Insper

LLM – Direito dos Mercados Financeiro e de Capitais

Karine Evangelista Araujo Oliveira

O legítimo interesse do controlador ou de terceiros para o tratamento de dados pessoais previsto na Lei nº 13.709/2018 e a prestação de serviços de pagamento

São Paulo

2021

Karine Evangelista Araujo Oliveira

O legítimo interesse do controlador ou de terceiros para o tratamento de dados pessoais previsto na Lei nº 13.709/2018 e a prestação de serviços de pagamento

Trabalho de Conclusão de Curso apresentado ao LLM de Direito dos Mercados Financeiro e de Capitais, como requisito parcial para a obtenção título de pós-graduada em Direito dos Mercados Financeiro e de Capitais.

Orientadora: Profa. Dra. Pamela Gabrielle Romeu Gomes Roque

São Paulo

2021

Oliveira. Karine Evangelista Araujo.

O legítimo interesse do controlador para o tratamento de dados pessoais previsto na Lei nº 13.709/2018 e a prestação de serviços de pagamento / Karine Evangelista Araujo Oliveira. – São Paulo, 2021. 50f.

Trabalho de Conclusão de Curso (LLM em Direito dos Mercados Financeiro e de Capitais) – Insper, 2021.

Orientadora: Profa. Dra. Pamela Gabrielle Romeu Gomes Roque

1. LGPD. 2. Proteção de dados. 3. Dados pessoais. 4. Legítimo interesse. 5. Instituições de Pagamento. I. Karine Evangelista Araújo Oliveira. II. O legítimo interesse do controlador para o tratamento de dados pessoais previsto na Lei nº 13.709/2018 e a prestação de serviços de pagamento

Agradecimentos

Primeiramente, aos colegas da turma do LLM de Direito dos Mercados Financeiro e de Capitais. A convivência com todos tornou a experiência incrivelmente rica.

À Profa. Dra. Pamela Gabrielle Romeu Gomes Roque, pela orientação para o desenvolvimento do trabalho, e à equipe da Biblioteca Telles, pelo auxílio para sua finalização.

Ao FAS Advogados e, especialmente, ao sócio Paulo Mertz Focaccia, pela confiança em meu comprometimento em aproveitar ao máximo esta oportunidade de aprimoramento profissional.

Às amigas queridas Ana Teresa de Abreu Coutinho Boscolo e Gabriella Rosón de Lima, pela paciência, pelo carinho e pelo incentivo.

Por fim, a meu marido, Guilherme, pelo amor e parceria sem os quais não teria sido possível concluir este trabalho.

Resumo

Tendo em vista que a Lei nº 13.709/2018 ("LGPD"), que regula o tratamento de dados pessoais no Brasil, entrou em vigor no mês de setembro de 2020 e que, a partir de agosto de 2021 a Autoridade Nacional de Proteção de Dados ("ANPD") poderá aplicar sanções administrativas substanciais em caso de descumprimento das disposições da norma, o presente trabalho possui o objetivo de analisar os requisitos para utilização da base legal do legítimo interesse do controlador ou de terceiros para o tratamento de dados pessoais pelas instituições prestadoras de serviços de pagamento, de forma a maximizar a segurança jurídica.

No decorrer deste artigo, foram abordados os principais conceitos da LGPD e as bases legais relevantes para o tratamento de dados pessoais, considerando as atividades desenvolvidas por instituições de pagamento.

Durante seu desenvolvimento, são apresentadas considerações sobre a forma como o tema é tratado no direito comunitário europeu e o tratamento do tema no ordenamento jurídico brasileiro, bem como o teste de proporcionalidade do legítimo interesse. Foi ressaltada a semelhança entre a LGPD e o Regulamento Geral de Proteção de Dados da União Europeia ("GDPR"), bem como a possibilidade de utilização das orientações das autoridades de proteção de dados europeias como referência para interpretação de questões controversas a respeito desta base legal, até que haja orientações da ANPD sobre o tema.

Por fim, trata-se especificamente do uso do legítimo interesse do controlador ou de terceiros para o tratamento de dados pessoais no âmbito da prestação de serviços de pagamento, ressaltando-se que, por atuarem em uma indústria classificada como uma plataforma multilateral, as instituições de pagamentos muitas vezes mantêm relacionamento contratual diretamente com um grupo de clientes, mas não com o outro – o qual, não obstante, usufrui dos benefícios da plataforma, ainda que indiretamente. Salienta-se que, neste cenário, muitas vezes, em situações concretas, o tratamento de dados pessoais será imprescindível e não será viável que a instituição responsável pelo tratamento colete o consentimento dos titulares de tais dados ou se utilize de outras bases legais para justificá-lo.

Conclui-se que, nestas situações, as instituições de pagamento deverão realizar o teste de ponderação do legítimo interesse e documentá-lo.

Palavras-chave: LGPD. Proteção de dados. Dados pessoais. Legítimo interesse. Instituições de Pagamento.

Abstract

Considering that Law No. 13,709/2018 ("LGPD"), from the Portuguese *Lei Geral de Proteção de Dados*), which regulates the processing of personal data in Brazil, came into force in September 2020 and that, as of August 2021, the National Data Protection Authority ("ANPD", from the Portuguese *Autoridade Nacional de Proteção de Dados*) may apply substantial administrative sanctions in case of non-compliance with its provisions, this work aims to analyze the requirements for using the legal basis of the legitimate interest of the controller or third parties for the processing of personal data by institutions which provide payment services, in order to maximize legal certainty.

Throughout this article, the main concepts of the LGPD and the relevant legal bases for the processing of personal data, considering the activities carried out by payment institutions, were addressed.

During its development, considerations are presented on the way the topic is treated in European community law and on the treatment of the topic in the Brazilian legal system, as well as on the test of proportionality of legitimate interest. The similarity between the LGPD and the General Data Protection Regulation (“GDPR”) was highlighted, as well as the possibility of using the guidelines of the European data protection authorities as a reference for the interpretation of controversial issues regarding this legal basis, until there is guidance from the ANPD on the subject.

Finally, it specifically addresses the use of the legitimate interest of the controller or third parties for the processing of personal data in the context of the provision of payment services, noting that, by operating in an industry classified as a multilateral platform, payment institutions often maintain a contractual relationship directly with one group of customers, but not with the other – which nevertheless enjoys the benefits of the platform, albeit indirectly. It should be noted that, in this scenario, often, in concrete situations, the processing of personal data will be essential and it will not be feasible for the institution responsible for the processing to collect the consent of the data subjects or use other legal bases to justify it.

The conclusion of this work is that, in these situations, payment institutions must carry out the legitimate interest weighting test and document it.

Keywords: LGPD. Data Protection. Personal Data. Legitimate Interest. Payment Institutions.

Sumário

1 INTRODUÇÃO **7**
2 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: CONCEITOS E BASES LEGAIS RELEVANTES PARA A COMPREENSÃO DO TEMA **16**
2.1 Dados pessoais **16**
2.2 Dados pessoais sensíveis **17**
2.3 Agentes de tratamento de dados pessoais **18**
2.4 Tratamento de dados pessoais **19**
2.5 Bases legais para tratamento **20**
2.5.1 Consentimento 22
2.5.2 Cumprimento de obrigação legal ou regulatória 24
2.5.3 Execução de contrato ou procedimentos preliminares 25
3 O LEGÍTIMO INTERESSE DO CONTROLADOR OU DE TERCEIROS PARA O TRATAMENTO DE DADOS PESSOAIS **27**
3.1 O legítimo interesse no direito comunitário europeu **27**
3.2 O legítimo interesse no direito brasileiro **30**
3.3 Teste de ponderação do legítimo interesse **33**
4 O USO DO LEGÍTIMO INTERESSE COMO BASE LEGAL PARA O TRATAMENTO DE DADOS PESSOAIS NO ÂMBITO DA PRESTAÇÃO DE SERVIÇOS DE PAGAMENTO **37**
5 CONCLUSÕES **40**
REFERÊNCIAS **43**

1 INTRODUÇÃO

O início do século 21 tem como uma de suas características mais marcantes a consolidação de um cenário com uma quantidade exponencialmente crescente de dados gerados e disponibilizados, bem como, paralelamente, o crescimento da capacidade de processamento desses dados[1].

A título ilustrativo, é possível mencionar alguns números: no ano de 2020, a cada minuto, mais de 40 milhões de mensagens são enviadas via Whatsapp, mais de 1 milhão de chamadas de vídeo e de voz são realizadas, um milhão de dólares são gastos online e cerca de 4 mil dólares são gastos em aplicativos móveis, de acordo com levantamento publicado pela empresa Domo, especializada em *cloud computing*[2].

