Direitos Difusos

2018	Instituto Brasileiro de Defesa do Consumidor	Via-Quatro (concessionária da Linha Amarela – Metrô/SP)	Tratamento de dados biométricos sem informação adequada e sem consentimento	R$ 100.000.000,00 (cem milhões de reais)	Liminar concedida, com efeito suspensivo

Fonte: ZANATTA, Rafael A. F. Tutela coletiva e coletivização da proteção de dados pessoais. Temas atuais de proteção de dados: p. 345 a 373. São Paulo: Thomson Reuters Brasil, 2020.

Em verdade, para além das ações interpostas pelo Ministério Público, já se nota um significativo número de demandas judiciais envolvendo o tema, nas quais as cortes são chamadas a decidir sobre a proteção de dados.

Observa-se, no Brasil, uma tendência em se manter na tutela da proteção de dados e privacidade o papel de protagonismo exercido pelo poder judiciário na resolução dos conflitos referentes à violação desses direitos, o que possivelmente deverá representar um aumento no número de casos a serem julgados pelos tribunais.

O afunilamento dos litígios para o judiciário se dá também pela morosidade na estruturação da Autoridade Nacional de Proteção de Dados – ANPD, que teve sua regulamentação publicada somente no final de agosto de 2020, por meio do Decreto nº 10.474:

> Art. 1º Ficam aprovados a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados - ANPD, na forma dos Anexos I e II.

Ainda assim, a ANPD não poderá desempenhar plenamente suas atribuições, tendo em vista a previsão normativa de possibilidade de aplicação de penalidades e sanções decorrentes do descumprimento da LGPD apenas a partir de agosto de 2021.

Já é possível observar a utilização do disposto na LGPD como fundamentação jurídica utilizada pelas partes. Um exemplo recente, e o primeiro que teve destaque nos meios de comunicação, foi a ação preparatória de Ação Civil Pública ajuizada pelo MPDFT em face da empresa Infortexto LTDA. em virtude da oferta de venda indevida de dados de milhares de usuários, de todas as unidades federativas, com possibilidade de diferentes formas de segmentação (ex.: categorizados por profissão).

Na peça, o *parquet* referenciou os dispositivos da Constituição que tratam do direito à privacidade, o Código de Defesa do Consumidor, o Marco Civil da Internet e a LGPD, em especial no trecho reproduzido a seguir:

> Sob a ótica da Lei Geral de Proteção de Dados Pessoais – LGPD fica claro que a empresa ré faz tratamento de dados pessoais de forma totalmente ilegal/irregular gerando prejuízos aos titulares dos dados pessoais.

Sob a mesma ótica, ajuizou outra ação civil pública o MPDFT, com pedido de tutela de urgência, em face de fornecedor flagrado comercializando bancos de dados pessoais no site de comércio eletrônico Mercado Livre. [11]

Na decisão interlocutória, pontuou o magistrado, decidindo favoravelmente ao *parquet*, após referenciar o art. 44 da LGPD:

> Tal prática, portanto, está em patente confronto com o princípio constitucional da inviolabilidade do sigilo de dados, insculpido no artigo 5º, XII, da Constituição Federal e o fundamento do respeito à privacidade, previsto no artigo 2º, I, da Lei Geral de Proteção de Dados Pessoais, sem prejuízo de outros Diplomas Legais aplicáveis à espécie, a demonstrar a probabilidade do direito invocado. O perigo de dano, por sua vez, dessai da **persistente violação à privacidade dos titulares dos dados, a tornar impositiva a suspensão do comércio erigido pelo réu** [...] (grifo nosso).

Para o juízo, não havia indícios de consentimento dos titulares de dados com a comercialização de suas informações, no caso em questão.

[11] Portal Migalhas. LGPD: MercadoLivre deve suspender anúncio sobre venda de dados pessoais. Disponível em: https://migalhas.uol.com.br/quentes/335049/lgpd--mercadolivre-deve-suspender-anuncio-sobre-venda-de-dados-pessoais. Acessado em: 19 de outubro de 2020.

5. *OPEN BANKING*: UM MODELO BASEADO EM *API*

O sistema financeiro não foge à tendência do aumento exponencial de dados capturados dos usuários e do tratamento desses dados para a realização de análises comportamentais e definição de perfis de consumo com o objetivo de oferecer produtos e serviços.

Dada a expressiva quantidade de pessoas que atualmente transacionam com as instituições financeiras por meio eletrônico, a coleta dessas informações permitiu a geração de bancos de dados consideravelmente robustos (THOMAZ, 2020).

Em artigo publicado em 2016, a *Euro Banking Association* discorreu sobre o *open banking*, destacando-o como uma ideia nova e em constante evolução, mas definiu o conceito em linhas gerais como sendo a padronização da forma como os bancos compartilham seus próprios dados e como permitem ao cliente mais opções de compartilhamento desses dados para uso em aplicativos de terceiros de forma segura.