Essa maior facilidade em se criar e disponibilizar dados tem suas implicações. Em razão da evolução tecnológica recente, que permite encurtar distâncias e tempo, sedimentou-se uma nova forma de organização social – a chamada Sociedade da Informação – em que a informação é o elemento nuclear para o desenvolvimento da economia, substituindo os recursos que um dia estruturaram as sociedades agrícola (terra), industrial (produção fabril) e pós-industrial (serviços ofertados), de acordo com Bruno Ricardo Bioni[3].

Como era de se esperar, dados se tornaram matéria prima de toda uma economia (a "economia de dados" ou "*data economy*") sendo, portanto, reconhecidos como verdadeiros ativos de empresas. De acordo com a revista *The Economist*[4], o recurso mais valioso do mundo deixou de ser o petróleo, passando a ser dados.

Conforme ressaltam Ricardo Oliveira e Márcio Cots, ao conhecer melhor seu público, mediante o tratamento de dados pessoais, especialmente no que diz respeito a seus hábitos de consumo, as empresas podem ofertar seus produtos e serviços de forma mais assertiva, refletir sobre novos negócios e oportunidades e obter para si diferenciais competitivos. Além disso, o

---

[1] Apenas para fins exemplificativos, cabe destacar o computador quântico desenvolvido pelo Google, que conseguiu descrever os prováveis resultados de um código criado por um gerador de números aleatórios em pouco mais de 3 minutos, quando um computador comum levaria cerca de 10 mil anos. (VIGGIANO, Giuliana. Google atinge "supremacia quântica", que promete revolucionar a computação. **Galileu**, 23 out. 2019. Disponível em https://revistagalileu.globo.com/Tecnologia/noticia/2019/10/google-atinge-supremacia-quantica-que-promete-revolucionar-computacao.html. Acesso em 14 dez. 2020.)

[2] DOMO, INC. **Data never sleeps 8.0.** Domo, 2020. Disponível em https://www.domo.com/learn/data-never-sleeps-8. Acesso em 06 dez. 2020.

[3] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2ª ed. Rio de Janeiro: Forense, 2020. p. 3-4.

[4] THE ECONOMIST. The world's most valuable resource is no longer oil, but data. **The Economist**. 06 maio 2017. Disponível em https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em 06 dez. 2020.

tratamento de dados pessoais permite a customização do atendimento ao consumidor, o que agrega valor às marcas[5].

O tratamento intensivo de dados pessoais tornou necessário resgatar e reestabelecer os termos do compromisso das instituições com os indivíduos, no que diz respeito à proteção e à garantia dos direitos humanos fundamentais, entre os quais a privacidade, já celebrados desde a Declaração Universal dos Direitos Humanos, de 1948, como salienta Patricia Peck Pinheiro[6].

Conforme destaca Rony Vainzof, a busca do equilíbrio "entre interesses sociais e econômicos, entre o público e o privado, entre liberdade, proteção e segurança" é, desde sempre, o maior desafio e elemento fundamental da atividade regulatória[7].

A par dessas mudanças, diversos países iniciaram seus movimentos no sentido de regular a utilização de dados ou aprimorar a regulação já existente – destacando-se o Regulamento Geral de Proteção de Dados da União Europeia – RGPD, mais conhecido como GDPR (do inglês *General Data Protection Regulation*).

A norma, aprovada em abril de 2016, teve efeitos que extrapolaram as fronteiras da União Europeia, uma vez que estabelece que "empresas europeias somente poderiam contratar empresas estrangeiras se estas estivessem localizadas em países que possuíssem grau de proteção igual ou superior ao estabelecido em seu território", como ressaltam Ricardo Oliveira e Marcio Cots[8].

Este foi um fator acelerador para a atividade legislativa nacional, haja vista que o Brasil não poderia se dar ao luxo de enfrentar dificuldades para fazer negócios com os países europeus.

Um outro fator, apontado por Pietra Daneluzzi Quinelato[9], foi o escândalo da *Cambridge Analytica*, noticiado no início de 2018, que trouxe à baila discussões a respeito dos limites ao tratamento de dados pessoais – de acordo com o apurado, o tratamento indevido de dados pessoais e direcionamento de propaganda eleitoral pode ter afetado o resultado das eleições americanas de 2016.

---

[5] OLIVEIRA, Ricardo; COTS, Márcio. **O legítimo interesse e a LGPDP**: Lei Geral de Proteção de Dados Pessoais. 1ª ed. São Paulo: RT, 2020. p. 28.
[6] PINHEIRO, Patrícia Peck. **Proteção de dados pessoais**: comentários à Lei 13.709/2018 (LGPD). 2ª ed. São Paulo: Saraiva Educação, 2020. p. 17.
[7] VAINZOF, Rony. Dados pessoais, tratamento e princípios. In: MALDONADO, Viviane Nobrega; BLUM, Renato Opice (Coord.). **Comentários ao GDPR – Regulamento Geral de Proteção de Dados da União Europeia**, 2ª ed. São Paulo: RT, 2019. p. 34.
[8] OLIVEIRA, Ricardo; COTS, Márcio. **O legítimo interesse e a LGPDP**: Lei Geral de Proteção de Dados Pessoais. 1ª ed. São Paulo: RT, 2020. p. 30.
[9] QUINELATO, Pietra Daneluzzi. A proteção de dados pessoais no âmbito das *startups*. In: OIOLI, Erik Frederico (Coord.). **Manual de direito para startups**. 2ª ed. São Paulo: RT, 2020. p. 251.

Após longas discussões no Congresso e debates calorosos, com a participação da sociedade civil, em agosto de 2018, a Lei nº 13.709, mais conhecida como Lei Geral de Proteção de Dados Pessoais ou LGPD, fortemente inspirada no GDPR, foi sancionada pelo então Presidente Michel Temer.

Até então, o ordenamento jurídico brasileiro não contava com uma normativa sistemática e transversal, que reconhecesse a proteção de dados como um direito autônomo, aplicável de forma ampla a entes públicos e privados, de todos os setores econômicos, atuantes tanto no meio digital quanto no meio físico, como salienta Felipe Schvartzman[10].

Isto, contudo, não significa que o ordenamento jurídico pátrio não regulava a proteção de dados pessoais. Embora, de fato, não houvesse uma legislação geral sobre o tema, havia uma série de normas esparsas que em certa medida traziam, direta ou indiretamente, disposições que tutelavam informações pessoais (o que sempre exigia um considerável esforço de interpretação, como salientam Danilo Leme Crespo e Dalmo Ribeiro Filho[11]). Entre tais normas, é possível destacar tanto normas de amplo escopo e quanto normas setoriais.

Entre as normas de amplo escopo, vale mencionar a Constituição Federal[12]; o Código Civil[13]; normas de proteção aos direitos do consumidor como o Código de Defesa do

---

[10] SCHVARTZMAN, Felipe. Lei Geral de Proteção de Dados Pessoais e riscos cibernéticos: coexistência de normas no mercado de meios de pagamento. In: COHEN, Gabriel Luiz Schvartzman (Coord.). **Direito dos Meios de Pagamento**. São Paulo: Quartier Latin, 2020, p. 379-380.

[11] CRESPO, Danilo Leme; FILHO, Dalmo Ribeiro. A evolução legislativa brasileira sobre a proteção de dados pessoais: a importância da promulgação da Lei Geral de Proteção de Dados Pessoais. **Revista de Direito Privado**. v. 98, p. 1-20. mar – abr 2019. Disponível em https://revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad6adc600000179f81daabd6fc295cb&docguid=I98c1d5d04a0611e9b1d8010000000000&hitguid=I98c1d5d04a0611e9b1d8010000000000&spos=2&epos=2&td=102&context=136&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1. Acesso em 10 jun. 2021. p. 9. (Paginação da versão eletrônica difere da versão impressa).

[12] O texto constitucional estabelece em seu art. 5º, X, que 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, protegendo assim "a esfera privada do indivíduo em diversas dimensões, inclusive na dimensão da privacidade de seus dados pessoais e na autodeterminação de suas informações", de acordo com Laura Schertel Mendes. (MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor**, v. 79, p. 1-26, 2011. Disponível em: https://revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad6adc60000017a5a98d7c0a617e29d&docguid=I1977b2a0008911e1968d00008558bdfc&hitguid=I1977b2a0008911e1968d00008558bdfc&spos=7&epos=7&td=7&context=294&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1. Acesso em 02 jun. 2021. p. 11. (Paginação da versão eletrônica difere da versão impressa).