O *open banking* representa, na visão da entidade, a ponte que une dois mundos, possibilitando que os clientes usem seu serviço bancário no contexto de outros serviços, combinando funcionalidades inovadoras alcançadas por meio de infraestrutura de aplicações.

Para compreender a proposta do *open banking* é importante entender que este é um modelo de negócio fundamentado em tecnologia e ciência de dados, que propõe a utilização de *APIs (Application Programming Interfaces)* para a integração de *softwares* e compartilhamento de informações entre diferentes instituições.

As *APIs* são conjuntos de definições e protocolos de desenvolvimento que permitem que a comunicação entre sistemas com diferentes estruturas de implementação seja fluida e facilitada, simplificando o processo e gerando economia de tempo e investimento financeiro. Em síntese, a *API* é uma interface para um componente de software que pode ser chamado à distância através de uma comunicação de rede, usando tecnologias baseadas em padrões. Nada mais é do que uma forma de comunicação entre sistemas, permitindo a troca de informações (RODRIGUES, 2017).

Ainda, de acordo com Jensen (2015), uma *API* moderna representa um conjunto de recursos que interessam para um público independente de qualquer

software específico, desenhados sob a ótica do consumidor do produto, não obstante incluírem uma interface definida.

Em outras palavras, a *API* pode ser vista como uma espécie de contrato, em que a documentação do sistema representa um acordo entre as partes interessadas. Quando uma dessas partes envia uma solicitação remota estruturada de uma forma específica, os protocolos determinam como o software da outra parte responderá.

Esse tipo de estrutura é caracterizado pela flexibilidade na gestão de uso, design, além de convergir com o processo de inovação.

O nível de abertura da *API* está diretamente relacionado ao seu potencial alcance e a sofisticação de suas funcionalidades. A proposta de *open banking* se baseia na troca de informações por *APIs* abertas. Ou seja, uma *API* que permite a possibilidade de acesso por terceiros, de fora da organização.

Especialmente na indústria financeira mostra-se necessário um cuidado maior no que diz respeito à segurança no compartilhamento de dados por meio de *APIs*. De todo modo esse nicho de mercado já é hoje altamente regulado, o que pode facilitar e até mesmo servir como exemplo para as demais áreas e instituições.

5.1. *OPEN BANKING* NO BRASIL

O *open banking* no Brasil é uma iniciativa que faz parte do pilar de Competitividade do planejamento estratégico do Banco Central do Brasil – Bacen (AgendaBC#).

Os primeiros passos foram dados por meio da divulgação do Comunicado nº 33.455/2019, que estabeleceu as diretrizes para a proposta de regulamentação do assunto em território nacional. O escopo da referida publicação definiu o objetivo de implementação, a justificativa estratégica, o conceito de *open banking* para o Bacen, o público-alvo do modelo, os tipos de dados abrangidos, a estratégia de regulação e o processo de implementação, além da previsão temporal.

De acordo com a Autarquia, o destaque mundial do tema somado à publicação da LGPD despertou a necessidade de manifestação da instituição no sentido de regulamentar o *open banking* de forma a assegurar o alcance de seus objetivos específicos.

Os requisitos estabelecidos pelo Bacen no referido Comunicado indicaram o compartilhamento das seguintes informações e serviços:

> I - produtos e serviços oferecidos pelas instituições participantes (localização de pontos de atendimento, características de produtos, termos e condições contratuais e custos financeiros, entre outros);
> II - dados cadastrais dos clientes (nome, número de inscrição no Cadastro de Pessoas Físicas - CPF, filiação, endereço, entre outros);
> III - dados transacionais dos clientes (dados relativos a contas de depósito, a operações de crédito, a demais produtos e serviços contratados pelos clientes, entre outros);
> IV - serviços de pagamento (inicialização de pagamento, transferências de fundos, pagamentos de produtos e serviços, entre outros).

Os resultados esperados com o compartilhamento de dados e informações entre as instituições financeiras são, para o cidadão, benefícios como o acesso a outros tipos de serviços financeiros, oferta de serviços personalizados a sua real necessidade e a inclusão financeira.

Por outro lado, para as instituições financeiras há o aumento da competitividade, democratizando a participação de novos *players* no mercado (*fintechs*) e o fomento à inovação, uma vez que há grande contribuição da tecnologia no compartilhamento de dados.

O Comunicado resultou no Edital de Consulta Pública de nº 73, que trouxe todo o detalhamento dos requisitos para o compartilhamento de dados e para a participação dos atores no processo de *open banking* no Brasil e acolheu sugestões e comentários das instituições financeiras e demais instituições autorizadas até janeiro de 2020.

A Autarquia dedicou seção específica para tratar do consentimento do titular dos dados, onde destacou uma série de requisitos para ratificar a legitimidade da obtenção deste por meio das instituições que deverão fornecer o serviço, entre eles: linguagem clara e objetiva, finalidade determinada e prazo de validade limitado a 12 (doze) meses.

Além disso, o mesmo capítulo trouxe vedações com o objetivo de tornar mais transparente o consentimento: este não pode ser obtido por meio de contrato de adesão, formulário preenchido previamente ou de forma presumida. Em outras palavras, o consentimento deve ser explícito.

O Edital previu, ainda, uma espécie de prestação de contas constante aos clientes, pois as instituições participantes do modelo de negócio deverão fornecer informações sobre a identificação de outras instituições participantes e que tenham relação com o consentimento, sobre os dados e serviços que serão compartilhados, o período de validade, a data de requisição e a finalidade do consentimento, além de assegurar a revogação a qualquer tempo pelo cliente, com a facilitação deste procedimento, devendo estar disponível ao menos no mesmo canal onde foi consentido o uso das informações em primeiro lugar.

Seguindo na linha do tempo do *open banking* brasileiro, em 04 de maio de 2020, o Banco Central, junto com o Conselho Monetário Nacional, publicou a Resolução Conjunta nº 1 e a Circular nº 4.015, regulamentando e disciplinando a implementação do novo modelo de negócios em território nacional.

A Resolução traz em seu conteúdo cinquenta e cinco artigos que preveem regras para o compartilhamento de dados no âmbito do território nacional, contemplando regras que preveem o quê de essencial deve conter nas plataformas digitais das instituições participantes, a fim de facilitar para o consumidor a contratação do serviço na instituição que melhor atenda suas expectativas e necessidades. Trouxe também o detalhamento dos dados pessoais e operacionais que poderão ser objeto de compartilhamento entre as instituições e a expectativa da autarquia é o aumento da eficiência, da competitividade e da transparência no sistema financeiro.

Todo o processo foi previsto para ser implementado em quatro fases, sendo a primeira com a data limite de 30 de novembro de 2020.

De acordo com a publicação feita pelo Bacen, o consumidor é o centro do projeto e o modelo é voltado para o princípio de que aquele é proprietário de seus dados pessoais e que cabe a ele a decisão sobre o tratamento desses dados. A proposta do *open banking*, na visão da autarquia, seria facilitar esse processo de escolha, na busca do consumidor por produtos e serviços financeiros mais adequados à sua realidade e expectativa.

Cabe aqui frisar que as instituições financeiras do Brasil estão sujeitas à Lei Complementar nº 105/2001 (Lei do Sigilo Bancário) e, de acordo com essa norma, as informações referentes a operações ativas e passivas, serviços prestados e grande parte dos dados pessoais dos clientes devem ser especialmente protegidos contra

quaisquer acessos, comercializações ou publicizações indevidas, salvo as exceções expressamente previstas na referida Lei Complementar.

Uma das exceções previstas dentro da própria Lei nº 105/2001 é a possibilidade de o titular dos dados permitir que seus dados sejam compartilhados com terceiros desde que o procedimento seja realizado mediante seu consentimento:

> § 3o Não constitui violação do dever de sigilo:
> I – a troca de informações entre instituições financeiras, para fins cadastrais, inclusive por intermédio de centrais de risco, observadas as normas baixadas pelo Conselho Monetário Nacional e pelo Banco Central do Brasil;
> II - o fornecimento de informações constantes de cadastro de emitentes de cheques sem provisão de fundos e de devedores inadimplentes, a entidades de proteção ao crédito, observadas as normas baixadas pelo Conselho Monetário Nacional e pelo Banco Central do Brasil;
> III – o fornecimento das informações de que trata o § 2o do art. 11 da Lei no 9.311, de 24 de outubro de 1996;
> IV – a comunicação, às autoridades competentes, da prática de ilícitos penais ou administrativos, abrangendo o fornecimento de informações sobre operações que envolvam recursos provenientes de qualquer prática criminosa;
> V – a revelação de informações sigilosas **com o consentimento expresso dos interessados**;
> VI – a prestação de informações nos termos e condições estabelecidos nos artigos 2o, 3o, 4o, 5o, 6o, 7o e 9 desta Lei Complementar.
> VII - o fornecimento de dados financeiros e de pagamentos, relativos a operações de crédito e obrigações de pagamento adimplidas ou em andamento de pessoas naturais ou jurídicas, a gestores de bancos de dados, para formação de histórico de crédito, nos termos de lei específica. (grifo nosso)

No mesmo sentido trouxe a Resolução do CMN nº 4.292/2013, ao dispor sobre a regulação da portabilidade de operações de crédito:

> Art. 5º Por **solicitação formal e específica do devedor**, a instituição proponente deve encaminhar requisição de portabilidade à instituição credora original, contendo, no mínimo, as seguintes informações [...].