[13] A proteção consagrada no texto constitucional é transposta no Capítulo II do Código Civil, que trata dos direitos da personalidade, os quais, de acordo com Nelson Nery Junior, compreendem "tudo aquilo que disser respeito à natureza do ser humano, como por exemplo, a vida, liberdade, proteção de dados pessoais, integridade física e moral, honra, imagem, vida privada, privacidade, intimidade, intangibilidade da família, autoestima, igualdade, segurança". (NERY JUNIOR, Nelson; Nery, Rosa Maria de Andrade. **Código Civil anotado e legislação extravagante**. 2. ed. rev. e ampl. São Paulo: Ed. RT, 2004, p. 157.)

Consumidor[14], a Lei nº 12.414/2011 (mais conhecida como "Lei do Cadastro Positivo")[15] e o Decreto nº 7.962/2013[16]; e, por fim, a Lei nº 12.965/2014, mais conhecida como Marco Civil da Internet[17], e o Decreto nº 8.771/2016, que o regulamenta[18].

---

[14] A norma contém uma seção específica a respeito dos bancos de dados e cadastro de consumidores, que estabelece uma série de salvaguardas para os consumidores e obrigações para as entidades responsáveis por tais bancos de dados e cadastros. Trata-se de dispositivo que, segundo Bruno Ricardo Bioni, consubstancia a intenção do legislador de regular todos os bancos de dados que poderiam afetar o livre desenvolvimento da personalidade dos consumidores. (BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2ª ed. Rio de Janeiro: Forense, 2020. p. 121.)

[15] A norma, que disciplina a formação e consulta a bancos de dados com informações de adimplemento de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito, contém disposições complementares às do CDC, proibindo a anotação de informações excessivas (assim consideradas aquelas que não estiverem vinculadas à análise de risco de crédito ao consumidor) e de informações sensíveis (assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas), bem como o uso das informações para finalidades estranhas à atividade de análise de crédito. Em sua redação original, privilegiava o consentimento, estabelecendo que a abertura de cadastro pressupunha autorização prévia (*opt-in*) do potencial cadastrado mediante consentimento informado por meio de assinatura em instrumento específico ou em cláusula apartada e que o compartilhamento de informação de adimplemento somente seria permitido se autorizado expressamente pelo cadastrado, por meio de assinatura em instrumento específico ou em cláusula apartada. Após a promulgação da Lei Complementar nº 166/2019, a norma foi modificada de forma que a autorização prévia passou a ser dispensada, ficando assegurado ao consumidor o direito de solicitar a retirada de seu nome do banco de dados (*opt-out*). Ademais, o compartilhamento de informações pelo gestor do banco de dados com outros bancos de dados passou a ser autorizado, sendo transferidas ao gestor receptor as obrigações e as responsabilidades do gestor que originariamente anotou a informação.

[16] Norma que regulamenta o CDC, para dispor sobre a contratação no comércio eletrônico, que determinou a obrigatoriedade de utilização de mecanismos de segurança eficazes para pagamento e para tratamento de dados do consumidor, conforme art. 4º, VII.

[17] Diploma legal que regula o uso da Internet no Brasil, estabelecendo princípios para sua disciplina (entre os quais estão a proteção da privacidade e a proteção dos dados pessoais), garantias, direitos e deveres, criando uma moldura de direitos e liberdades civis, que pretendeu traduzir os princípios constitucionais fundamentais para a Internet, conforme salienta Ronaldo Lemos. (LEMOS, Ronaldo. O Marco Civil como símbolo do desejo por inovação no Brasil. In: LEITE, George Salomão; LEMOS, Ronaldo (Coord.). **Marco Civil da Internet**. São Paulo: Atlas, 2014, p. 3-11.)

[18] Entre outras disposições, referido decreto estabelece regras específicas para a proteção aos registros, aos dados pessoais e às comunicações privadas.

Entre as normas setoriais, para os fins deste artigo, merecem destaque a Lei nº 12.865/2013[19]; a Lei Complementar nº 105/2013, mais conhecida como Lei de Sigilo Bancário[20]; e a Circular BCB nº 3.681/2013[21].

A LGPD foi editada justamente com o objetivo de centralizar em um único diploma legal as principais determinações relativas ao tratamento de dados referentes a pessoas naturais, acarretando consequências extensíveis a todos os setores da economia, contemplando as atividades de entes públicos e privados, independentemente de o tratamento ser realizado por meio eletrônico ou não.

Dessa forma, considerando-se que as atividades da indústria de meios de pagamento como um todo e das instituições de pagamento[22], especificamente, desenvolvem-se em um cenário de intensa coleta, processamento e compartilhamento de dados pessoais[23], é pertinente

---

[19] Marco regulatório do setor de pagamentos, introduziu no ordenamento jurídico brasileiro as figuras dos arranjos e das instituições de pagamentos, atribuindo competência ao Banco Central do Brasil ("BCB") para regulá-las e supervisioná-las, conforme diretrizes estabelecidas pelo Conselho Monetário Nacional ("CMN"). No exercício desta competência, e em observância ao princípio previsto no art. 7º, IV, da Lei nº 12.865/2013, que estabelece que os arranjos e instituições de pagamento devem atender "às necessidades dos usuários finais, em especial liberdade de escolha, segurança, proteção de seus interesses econômicos, tratamento não discriminatório, privacidade e proteção de dados pessoais, transparência e acesso a informações claras e completas sobre as condições de prestação de serviços", o BCB e o CMN editaram regras que disciplinam pontos que tangenciam a proteção de dados pessoais

[20] Por força da Resolução nº 4.282/2013, do CMN, que estabelece as diretrizes que devem ser observadas na regulamentação, na vigilância e na supervisão das instituições de pagamento e dos arranjos de pagamento integrantes do Sistema de Pagamentos Brasileiro, os instituidores de arranjos de pagamento e as instituições de pagamento ficam sujeitos ao disposto na Lei de Sigilo Bancário, que trata do sigilo das operações de instituições financeiras, estabelecendo que em regra, salvo se houver ordem judicial ou solicitação de comissão parlamentar de inquérito para revelação de informações, as instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados.

[21] Referido ato normativo dispõe sobre o gerenciamento de riscos, os requerimentos mínimos de patrimônio, a governança de instituições de pagamento, a preservação do valor e da liquidez dos saldos em contas de pagamento, e dá outras providências, sendo que, no que diz respeito a elementos de controle operacional, a norma determina que as instituições de pagamento devem criar mecanismos que lhe permitam prever os riscos inerentes a suas atividades, conforme destaca Fabio de Almeida Braga, o qual ressalta ainda que "esse propósito está presente, também, na regra do art. 4º da citada Circular, que determina que a estrutura de gerenciamento de riscos deve prever mecanismos de proteção e segurança de dados armazenados, processados ou transmitidos, além de procedimentos para monitorar, rastrear e restringir acesso a dados sensíveis, redes, sistemas, bases de dados e módulos de segurança, e ainda, revisão das medidas de segurança e de sigilo de dados". (BRAGA, Fabio de Almeida. Aplicabilidade da Lei de Sigilo Bancário na Atuação dos Instituidores de Arranjos e das Instituições de Pagamento. In: COHEN, Gabriel Luiz Schvartzman (Coord.). **Direito dos Meios de Pagamento**. São Paulo: Quartier Latin, 2020, p. 447.)

[22] Pessoa jurídica que, aderindo a um ou mais arranjos de pagamento, tenha como atividade principal ou acessória, alternativa ou cumulativamente: (a) disponibilizar serviço de aporte ou saque de recursos mantidos em conta de pagamento; (b) executar ou facilitar a instrução de pagamento relacionada a determinado serviço de pagamento, inclusive transferência originada de ou destinada a conta de pagamento; (c) gerir conta de pagamento; (d) emitir instrumento de pagamento; (e) credenciar a aceitação de instrumento de pagamento; (f) executar remessa de fundos; (g) converter moeda física ou escritural em moeda eletrônica, ou vice-versa, credenciar a aceitação ou gerir o uso de moeda eletrônica; e (h) outras atividades relacionadas à prestação de serviço de pagamento, designadas pelo Banco Central do Brasil, conforme art. 6º, III, da Lei nº 12.865/2013.

[23] A este respeito, Fabio de Almeida Braga esclarece que, ao permitirem a realização de pagamentos independentemente de relacionamentos com bancos e outras instituições financeiras, possibilitando, até mesmo, a realização de transações de pagamento mediante o uso de telefones celulares, as instituições de

examinar as hipóteses de tratamento de dados pessoais previstas na LGPD, para se identificar quais seriam as bases legais para o tratamento realizado no âmbito das atividades de tais instituições.

A norma estabelece que o tratamento de dados pessoais somente pode ser realizado quando configuradas as hipóteses listadas em seu art. 7º, quais sejam: (i) mediante o consentimento do titular; (ii) para o cumprimento de obrigação legal ou regulatória; (iii) pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congênere; (iv) para a realização de estudos por órgão de pesquisa; (v) quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; (vi) para o exercício regular de direitos em processo judicial, administrativo ou arbitral; (vii) para a proteção da vida ou da incolumidade física do titular ou de terceiro; (viii) para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (ix) quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou (x) para a proteção do crédito.

A redação da maioria das bases de tratamento previstas na legislação é bastante precisa e objetiva, mas isto não pode ser dito a respeito do interesse legítimo. A terminologia adotada é ampla e carregada de subjetividade, o que torna um desafio o adequado manejo desta base legal de tratamento de dados pessoais.

Assim, pretende-se analisar os limites do legítimo interesse do controlador ou de terceiros para o tratamento de dados pessoais previsto na Lei nº 13.709/2018, para que se possa identificar os casos em que o tratamento de dados pessoais pelas instituições de pagamento poderá justificar-se pelo legítimo interesse – ficando dispensada a obtenção do consentimento dos titulares de tais dados (as pessoas físicas às quais os dados dizem respeito).

O tema possui grande potencial de gerar debate, tendo em vista que a LGPD entrou em vigor no mês de setembro de 2020 (ainda sem a possibilidade de aplicação de sanções

---

pagamento lidam diretamente com os dados e informações financeiras dos usuários. O autor salienta que, assim sendo, tais instituições têm acesso não só a informações e a valores transferidos entre pagadores e recebedores, mas também a inúmeras informações e dados referentes à identidade e diversas peculiaridades de perfil dos usuários – sejam eles remetentes pagadores ou destinatários e beneficiários do fluxo de recursos financeiros. (BRAGA, Fabio de Almeida. Aplicabilidade da Lei de Sigilo Bancário na Atuação dos Instituidores de Arranjos e das Instituições de Pagamento. In: COHEN, Gabriel Luiz Schvartzman (Coord.). **Direito dos Meios de Pagamento**. São Paulo: Quartier Latin, 2020, p. 435).

administrativas[24], que serão aplicáveis apenas a partir de agosto de 2021), após sucessivas mudanças na data de início de sua vigência e a superação da inércia governamental quanto à criação da Autoridade Nacional de Proteção de Dados ("ANPD").

O órgão iniciou suas atividades em dezembro de 2020, com a publicação de seu sítio eletrônico (canal oficial de comunicação com o público externo) e já adotou algumas medidas importantes, tais como a publicação da agenda regulatória 2021/2022, a tomada de subsídios para regulamentação da aplicação da LGPD para microempresas e empresas de pequeno porte, a publicação do planejamento estratégico 2021/2023, a disponibilização de canal para encaminhamento de dúvidas sobre a interpretação da norma, a tomada de subsídios para regulamentação da notificação de incidentes de segurança[25] e a abertura de consulta pública sobre a norma que regulará o processo de fiscalização e aplicação de sanções pelo órgão[26].

Contudo, as atividades ainda são bastante incipientes e há diversas incertezas a respeito da interpretação da LGPD, sendo uma delas os limites do legítimo interesse do controlador ou de terceiros para o tratamento de dados pessoais. Como utilizar esta base legal com bom grau de segurança jurídica, de forma a viabilizar o desenvolvimento da livre iniciativa e de novos negócios, sem expor os titulares dos dados a riscos extraordinários?

No decorrer das atividades de uma instituição de pagamentos, tais como a criação dos termos e condições de uso dos produtos ofertados, a criação de sua política de privacidade, o desenvolvimento de novos produtos, a definição do processo de *onboarding* de clientes para cada produto, a definição da estratégia de comunicação com *prospects* e abordagem de *leads*, a elaboração de diversos contratos com fornecedores e parceiros, entre outras, verifica-se que a

---

[24] De acordo com o art. 52 da norma, podem ser aplicadas as penalidades de advertência, com indicação de prazo para adoção de medidas corretivas; multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; multa diária, observado o limite total de R$ 50.000.000,00 (cinquenta milhões de reais) por infração; publicização da infração após devidamente apurada e confirmada a sua ocorrência; bloqueio dos dados pessoais a que se refere a infração até a sua regularização; eliminação dos dados pessoais a que se refere a infração; suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; e até mesmo a proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

[25] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Confira linha do tempo sobre principais ações da ANPD. 14 abr. 2021. Disponível em https://www.gov.br/anpd/pt-br/assuntos/noticias/confira-linha-do-tempo-com-as-principais-acoes-da-anpd. Acesso em 01 jun. 2021.

[26] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. ANPD abre consulta pública sobre norma de fiscalização. 28 maio. 2021. Disponível em https://www.gov.br/anpd/pt-br/assuntos/noticias/confira-linha-do-tempo-com-as-principais-acoes-da-anpd. Acesso em 01 jun. 2021.

execução de tais atividades depende do tratamento de dados pessoais e as perguntas “Preciso de consentimento?” e “Pode ser legítimo interesse?” surgem com frequência.

Buscar a resposta desta pergunta é de grande importância, pois as penalidades administrativas previstas para os casos de tratamento irregular de dados pessoais incluem multas que podem chegar a R$ 50.000.000,00 (cinquenta milhões de reais) por infração – isso sem mencionar o potencial prejuízo à imagem da empresa. Trata-se de um desafio considerável, tendo em vista que a LGPD entrou em vigor há pouco tempo e não existe um consenso a respeito de como a norma deve ser interpretada.

Em atenção a este cenário, este trabalho possui o objetivo de analisar os requisitos para utilização da base legal do legítimo interesse do controlador ou de terceiros para o tratamento de dados pessoais pelas instituições prestadoras de serviços de pagamento, de forma a maximizar a segurança jurídica.

Para sua elaboração, será realizada a análise de textos legais e infralegais relevantes, bem como o estudo de doutrina nacional e estrangeira relativas à temática escolhida – notadamente, materiais a respeito do entendimento adotado pelas autoridades de proteção de dados europeias para utilização da base legal do legítimo interesse do controlador ou de terceiros, uma vez que a o GDPR inspirou a LGPD, em grande medida.

Inicialmente, o trabalho tratará da LGPD em si, apresentando os principais conceitos e as bases legais relevantes, considerando as atividades desenvolvidas por instituições de pagamento.

O legítimo interesse será tratado em um capítulo específico, subsequente ao primeiro. Nele são apresentadas considerações sobre a forma como o tema é tratado no direito comunitário europeu, discorre-se sobre o tratamento do tema no ordenamento jurídico brasileiro e trata-se, ainda, do teste de proporcionalidade do legítimo interesse. Ao longo do capítulo, ressalta-se a semelhança entre a LGPD e o GDPR, bem como a possibilidade de utilização das orientações das autoridades de proteção de dados europeias como referência para interpretação de questões controversas a respeito desta base legal, até que haja orientações da ANPD sobre o tema.

Por fim, trata-se especificamente do uso do legítimo interesse do controlador ou de terceiros para o tratamento de dados pessoais no âmbito da prestação de serviços de pagamento.

Naturalmente, não se pretende esgotar o tema, tendo em conta que analisar a aplicação da LGPD a indústria de pagamentos é uma atividade que envolve o estudo de uma nova norma, que entrou em vigor há pouco, que está sujeita à atuação da ANPD. Assim, este trabalho tem o

propósito descritivo e, em certa medida, também prescritivo, diante das expectativas em relação à aplicação do texto legal.

2 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: CONCEITOS E BASES LEGAIS RELEVANTES PARA A COMPREENSÃO DO TEMA

A Lei Geral de Proteção de Dados representa não só uma mudança legislativa, mas "o marco de uma nova cultura de tutela da privacidade e dos dados pessoais no Brasil", segundo Mario Viola e Chiara Spadaccini de Teffé[27], fazendo com que os indivíduos tenham a seu dispor instrumentos mais específicos e adequados para zelar pelas informações que lhes dizem respeito – sem deixar de reconhecer a importância de fomentar o desenvolvimento econômico e tecnológico e a inovação, vale ressaltar.

Neste sentido, a norma estabelece que a disciplina da proteção de dados pessoais possui como fundamentos:

a) o respeito à privacidade;
b) a autodeterminação informativa;
c) a liberdade de expressão, de informação, de comunicação e de opinião;
d) a inviolabilidade da intimidade, da honra e da imagem;
e) o desenvolvimento econômico e tecnológico e a inovação;
f) a livre iniciativa, a livre concorrência e a defesa do consumidor; e
g) os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Feitas estas considerações iniciais sobre a norma, apresenta-se, a seguir, seus principais conceitos e as bases legais relevantes para compreensão do tema deste artigo.