Conforme observado por Thomaz (2020):

> Assim, diferentemente do que dispõe a LGPD, autorizando o tratamento (e, portanto, o compartilhamento) de dados pessoais em outras bases legais que o consentimento do titular, a portabilidade ou compartilhamento de dados dentro do sistema open banking **dependerá sempre do consentimento do titular de dados**. (grifo nosso)

Nota-se, de pronto, um papel de destaque do consentimento enquanto base legal fundamental para o modelo de negócio do *open banking*, que vai ao encontro da intenção do legislador ao se inspirar no regulamento europeu para pensar a LGPD.

O destaque dado a essa base legal no normativo dá ao indivíduo um papel de protagonismo, "incentivando um comportamento ativo da parte do titular e responsável por parte do agente que realizar o tratamento dos dados" (TEPEDINO;TEFFÉ, 2019).

5.2. PIX E SPI: SISTEMA DE PAGAMENTO DO BANCO CENTRAL

Embora não seja o tema central do presente trabalho, não é demais mencionar que, na esteira das ações da Agenda BC#, o Banco Central publicou em fevereiro de 2020 a Carta Circular nº 4.006 dispondo sobre o arranjo de pagamentos instantâneos (Pix) e o sistema de pagamentos instantâneos (SPI).

O Pix é um mecanismo de pagamento em tempo real, que foi idealizado em 2018 pelo grupo de trabalho da Autarquia, que resolveu iniciar os trabalhos relativos à modernização e abertura do sistema financeiro. Já o SPI é a plataforma tecnológica que suportará as transações realizadas pelas instituições por meio do Pix.[12]

A diferença essencial entre o Pix e os meios de pagamento tradicionais (ex.: DOC, TED) consiste na disponibilidade (o Pix deverá operar 24 horas por dia, todos os dias) e na possibilidade de transacionar usando dados diversos, para além de agência e conta bancária (ex.: CPF ou número de telefone).[13]

Assim como a proposta do *open banking*, o Pix funciona baseado em *APIs*, por meio das quais as instituições financeiras se comunicam com a base do Banco Central.

No estabelecimento das regras de funcionamento do novo meio de pagamento, restou demonstrada a preocupação da autarquia em estimular a observância de requisitos mínimos de segurança e de proteção aos dados. Um

[12] Banco Central do Brasil. Sistema de Pagamentos Instantâneos (SPI). Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/sistemapagamentosinstantaneos. Acessado em: 01 de outubro de 2020.
[13] Banco Central do Brasil. Pix. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/pagamentosinstantaneos. Acessado em: 29 de setembro de 2020.

exemplo pode ser percebido no § 5º do art. 3º da Resolução nº 1, de 12 de agosto de 2020, que instituiu o Pix e aprovou seu regulamento, ao prever os seguintes requisitos para as instituições aderentes à proposta, mas não integrantes do Sistema de Pagamentos Brasileiro:

> § 5º Enquanto não vierem a preencher os demais critérios previstos na regulamentação em vigor para serem autorizadas a funcionar pelo Banco Central do Brasil, aplicam-se às instituições de pagamento que integrarem o SPB exclusivamente em virtude de sua adesão ao Pix, na forma do § 4º:
> I - regulação mínima, abrangendo normas atinentes a:
> a) estrutura de gerenciamento de riscos operacional e de liquidez, conforme disposto na Circular nº 3.681, de 4 de novembro de 2013;
> b) **política de segurança cibernética, plano de ação e de resposta a incidentes**, contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, conforme disposto na Circular nº 3.909, de 16 de agosto de 2018 [...] (grifo nosso)

Muito se fala sobre a democratização que se busca alcançar com o lançamento do Pix, iniciado em outubro de 2020 com o cadastramento de chaves para os usuários que assim desejarem, uma vez que tem como premissa facilitar a movimentação de recursos entre diferentes instituições, por meio de diferentes formas de identificação.

Nas palavras de Silva e Cruz (2020), com a regulamentação do Pix, o Bacen entende que o novo sistema:

> [...] atenderá toda a população brasileira, porém não se pode ignorar a realidade de que existe um número significativo de pessoas que não têm acesso a esse tipo de tecnologia, bem como usuários que têm preferência e familiaridade com a forma de pagamento mais tradicional e antiga, reconhecida como o pagamento em espécie.

Impulsionado pelo cenário de pandemia, que fez com que as relações sociais e comerciais acelerassem rumo ao digital, é notório o esforço da Autarquia no sentido de ampliar o acesso de pessoas antes não bancarizadas às soluções financeiras rastreáveis.

Nesse sentido, é importante compreender, conforme Silva e Cruz (2020):

> [...] que tal mecanismo não só traz vantagens inovadoras e facilitadores para os consumidores, mas também atende aos interesses do Estado, o que significa dizer que **a implantação do ecossistema de pagamento instantâneo viabilizará, também, a**

> **troca informacional dos usuários através da verificação de informações pessoais** disponibilizadas pelo pagador ao recebedor (CPF/CNPJ, CELULAR, E-MAIL) [...] facilitando a fiscalização do Estado nas investigações de usuários que, possivelmente, estejam cometendo crimes contra o Sistema Financeiro Nacional, como por exemplo indivíduos que estejam praticando os crimes de sonegação fiscal ou lavagem de dinheiro.