2.1 Dados pessoais

Conforme aponta Rony Vainzof, a LGPD adotou o conceito expansionista de dado pessoal[28], haja vista que, de acordo seu art. 5º, I, dado pessoal é qualquer "informação relacionada a pessoa natural identificada ou identificável". Assim, são considerados dados pessoais não apenas aquelas informações que identificam um indivíduo de forma direta, mas

---

[27] VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11º. In: BIONI, Bruno et al (Coords.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Grupo GEN, 2020, p. 159.

[28] VAINZOF, Rony. Comentários ao art. 5º. In: MALDONADO, Viviane Nobrega; BLUM, Renato Opice (Coord.). **LGPD**: Lei Geral de Proteção de Dados comentada, 2ª ed. São Paulo: RT, 2019. p. 89.

também aquelas que possuem o potencial de identificá-lo, ainda que mediante sua combinação com outras informações.

A definição adotada pela LGPD, que já havia sido utilizada anteriormente, quando da edição do Decreto nº 8.771/2016, que regulamentou o Marco Civil da Internet, é semelhante à do GDPR, segundo o qual dado pessoal é "qualquer informação relativa a uma pessoa natural identificada ou identificável" – o normativo europeu, contudo, vai um pouco além, detalhando em seu atr. 4º, 1, o que considera ser uma pessoa natural identificável (o que não ocorre na lei brasileira)[29]:

> é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular;

Vale ressaltar que, para os fins da LGPD, dados anonimizados não são considerados dados pessoais, salvo quando o processo de anonimização for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis[30], puder ser revertido, conforme determina o art. 12 da norma.

Neste sentido, podem ser considerados como dados pessoais, para os fins da LGPD, as informações utilizadas para formação do perfil comportamental de determinada pessoa natural, se identificada.

2.2 Dados pessoais sensíveis

A LGPD introduz no ordenamento jurídico brasileiro a definição de 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.

O conceito contempla um conjunto de dados pessoais cujo tratamento pode implicar algum tipo de discriminação, acarretando "riscos e vulnerabilidades potencialmente mais

---

[29] UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados**). Jornal Oficial da União Europeia**, Bruxelas, 04 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=PT. Acesso em: 17 jun. 2021.

[30] Conforme §1º de tal dispositivo legal, a determinação da razoabilidade deve levar em consideração critérios objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

gravosas aos direitos e liberdades fundamentais dos titulares", conforme aponta Rony Vainzof.[31] – por esta razão, tais dados exigem uma proteção específica.

Em relação a tais dados, é importante destacar dois pontos de atenção para o mercado de pagamentos, como salienta Felipe Schvartzman[32]:

> Primeiro, os dados financeiros, por si, não são considerados dados sensíveis. Embora possa haver algum senso popular de que informações como salários, transações bancárias, dados transacionais e lançamentos na fatura do cartão de crédito seriam dados "sensíveis", a LGPD não os reconhece com esse status em princípio.
>
> Em segundo lugar, vale registrar que os dados biométricos compõem o rol de dados sensíveis previsto na lei. Assim, à medida que alguns serviços lançam mão de soluções de pagamento com o uso de biometria, tais situações passam a atrair o conjunto de regras mais protetivas para o tratamento de dados sensíveis.

A LGPD estabelece uma proteção especial em relação a tais dados, ao determinar hipóteses mais limitadas para seu tratamento (inexistindo, por exemplo, a possibilidade de tratamento de dados pessoais sensíveis com base em legítimo interesse do controlador ou de terceiros) e ao exigir que, nos casos em que a base legal para tratamento de tais dados seja o consentimento, este seja específico e destacado.

2.3 Agentes de tratamento de dados pessoais

A norma define, ainda, duas categorias de agentes de tratamento de dados pessoais: o controlador (a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões sobre o tratamento de dados pessoais) e o operador (a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados em nome do controlador).

Como não poderia deixar de ser, é sobre o controlador que recai a maior parte do ônus regulatório estabelecido pela LGPD, haja vista que este é o agente responsável pela tomada de decisões sobre o tratamento de dados – entre as quais vale destacar a decisão quanto ao enquadramento de cada operação de tratamento de dados em pelo menos uma das bases legais previstas na norma.

---

[31] VAINZOF, Rony. Comentários ao art. 5º. In: MALDONADO, Viviane Nobrega; BLUM, Renato Opice (Coord.). **LGPD**: Lei Geral de Proteção de Dados comentada, 2ª ed. São Paulo: RT, 2019. p. 92.

[32] SCHVARTZMAN, Felipe. Lei Geral de Proteção de Dados Pessoais e riscos cibernéticos: coexistência de normas no mercado de meios de pagamento. In: COHEN, Gabriel Luiz Schvartzman (Coord.). **Direito dos Meios de Pagamento**. São Paulo: Quartier Latin, 2020, p. 389.

Não obstante, a norma também impõe certas obrigações para os operadores, sendo que a principal é realizar o tratamento em consonância com as normas de proteção de dados e apenas nos limites das determinações do controlador.

2.4 Tratamento de dados pessoais

Para fins da LGPD, tratamento é toda e qualquer operação realizada com dados pessoais, adotando-se, mais uma vez, um conceito expansionista. Assim, a norma não traz um rol taxativo de operações de tratamento de dados, mas exemplifica algumas hipóteses de tratamento, quais sejam: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração de dados pessoais.

Novamente, a definição adotada é bastante semelhante àquela constante no GDPR, que define tratamento como "operação ou conjunto de operações efetuada sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados", passando, então a um rol exemplificativo de operações de tratamento.

Ainda, a LGPD dispõe que as atividades de tratamento de dados pessoais devem observar a boa-fé e uma série de princípios, quais sejam:

a) finalidade, segundo o qual o tratamento somente pode ocorrer para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
b) adequação, exigindo-se que o tratamento seja compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
c) necessidade, devendo o tratamento limitar-se ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
d) livre acesso, sendo garantido aos titulares a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

e) qualidade dos dados, de acordo com o qual deve ser garantida aos titulares a exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

f) transparência, sendo necessário garantir aos titulares informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

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

h) prevenção, sendo necessário adotar medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

i) não discriminação, ficando vedada a realização do tratamento para fins discriminatórios ilícitos ou abusivos; e

j) responsabilização e prestação de contas, de acordo com o qual o agente de tratamento de dados fica obrigado a demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, até mesmo, da eficácia dessas medidas.

2.5 Bases legais para tratamento

A história nos mostra que a proteção de dados pessoais tem sido interpretada como o direito de o titular das informações autodeterminar seus dados pessoais, como aponta Bruno Ricardo Bioni[33]. A este respeito, Felipe Schvartzman destaca que:

> Ao longo do tempo, a perspectiva de que o próprio titular deve ter controle sobre os seus dados pessoais, durante todo o fluxo da informação, tornou-se a tônica das leis de proteção de dados pessoais pelo mundo, o que se traduziu, em regra, pela técnica de se exigir o consentimento para que os dados sejam coletados, armazenados, processados e compartilhados. A partir de então, adotou-se como parâmetro normativo a ciência do usuário, seguida da sua escolha em permitir ou barrar a coleta, tratamento, uso e transmissão de dados pessoais, sob pena de tal prática ser ilícita.[34]

---

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

[34] SCHVARTZMAN, Felipe. Lei Geral de Proteção de Dados Pessoais e riscos cibernéticos: coexistência de normas no mercado de meios de pagamento. In: COHEN, Gabriel Luiz Schvartzman (Coord**.). Direito dos Meios de Pagamento**. São Paulo: Quartier Latin, 2020, p. 392.

No ordenamento jurídico brasileiro pré-LGPD, as normas que tangenciavam o tema da proteção de dados pessoais também se centravam no consentimento como a base legal que autorizava o tratamento de dados pessoais, "relegando algumas situações à margem da lei, mesmo quando o consentimento não deveria ser necessário ou mesmo desejável", como salienta o já mencionado Felipe Schvartzman[35].

Não se pode esquecer que a força motriz de nossa economia é a atividade empresária e que, ao reduzirmos seu desempenho, por qualquer razão, impacta-se toda uma cadeia de *stakeholders* – assim, a implementação de uma norma geral de proteção de dados pessoais não deve ser um entrave ao empreendedorismo e sim um mecanismo para que a atividade empresarial se desenvolva com maior segurança jurídica, como ressaltam Ricardo Oliveira e Márcio Cots[36].