Em uma primeira análise, considerando o ambiente altamente regulado que compõe o sistema financeiro, não se visualiza grandes dificuldades de adequação e de atendimento ao previsto na LGPD, uma vez que as instituições que fazem parte do Sistema Brasileiro de Pagamentos já estão sob a égide da Lei do Sigilo Bancário e, portanto, familiarizadas com os riscos de um eventual vazamento de dados.

No entanto, e aqui pode-se compreender melhor a inclusão do referido tópico no presente trabalho, já é possível observar na prática exemplos da não observância do disposto na LGPD. Reclamações recentes foram publicadas por usuários nas redes sociais, em especial no Twitter, sob a alegação de que algumas instituições haviam cadastrado chaves Pix sem o consentimento dos titulares de dados[14].

O Bacen se manifestou no sentido de que já está realizando a fiscalização referente ao novo meio de pagamento e que eventuais irregularidades, se comprovadas, serão punidas na forma da regulamentação aprovada.

Ressalte-se que a consequência do cadastramento em massa de chaves Pix pelas instituições, sem o devido consentimento dos usuários, além de configurar tratamento não permitido e abusivo de seus dados, amplia o risco de impossibilidade do cadastro consentido posterior pelo próprio usuário de suas chaves Pix nas instituições em que desejar, uma vez que, de acordo com os normativos, é permitido ao usuário cadastrar até cinco chaves para uso do sistema de pagamentos. Esgotado esse limite, o usuário deve solicitar a portabilidade caso queira vincular sua chave a outra instituição.[15]

Tal conduta vai de encontro aos princípios da LGPD, especialmente no que diz respeito à boa-fé, à finalidade, à transparência e à prevenção.

---

[14] SOUZA. Ramon de. Nubank e Mercado Pago são acusados de cadastrar chaves Pix sem autorização. Disponível em: https://canaltech.com.br/mercado/nubank-e-mercado-pago-sao-acusados-de-cadastrar-chaves-pix-sem-autorizacao-173188/. Acessado em 17 de outubro de 2020.

[15] Banco Central do Brasil. Perguntas e Respostas. Pagamento Instantâneo (Pix). Disponível em: https://www.bcb.gov.br/acessoinformacao/perguntasfrequentes-respostas/faq_pixpagtoinstantaneo. Acessado em: 20 de setembro de 2020.

Mais uma vez fica evidente o impacto da ausência do funcionamento por completo da Autoridade Nacional de Proteção de Dados, que atuaria em conjunto com o Bacen para garantir a proteção aos dados dos usuários nesse contexto e o risco de aumento do gargalo da judicialização.

6. CONSIDERAÇÕES FINAIS

Superadas as referências teóricas e exemplos práticos abordados, retoma-se ao ponto inicial: o presente trabalho trata de uma temática bastante nova, não só no âmbito do Direito, mas da sociedade, e não se propõe a encerrar os debates sobre a conexão entre os dois assuntos (*open banking* e LGPD), bem como sobre as consequências jurídicas dessa relação.

Nas palavras de Tepedino e Teffé (2019), "ao trazer a tutela focada na pessoa humana e no livre desenvolvimento de sua personalidade, a LGPD assegura o exercício da liberdade existencial e a igualdade material" frente à importância das informações para a tomada de decisão dos indivíduos e de seu relacionamento com a sociedade.

Entre as bases legais da LGPD, sem dúvidas merece grande atenção o consentimento como fundamento e elemento essencial para que o *open banking* consiga trazer de fato consequências positivas para os usuários e a democratização esperada pelo movimento de abertura no sistema financeiro.

No entanto, é salutar a atuação conjunta do Bacen e da ANPD a fim de garantir que essa base legal esteja sendo aplicada e seguida corretamente pelas instituições. Que o usuário seja respeitado em relação às suas escolhas e que, especialmente, essas escolhas sejam livres e claras, e não dotadas de obscuridade e tecnicismos que interfiram na correta tomada de decisão dos indivíduos.

Ressalte-se um exemplo de consequência para os usuários nesse contexto bancário/financeiro: o risco de impossibilidade de cadastramento consentido de suas chaves Pix nas instituições em que desejar, uma vez que, de acordo com os normativos, é permitido ao usuário cadastrar até cinco chaves para uso do sistema de pagamentos. Esgotado esse limite, o usuário deve solicitar a portabilidade caso queira vincular sua chave a outra instituição.[16]

Por outro lado, é importante destacar que a base legal do consentimento amplia substancialmente o risco para os operadores e controladores de dados, visto

[16] Banco Central do Brasil. Perguntas e Respostas. Pagamento Instantâneo (Pix). Disponível em: https://www.bcb.gov.br/acessoinformacao/perguntasfrequentes-respostas/faq_pixpagtoinstantaneo. Acessado em: 20 de setembro de 2020.

que este pode ser revogado a qualquer momento pelo titular de dados. Portanto, faz-se necessária uma análise minuciosa, dentro do contexto do *open banking*, que é o foco deste trabalho, a fim de identificar eventuais possibilidades de se trabalhar, como complementação ao consentimento, com a base legal de execução de contrato. Especialmente em se considerando o uso de *API*s como subsídios tecnológicos para suportar a solução, há total convergência no uso dessa base legal, uma vez que toda a documentação e requisitos envolvidos no uso dessa tecnologia funcionam sob a mesma lógica contratual.

Não obstante se tratar de um conceito de certa forma não muito bem definido pela LGPD, o legítimo interesse também é uma base que tende a ser usada amplamente pelos agentes de tratamento para buscar maior solidez nas relações com os titulares de dados.

A própria proteção ao crédito é uma base legal muito forte a ser justificada como fundamento para o tratamento de dados pelas instituições financeiras. Não se pode esquecer que a segurança jurídica esperada nessa relação instituição financeira x usuário dos serviços deve ser buscada e garantida para ambos os atores. E usar somente a base legal do consentimento poderia trazer consequências negativas para os operadores e controladores de dados, visto que o consentimento é apenas o ponto de partida para o início do tratamento de dados e que diversos contratos podem surgir a partir dessa concessão.

Por fim, pode-se perceber, pelo exposto até o presente momento, que a proteção de dados é uma temática que demanda esforços contínuos do legislador e do poder judiciário a fim de acompanhar a dinamicidade própria da tecnologia, que consome o grande volume de informações que suportam os negócios da era digital. Essa atuação deve estar sempre voltada a proteger o indivíduo, pois é a parte mais frágil das relações que envolvem seus dados. E a Lei Geral de Proteção de Dados deve ser apenas o início desse movimento.

REFERÊNCIAS

ALMEIDA, Ana Rita Bibá Gomes de. **A LGPD está em vigor. E agora?**. Disponível em: https://www.nextlawacademy.com.br/blog/a-lgpd-esta-em-vigor-e-agora. Acessado em: 03 de outubro de 2020.

Banco Central do Brasil. **Circular nº 4.015 de 4 de maio de 2020**. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Circular&numero=4015.

_____. **Comunicado nº 33.455 de 24 de abril de 2019**. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=33455.

_____. **Conselho Monetário Nacional e Banco Central regulamentam o *Open banking* no país**. Disponível em: https://www.bcb.gov.br/detalhenoticia/448/noticia.

_____. **Pix**. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/pagamentosinstantaneos. Acessado em: 08 de outubro de 2020.

_____. **Resolução conjunta nº 1, de 4 de maio de 2020**. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20Conjunta&numero=1.

BESSA, Jorge. **O escândalo da espionagem no Brasil – o caso Snowden**. Brasília: Trampolim Digital, 2017.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2 ed. Rio de Janeiro: Forense, 2020.

BLUM, Rita Peixoto Ferreira. **O Direito à Privacidade e à Proteção dos Dados do Consumidor**. 1 ed. São Paulo: Almedina, 2018.

BORGES, Luana Chystyna Carneiro. **Teorias ciberregulatórias e o caso brasileiro: entre regulação e governança**. Disponível em: https://repositorio.unb.br/handle/10482/35686. Acessado em: 05 de agosto de 2020.

BRASIL. Conselho Nacional de Justiça. **Justiça em números 2019**. Disponível em: https://www.cnj.jus.br/wp-content/uploads/conteudo/arquivo/2019/08/8ee6903750bb4361b5d0d1932ec6632e.pdf

_____. **Exposição de motivos da lei nº 12.965 de 23 de abril de 2014 (Marco Civil da Internet)**. Disponível em: http://www.planalto.gov.br/ccivil_03/Projetos/ExpMotiv/EMI/2011/86-MJ%20MP%20MCT%20MC.htm

_____. Ministério da Justiça. Secretaria de Direito Econômico. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia**. Brasília: SDE/DPDC, 2010. Disponível em: https://legado.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf

_____. Ministério Público do Distrito Federal e Territórios. **MPDFT ajuíza 1ª ação civil pública com base na LGPD**. Disponível em: https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2020/12384-mpdft-ajuiza-1-acao-civil-publica-com-base-na-lgpd. Acessado em: 06 de outubro de 2020.

_____. Senado Federal. **Lei Geral de Proteção de Dados entra em vigor**. Disponível em: https://www12.senado.leg.br/noticias/materias/2020/09/18/lei-geral-de-protecao-de-dados-entra-em-vigor. Acessado em: 07 de outubro de 2020.