A LGPD reconhece este cenário, ao acolher como um dos princípios da disciplina da proteção de dados pessoais no Brasil o desenvolvimento econômico e tecnológico e a inovação, bem como a livre iniciativa e a livre concorrência e ao prever uma série de bases legais que autorizam o tratamento de dados pessoais sem a necessidade de obtenção do consentimento do titular.

Ao todo, além do consentimento, a norma prevê nove outras hipóteses para o tratamento de dados pessoais e sete outras para o tratamento de dados pessoais sensíveis.

Vale ressaltar que, conforme salienta Marcel Leonardi, é muito importante compreender que não existe hierarquia entre as bases legais, uma vez que todas possuem a mesma importância e podem ser utilizadas, sem a prevalência ou sobreposição de qualquer uma delas em relação às outras. Dessa forma, cabe ao controlador avaliar as bases legais disponíveis e definir aquela que é mais apropriada em cada caso, considerando as finalidades do tratamento[37].

A correta definição da base legal mais adequada para cada operação de tratamento de dados pessoais possui grande relevância, haja vista que optar por uma base legal quando outra

---

[35] SCHVARTZMAN, Felipe. Lei Geral de Proteção de Dados Pessoais e riscos cibernéticos: coexistência de normas no mercado de meios de pagamento. In: COHEN, Gabriel Luiz Schvartzman (Coord.). **Direito dos Meios de Pagamento**. São Paulo: Quartier Latin, 2020, p. 393.

[36] OLIVEIRA, Ricardo; COTS, Márcio. **O legítimo interesse e a LGPDP**: Lei Geral de Proteção de Dados Pessoais. 1ª ed. São Paulo: RT, 2020. p. 24.

[37] LEONARDI, Marcel. Legítimo Interesse. In: **Revista do Advogado**, nº 144. Novembro, 2019, Lei Geral de Proteção de Dados Pessoais, p. 69.

seria mais apropriada pode gerar ônus indesejados pelo controlador. Por esta razão, é necessário compreender o escopo de cada uma das bases legais disponíveis.

Passa-se, então, a discorrer sobre aquelas que são consideradas as bases legais de maior interesse para as instituições de pagamento, quais sejam: o consentimento, o cumprimento de obrigação legal ou regulatória, a execução de contrato ou de procedimentos preliminares a pedido do titular e o legítimo interesse do controlador ou de terceiros, sendo que esta última base legal será tratada em um capítulo específico.

2.5.1 Consentimento

De acordo com a definição constante no art. 5º, XII, da LGPD, o consentimento é a manifestação livre, informada e inequívoca por meio da qual o titular concorda com o tratamento de seus dados pessoais, para uma finalidade determinada.

Conforme salienta Caio César Carvalho Lima, a norma não especifica o que se deve compreender como "livre, informado e inequívoco", mas é possível fazê-lo, com fundamento, especialmente, na interpretação de tais conceitos a partir do GDPR[38] – especificamente das Diretrizes 05/2020 do Comitê Europeu para a Proteção de Dados, que tratam do consentimento[39].

Segundo tais diretrizes, "livre" implica que efetivamente haja escolha e manifestação do controle dos dados pessoais pelo titular, sem vícios de vontade, sendo possível recusá-lo ou revogá-lo sem que isso lhe cause prejuízo – caso o consentimento esteja vinculado a uma parte não negociável de um contrato, presume-se que este não foi livre.

Para que o consentimento seja "informado", é necessário fornecer informações aos titulares dos dados antes de se obter o consentimento, para que estes possam tomar decisões informadas, cientes daquilo com que estão a concordar e exercer os direitos que lhe são assegurados, tais como o de revogar o consentimento posteriormente – para fins da LGPD, Caio César Carvalho Lima indica que devem ser apresentadas, no mínimo, as informações listadas

---

[38] LIMA, Caio César Carvalho. Do tratamento de dados pessoais. In: MALDONADO, Viviane Nobrega; BLUM, Renato Opice (Coord.). **Comentários ao GDPR**: Regulamento Geral de Proteção de Dados da União Europeia, 2ª ed. São Paulo: RT, 2019. p. 179-180.

[39] COMITÊ EUROPEU PARA A PROTEÇÃO DE DADOS. Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679. 04 maio 2020. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pt.pdf. Acesso em: 20 jun. 2021.

nos incisos do art. 9º: finalidade específica do tratamento; forma e duração do tratamento, observados os segredos comercial e industrial; identificação do controlador; informações de contato do controlador; informações referentes ao uso compartilhado de dados pelo controlador e a finalidade; responsabilidades dos agentes que realizarão o tratamento; e direitos do titular[40].

"Inequívoco", por sua vez, é aquele consentimento manifestado por meio de uma clara declaração de vontade – a qual pode ser demonstrada por escrito ou por qualquer outro meio, conforme art. 8º da LGPD, sendo que caso o consentimento seja fornecido por escrito, este deve constar de cláusula destacada das demais cláusulas contratuais, nos termos do § 1º de tal artigo – havendo a obrigação de consentimento destacado e específico também em relação ao consentimento para o tratamento de dados pessoais sensíveis, conforme art. 11, I, que ressalta ainda a necessidade de definição de finalidades específicas.

Devido aos requisitos definidos pela norma para que o consentimento seja válido, esta é a base legal que mais exige a interação entre o controlador e o titular dos dados – usualmente mediante a aceitação de termos de uso, contratos, políticas de privacidade, avisos de coleta de *cookies* e outros documentos, como destaca Felipe Schvartzman. Sem prejuízo, esta base legal também pode ser utilizada para autorizar o tratamento de dados pessoais nos casos em que o controlador não possuir uma relação direta com o titular dos dados, na hipótese de um segundo controlador utilizar o consentimento específico para compartilhamento de dados pessoais coletado pelo controlador originário, conforme salienta o autor[41].

Embora esta seja uma base legal de grande relevância, nem sempre o consentimento será a base legal mais adequada, uma vez que pode haver outra mais apropriada para o tratamento em questão, como ressaltam Mario Viola e Chiara Spadaccini de Teffé[42].

Para avaliar qual a base legal mais adequada para determinada operação de tratamento de dados, o controlador deve levar dois pontos em consideração, segundo Felipe Schvartzman:

> Em primeiro lugar, diante da adjetivação que acompanha o conceito de consentimento na LGPD (*livre, informado e inequívoco*), o descumprimento dos requisitos legais pode tornar a autorização do titular inválida. De forma específica, a lei prevê que o consentimento deve referir-se a finalidades determinadas, de modo que as autorizações genéricas serão consideradas nulas

---

[40] LIMA, Caio César Carvalho. Do tratamento de dados pessoais. In: MALDONADO, Viviane Nobrega; BLUM, Renato Opice (Coord.). **Comentários ao GDPR**: Regulamento Geral de Proteção de Dados da União Europeia, 2ª ed. São Paulo: RT, 2019. p. 181.

[41] SCHVARTZMAN, Felipe. Lei Geral de Proteção de Dados Pessoais e riscos cibernéticos: coexistência de normas no mercado de meios de pagamento. In: COHEN, Gabriel Luiz Schvartzman (Coord.). **Direito dos Meios de Pagamento**. São Paulo: Quartier Latin, 2020, p. 394-395.

[42] VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11º. In: BIONI, Bruno et al (Coords.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Grupo GEN, 2020, p. 133.

> (art. 8º, § 4º). Como a LGPD, portanto, impõe requisitos e exige uma qualificação necessária para o consentimento não ser considerado nulo, é natural que despontem discussões em torno da validade das autorizações obtidas por titulares de dados.
>
> Em segundo lugar, mesmo que o consentimento seja válido, ele pode ser revogado a qualquer tempo, mediante manifestação expressa do titular dos dados, por procedimento que deve ser gratuito e facilitado (art. 8º, §5º). Ainda que possa haver eventual abuso do titular, a ser avaliado por ocasião da revogação, a retirada da manifestação de vontade do titular pode impedir o controlador de dados de realizar uma atividade de tratamento baseada no consentimento[43].

Assim, a escolha do consentimento como base legal para o tratamento implica ônus ao controlador, que deverá implementar uma sistemática de governança de dados que lhe permita demonstrar que foi obtido um consentimento válido (o que, em certos casos, pode não ser possível), e também uma certa insegurança jurídica, haja vista que uma eventual revogação do consentimento poderia causar dificuldades operacionais, chegando a, em determinados casos, obstar a execução de um serviço ou o cumprimento de uma obrigação regulatória.

Por estas razões, existem situações em que o consentimento não deve ser a base legal adotada para o tratamento de dados pessoais.