_____. Senado Federal. **Proposta de Emenda à Constituição nº 17, de 2019**. Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Brasília: Senado Federal, 2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594.

_____. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade. Arts. 20 e 21 da lei n. 10.406/2002 (código civil). Preliminar de ilegitimidade ativa rejeitada. Requisitos legais observados. Mérito: aparente conflito entre princípios constitucionais: liberdade de expressão, de informação, artística e cultural, independente de censura ou autorização prévia (art. 5º incs. IV, IX, XIV; 220, §§ 1º E 2º) e inviolabilidade da intimidade, vida privada, honra e imagem das pessoas (art. 5º, inc. X). Adoção de critério da ponderação para interpretação de princípio constitucional. Proibição de censura (estatal ou particular). Garantia constitucional de indenização e de direito de resposta. Ação direta julgada procedente para dar interpretação conforme à constituição aos arts. 20 e 21 do código civil, sem redução de texto. **Acórdão em Ação Direta de Inconstitucionalidade nº4815/DF**. Associação Nacional dos Editores de Livros – ANEL e Presidente da República e Presidente do Congresso Nacional. Relatora: Ministra Carmen Lúcia. DJ, 10 jun. 2015. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=10162709. Acessado em: 03 de outubro de 2020.

BSA. The Software Alliance. **Qual é o "x" da questão com relação a dados?** Disponível em: https://data.bsa.org/wp-content/uploads/2015/10/BSADataStudy_br.pdf. Acessado em: 02 de setembro de 2020.

CALABRICH, Bruno Freire de Carvalho. **O conceito de tratamento de dados pessoais e o acórdão Lindqvist, do Tribunal de Justiça da União Europeia**. Disponível em: https://rtrf1.emnuvens.com.br/trf1/article/view/103/92. Acessado em: 05 de outubro de 2020.

COSTA, José Américo Martins da. **Releitura constitucional no conflito entre os direitos fundamentais na proteção conferida à privacidade e o acesso à informação**. Disponível em: http://hdl.handle.net/10451/32567. Acessado em: 05 de outubro de 2020.

CRUVINEL, Guilherme Ferreira Araújo. **A (hiper)vulnerabilidade do consumidor no tratamento de seus dados pessoais**. Estudos essenciais de Direito Digital: posição 3516 a 3978. Uberlândia: LAECC, 2019. Acessado em: Amazon Kindle.

Euro Banking Association. **Understanding the business relevance of Open APIs and *Open banking* for banks**. Disponível em: https://www.abe-eba.eu/media/azure/production/1522/business-relevance-of-open-apis-and-open-banking-for-banks.pdf.

FACCHINI NETO, Eugênio; DEMOLINER, Karine Silva. **Direito à privacidade na era digital – uma releitura do art. XII da Declaração Universal dos Direitos Humanos (DUDH) na sociedade do espetáculo**. Disponível em: https://revistaconsinter.com/revistas/ano-v-numero-ix/direitos-difusos-coletivos-e-individuais-homogeneos/direito-a-privacidade-na-era-digital-uma-releitura-do-art-xii-da-declaracao-universal-dos-direitos-humanos-dudh-na-sociedade-do-espetaculo/. Acessado em: 08 de outubro de 2020.

INTEGRAÇÃO: o que significa API e como ela funciona. **Red Hat**. Disponível em: https://www.redhat.com/pt-br/topics/api/what-are-application-programming-interfaces.

JARDIM, José Maria. **A lei de acesso à informação pública: dimensões político-informacionais**. Disponível em: https://revistas.ancib.org/index.php/tpbci/article/view/266. Acessado em: 06 de outubro de 2020.

JENSEN, Claus T. **APIs for dummies, IBM Limited Edition**. Hoboken: John Wiley & Sons, INC, 2015.

LAPAIRE, Jean-Rémi. **Why content matters. Zuckerberg: vox media and the cambridge analytica data leak**. Disponível em: http://www.ucs.br/etc/revistas/index.php/antares/article/view/6583/3418. Acessado em 02 de outubro de 2020.

LEONARDI, Marcel. **Aspectos controvertidos entre a lei geral de proteção de dados e o marco civil da internet**. Temas atuais de proteção de dados: p. 217 a 243. São Paulo: Thomson Reuters Brasil, 2020.

MACHADO, Diego; DONEDA, Danilo. **Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados**. Revista dos Tribunais. vol. 998. Caderno Especial. p. 99-128. São Paulo: RT, dezembro 2018.

MACHADO, José Mauro Decossau. SANTOS, Matheus Chucri dos. PARANHOS, Mário Cosac Oliveira. **LGPD e GDPR: Uma análise comparativa entre as legislações.** Disponível em: http://www.pinheironeto.com.br/publicacoes/lgpd-e-gdpr-uma-analise-comparativa-entre-as-legislacoes. Acessado em 05 de agosto de 2020.