2.5.2 Cumprimento de obrigação legal ou regulatória

A segunda base legal constante no rol do art. 7º da LGPD, o cumprimento de obrigação legal ou regulatória pelo controlador, é de grande importância para instituições de pagamento, que, conforme salienta Felipe Schvartzman[44], estão sujeitas a intensa regulação, devido à qual uma série de deveres lhes são impostos, sendo que muitas vezes o cumprimento de referidos deveres pressupõe o tratamento de dados pessoais[45].

Este é caso, por exemplo, da Circular BCB nº 3.978/2020, que dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições autorizadas a funcionar pelo BCB visando à prevenção da utilização do sistema financeiro para a prática dos crimes de “lavagem” ou ocultação de bens, direitos e valores, de que trata a Lei nº 9.613, de 3

---

[43] SCHVARTZMAN, Felipe. Lei Geral de Proteção de Dados Pessoais e riscos cibernéticos: coexistência de normas no mercado de meios de pagamento. In: COHEN, Gabriel Luiz Schvartzman (Coord**.). Direito dos Meios de Pagamento**. São Paulo: Quartier Latin, 2020, p. 395-396.

[44] SCHVARTZMAN, Felipe. Lei Geral de Proteção de Dados Pessoais e riscos cibernéticos: coexistência de normas no mercado de meios de pagamento. In: COHEN, Gabriel Luiz Schvartzman (Coord.). **Direito dos Meios de Pagamento**. São Paulo: Quartier Latin, 2020, p. 397.

[45] Caso seja necessário tratar dados pessoais sensíveis, esta base legal também poderá ser utilizada, considerando o disposto no art. 11, II, da LGPD.

de março de 1998, e de financiamento do terrorismo, previsto na Lei nº 13.260, de 16 de março de 2016.

A norma estabelece, entre outras, a obrigação de adoção, pelas instituições autorizadas, de procedimentos destinados a conhecer seus clientes, mediante procedimentos de identificação, qualificação e classificação realizados a partir da coleta, verificação e validação de informações, de acordo com o perfil de risco do cliente e com a natureza da relação de negócio – devendo armazenar tais informações e mantê-las à disposição do BCB por no mínimo uma década. Há, ainda, disposições semelhantes referentes a procedimentos destinados a conhecer os funcionários, parceiros e prestadores de serviços terceirizados contratados pelas instituições autorizadas.

2.5.3 Execução de contrato ou procedimentos preliminares

Há situações em que certos dados pessoais devem necessariamente ser tratados para que o controlador possa executar obrigações assumidas contratualmente perante o titular dos dados, ou ainda para que possa realizar um procedimento preliminar.

Na indústria de pagamentos, por exemplo, uma instituição de pagamentos emissora de instrumentos de pagamentos pós-pagos necessitará tratar dados pessoais para avaliar a possibilidade de emitir um cartão de crédito para uma determinada pessoa física interessada em contratar seus serviços e definir o limite de crédito que será disponibilizado (um procedimento preliminar à execução do contrato) e, após a celebração do contrato, para a adequada execução dos serviços, o tratamento será necessário para realizar o processamento das transações, encaminhar a fatura para pagamento, entre outras atividades.

Para tais casos, o controlador pode valer-se de uma terceira hipótese que autoriza o tratamento de dados pessoais sem a necessidade de obtenção do consentimento do usuário, prevista no art. 7º, V, da LGPD, que admite a possibilidade de tratamento quando este for necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.

Esta base legal, de acordo com Mario Viola e Chiara Spadaccini de Teffé[46], possui certa semelhança com a hipótese do consentimento, mas há um elemento distintivo marcante,

---

[46] VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11º. In: BIONI, Bruno et al (Coords.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Grupo GEN, 2020, p. 149.

qual seja: o titular dos dados não poderá revogar o seu consentimento e solicitar a exclusão de seus dados, uma vez que o controlador estará autorizado pela LGPD a mantê-los e tratá-los enquanto durar a execução do contrato – na medida em que isto seja necessário para referida execução, sendo certo que, se o contrato ou os procedimentos preliminares puderem ser executados de outra forma e outros meios, menos intrusivos, estiverem disponíveis, outras bases legais devem ser avaliadas, como salienta Felipe Schvartzman[47].

[47] SCHVARTZMAN, Felipe. Lei Geral de Proteção de Dados Pessoais e riscos cibernéticos: coexistência de normas no mercado de meios de pagamento. In: COHEN, Gabriel Luiz Schvartzman (Coord.). **Direito dos Meios de Pagamento**. São Paulo: Quartier Latin, 2020, p. 399.

3 O LEGÍTIMO INTERESSE DO CONTROLADOR OU DE TERCEIROS PARA O TRATAMENTO DE DADOS PESSOAIS

A quarta e última base legal especialmente relevante para as atividades das instituições de pagamento prevista na LGPD é o legítimo interesse do controlador ou de terceiros para o tratamento de dados pessoais.

Antes de debruçarmo-nos sobre a previsão constante na norma, vale trazer à baila a observação de Bruno Ricardo Bioni, Mariana Rielli e Marina Katayama, que destacam que o legítimo interesse, no ordenamento jurídico brasileiro, advém dos debates ocorridos durante os trabalhos preparatórios da LGPD, sendo que até então, este conceito era completamente inédito[48].

Foi somente na fase da segunda consulta pública ao Anteprojeto de Lei de Proteção de Dados Pessoais que despontaram as discussões sobre esta base legal, prevista nas melhores práticas internacionais, como salientam tais autores[49].

Por esta razão, serão apresentadas considerações sobre o legítimo interesse no direito comunitário europeu, cujas normas (entre as quais o GDPR) são, em grande medida, tidas como as melhores práticas internacionais de proteção de dados pessoais. Isto fornecerá um contexto que permitirá a melhor compreensão do legítimo interesse na LGPD – sendo possível a utilização das orientações das autoridades de proteção de dados europeias como referência para interpretação de questões controversas a respeito desta base legal, até que haja orientações da ANPD sobre o tema.

3.1 O legítimo interesse no direito comunitário europeu

O legítimo interesse foi consagrado enquanto base legal para o tratamento de dados pessoais, no âmbito do direito comunitário europeu, quando da edição da Diretiva 95/46/EC do Parlamento Europeu e Conselho da União Europeia, como ressaltam os já mencionados autores

---

[48] BIONI, Bruno; KITAYAMA, Marina; RIELLI, Mariana. **O Legítimo Interesse na LGPD**: quadro geral e exemplos de aplicação. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021. Disponível em: https://conteudo.dataprivacy.com.br/ebook-legitimo-interesse. Acesso em 26 jun. 2021. p. 6.

[49] BIONI, Bruno; KITAYAMA, Marina; RIELLI, Mariana. **O Legítimo Interesse na LGPD**: quadro geral e exemplos de aplicação. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021. Disponível em: https://conteudo.dataprivacy.com.br/ebook-legitimo-interesse. Acesso em 26 jun. 2021. p. 16-17.

Bruno Ricardo Bioni, Mariana Rielli e Marina Katayama[50]. Assim, quando da entrada em vigor do GDPR, em 2018, a figura do legítimo interesse já existia no direito comunitário europeu há décadas.

Entre as hipóteses previstas no art. 7º da referida diretiva, constava a autorização para o tratamento quando este fosse "necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais" do titular dos dados[51].

De acordo com Ricardo Oliveira e Marcio Cots[52], tal diretiva teve como bases as diretrizes da Organização para Cooperação e Desenvolvimento Econômico para a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais[53] e da Convenção 108 do Conselho da Europa[54]

A previsão constante na Diretiva 95/46/EC do Parlamento Europeu e Conselho da União Europeia foi quase que integralmente reproduzida no GDPR, que a revogou. De acordo com o art. 6º, alínea f, da norma ora vigente: o tratamento é lícito nas hipóteses em que é "necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança"[55].

---

[50] BIONI, Bruno; KITAYAMA, Marina; RIELLI, Mariana. **O Legítimo Interesse na LGPD**: quadro geral e exemplos de aplicação. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021. Disponível em: https://conteudo.dataprivacy.com.br/ebook-legitimo-interesse. Acesso em 26 jun. 2021. p. 13.

[51] UNIÃO EUROPEIA. Directiva (UE) nº 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. **Jornal Oficial das Comunidades Europeias**, Luxemburgo, 23 nov. 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT. Acesso em: 26 jun. 2021.

[52] OLIVEIRA, Ricardo; COTS, Márcio. **O legítimo interesse e a LGPDP**: Lei Geral de Proteção de Dados Pessoais. 1ª ed. São Paulo: RT, 2020. p. 246-247.