MARTINS, Marcelo Guerra; TATEOKI, Victor Augusto. **Proteção de dados pessoais e democracia: fake news, manipulação do eleitor e o caso da Cambridge Analytica**. Disponível em: https://www.revistas.unilasalle.edu.br/index.php/redes/article/view/5610/pdf. Acessado em: 05 de outubro de 2020.

PALHARES, Felipe. **Cookies: contornos atuais**. Temas atuais de proteção de dados: p. 9 a 59. São Paulo: Thomson Reuters Brasil, 2020.

PALUDETTO, Vitor; BARBIERI, Henrique Shirassu. **Guia sobre a nova lei geral de proteção de dados**. Acessado em: Amazon Kindle. São Paulo: Go LGPD, 2020.

PEREIRA, Weberson. **API: conceito, exemplos de uso e importância da integração para desenvolvedores**. Disponível em: https://take.net/blog/devs/api-conceito-e-exemplos.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD)**. São Paulo: Saraiva Educação, 2018.

REIS, Débora. **Data Science, GDPR e LGPD: 20 coisas que você precisa fazer para não ser acusado por maus tratos a dados pessoais**. 2 ed. Amazon Kindle: Bestseller, 2019.

RODRIGUES, Fernando de Assis. **Coleta de dados em redes sociais: privacidade de dados pessoais no acesso via Application Programming Interface**. Disponível em: http://hdl.handle.net/11449/149768. Acessado em: 28 de setembro de 2020.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro; FINGER, Brunize. **O direito à proteção de dados pessoais e a privacidade**. Disponível em: https://revistas.ufpr.br/direito/article/view/30768/19876.

SILVA, Natália Balbino da. **O que esperar do contencioso de dados**. Temas atuais de proteção de dados: p. 375 a 399. São Paulo: Thomson Reuters Brasil, 2020.

SILVA, Ricardo Antunes; CRUZ, Caroline Quaresma Piccinato da. **O impacto do novo ecossistema democrático de pagamento instantâneo (Pix) no sistema financeiro nacional**. Disponível em: http://portaldeperiodicos.unisul.br/index.php/U_Fato_Direito/article/view/9828/5362. Acessado em: 10 de outubro de 2020.

TEFFÉ, C. S. De; VIOLA, M. **Tratamento de dados pessoais na LGPD: estudo sobre as bases legais**. Disponível em: https://civilistica.emnuvens.com.br/redc/

article/view/510.

TEPEDINO, Gustavo; TEFFÉ, C. S. De. **Consentimento e proteção de dados pessoais na LGPD**. Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro: p. 287 a 322. São Paulo: Thomson Reuters Brasil, 2019.

THOMAZ, Alan Campos Elias. **Privacidade e proteção de dados na indústria financeira**. Temas atuais de proteção de dados: p. 127 a 152. São Paulo: Thomson Reuters Brasil, 2020.

ZANATTA, Rafael A. F. **Tutela coletiva e coletivização da proteção de dados pessoais**. Temas atuais de proteção de dados: p. 345 a 373. São Paulo: Thomson Reuters Brasil, 2020.

ANEXO A – GLOSSÁRIO

Anonimização:	Aplicação de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo
API:	*Application programming interface* - estrutura formal de regras e protocolos que proporcionam a interação de conjunto de dados, por dois ou mais sistemas de informação, independentes de plataforma, de acesso público, privado ou misto, usando padrões abertos ou fechados para o intercâmbio dos dados e contém documentação disponível na origem para o entendimento de todas as partes sobre o seu modo de operacionalização.[17]
Arranjo de pagamento:	Conjunto de regras e procedimentos que disciplina a prestação de determinado serviço de pagamento ao público, aceito por mais de um recebedor, mediante acesso direto pelos usuários finais, pagadores e recebedores.
Consentimento:	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.
FinTech:	Atividade financeira viabilizada ou fornecida através de novas tecnologias, que tem repercussões na totalidade do setor financeiro em todas as suas vertentes, da banca e dos seguros, aos fundos de pensões, à consultoria de investimentos, aos serviços de pagamento e às infraestruturas de mercado.
GDPR:	*General Data Protection Regulation* – Regulamento Geral sobre a Proteção de Dados da União Europeia
LGPD:	Lei Geral de Proteção de Dados – Lei nº 13.709/2018
Open banking:	Compartilhamento padronizado de dados e serviços por meio de abertura e integração de sistemas.
Pix	Meio de pagamento instantâneo lançado e regulado pelo Banco Central do Brasil

[17] RODRIGUES, Fernando de Assis. Coleta de dados em redes sociais: privacidade de dados pessoais no acesso via Application Programming Interface. Disponível em: http://hdl.handle.net/11449/149768. Acessado em: 28 de setembro de 2020.

Pseudonimização/ pseudoanonimização:	Tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.
SPI	Sistema de Pagamentos Interbancário – plataforma tecnológica que suporte a solução Pix