[53] De acordo com o art. 7º de tais diretrizes, em uma tradução livre, deve haver limites à coleta de dados pessoais e tais dados devem ser obtidos por meios legais e justos, e, quando apropriado, com o conhecimento ou consentimento do titular dos dados e, de acordo com art. 8º, os dados devem ser relevantes para as finalidades para os quais serão coletados (ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT. Guidelines on the Protection of Privacy and Transborder Flows of Personal, of September 23rd, 1980. 23 set. 1980. Disponível em: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Acesso em 26 jun. 2021).

[54] Nos termos de seu art. 5º, alínea a, em uma tradução livre, os dados pessoais passíveis de tratamento automatizado devem ser obtidos e tratados de forma justa e lícita. (COUNCIL OF EUROPE. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. **European Treaty Series**. Estrasburgo. 28 jan. 1981. Disponível em https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37. Acesso em 26 jun. 2021.)

[55] UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de

Embora não tenha inovado de forma substancial quanto à previsão da possibilidade de tratamento com base no legítimo interesse, o GDPR inovou em relação à norma anterior, ao trazer critérios para aplicação desta base legal que vão além da ponderação entre os interesses legítimos do controlador ou de terceiros em relação aos interesses ou direitos e liberdades fundamentais do titular dos dados[56]. Resumidamente, a norma estabelece os seguintes requisitos:

a) existência de expectativas razoáveis dos titulares de dados pessoais quanto à realização do tratamento, baseadas na relação entre o titular e o controlador[57];
b) realização de uma criteriosa avaliação quanto à possibilidade razoável de o titular dos dados prever, no momento e no contexto em que os dados pessoais são coletados, que esses poderão vir a ser tratados com a finalidade em questão[58];
c) informar ao titular quais são os interesses legítimos do controlador ou de terceiros que justificam o tratamento para uma determinada finalidade.

Contudo, vale destacar que o "texto duro" do GDPR não contém previsão expressa da obrigatoriedade de documentação do teste de ponderação do legítimo interesse – somente suas considerandas (diretrizes para sua interpretação, que apresentam a racionalidade da norma) apresentam os elementos que devem ser levados em consideração para tal ponderação, como bem aponta Bruno Ricardo Bioni[59]. Sem prejuízo, há entendimentos doutrinários no sentido de

---

Dados). **Jornal Oficial da União Europeia**, Bruxelas, 04 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=PT. Acesso em: 17 jun. 2021.

[56] Conforme ressalta Bruno Ricardo Bioni, a antiga diretiva não detalhava os critérios para sua aplicação, o que acarretou: "a) ausência de uma aplicação harmônica e consistente de tal base legal entre os países do antigo bloco econômico europeu. Isso porque cada um deles estabeleceu regras e leituras distintas do legítimo interesse; e b) o risco de o âmbito de aplicação das outras bases legais ser esvaziado, na medida em que o legítimo interesse poderia ser visto como aquela menos restritiva que as demais." Neste cenário, o Grupo de Trabalho do Artigo 29, órgão de aconselhamento criado pela diretiva, que congregava representantes das autoridades de proteção de dados pessoais de todos os países membros da União Europeia (posteriormente substituído pelo Comitê Europeu de Proteção de Dados), formulou um parecer sobre o legítimo interesse, que estabeleceu critérios para a aplicação de tal base legal, com o objetivo de "a) trazer previsibilidade e segurança jurídica na aplicação desta base em todo o bloco europeu, evitar que o legítimo interesse fosse uma porta aberta para contornar os direitos e princípios da diretiva, em especial as outras bases legais para o tratamento de dados". (BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2ª ed. Rio de Janeiro: Forense, 2020. p. 233)

[57] De acordo com a consideranda 47, "poderá haver um interesse legítimo, por exemplo, quando existir uma relação relevante e apropriada entre o titular dos dados e o responsável pelo tratamento, em situações como aquela em que o titular dos dados é cliente ou está ao serviço do responsável pelo tratamento".

[58] Ainda de acordo com a consideranda 47, "os interesses e os direitos fundamentais do titular dos dados podem, em particular, sobrepor-se ao interesse do responsável pelo tratamento, quando que os dados pessoais sejam tratados em circunstâncias em que os seus titulares já não esperam um tratamento adicional."

[59] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2ª ed. Rio de Janeiro: Forense, 2020. p. 245.

que tal documentação é obrigatória, como consequência lógica do princípio da responsabilidade[60], como apontam Irene Kamara e Paul De Heart[61].

Além de apresentar tais requisitos, o GDPR apresenta também alguns exemplos de hipóteses em que se admite a aplicação do legítimo interesse como base legal para o tratamento de dados pessoais, quais sejam:

a) tratamento realizado com a finalidade de prevenção e controle de fraudes;
b) tratamento de dados pessoais realizado para fins de marketing direto;
c) tratamento realizado "na medida estritamente necessária e proporcionada" para assegurar a segurança da rede e das informações em relação a uma rede ou sistema informático, bem como a segurança dos serviços conexos oferecidos ou acessíveis através destas redes e sistemas; e
d) transmitir dados pessoais no âmbito do grupo de empresas para fins administrativos internos, incluindo o tratamento de dados pessoais de clientes ou funcionários – desde que observadas as regras referentes a transferências internacionais, se aplicável.

3.2 O legítimo interesse no direito brasileiro

De acordo com o art. 7º, IX, da LGPD, o tratamento de dados pessoais pode ser realizado quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Esta base legal é detalhada no art. 10 da norma, o qual prevê que sua utilização somente poderá ocorrer para fundamentar o tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam, ao apoio e promoção de atividades do controlador; a proteção, em relação ao titular, do exercício regular

---

[60] Conforme art. 5º, 2, o responsável pelo tratamento é responsável pelo cumprimento dos princípios previstos no art.5º, 1 (licitude, lealdade, transparência, limitação das finalidades, minimização dos dados, exatidão, limitação da conservação, integridade e confidencialidade), e precisa poder comprovar referido cumprimento.
[61] Em uma tradução livre, os autores indicam que, com a introdução do princípio da prestação de contas e do elemento da demonstração, o controlador fica obrigado a documentar sua decisão de adotar a base legal do legítimo interesse (e sua justificativa para tanto), não apenas no momento da decisão, mas enquanto utilizar tal base legal para justificar o tratamento". (KAMARA, Irene; DE HERT, Paul. Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach**. Brussels Privacy Hub Working Paper**, v. 4, n. 12, ago. 2018. Disponível em: https://ssrn.com/abstract=3228369. Acesso em 27 jun. 2021. p. 15.

de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos da LGPD.

Nota-se, portanto, que o adjetivo "legítimo" é utilizado para qualificar tanto as finalidades do tratamento quanto a base legal ora analisada. A respeito da utilização do termo, Bruno Ricardo Bioni, Marina Kitayama e Mariana Rielli apontam que embora a terminologia seja a mesma, as funções exercidas são diferentes:

> No primeiro caso, seu significado serve a uma análise mais restrita: a atividade de tratamento de dados em questão não deve ser vedada por lei ou norma infralegal. Já no segundo caso, o termo funcionaliza uma análise de aderência às condicionantes contidas no artigo 10 para que um interesse possa ser considerado legítimo. É recomendável levar em consideração tal distinção de escopo e alcance do termo[62].

Os parágrafos de tal artigo determinam, ainda, que somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados com fundamento no legítimo interesse do controlador, o qual deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse, sendo possível que, nestes casos, a ANPD solicite ao controlador relatório de impacto à proteção de dados pessoais[63], observados os segredos comercial e industrial.

Não há, contudo, uma definição do que seria "legítimo interesse". Segundo Marcela Joelsons, "esse hiato conceitual foi trazido de forma proposital pelas autoridades legislativas, visando manter a fundamentação jurídica do legítimo interesse do controlador com significado amplo, flexível e com aplicação concreta", viabilizando a manutenção de "seu caráter casuístico e maleável para que possa abarcar situações infindáveis que não poderiam ser previstas uma a uma na lei"[64].

Não obstante, segundo Laura Schertel Mendes, "tal cláusula não deve ser lida como uma válvula de escape geral, a partir da qual qualquer tratamento de dados pessoais passa a ser

---

[62] BIONI, Bruno; KITAYAMA, Marina; RIELLI, Mariana. **O Legítimo Interesse na LGPD**: quadro geral e exemplos de aplicação. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021. Disponível em: https://conteudo.dataprivacy.com.br/ebook-legitimo-interesse. Acesso em 26 jun. 2021. p. 22.

[63] Conforme art. 5º, XVII, trata-se de documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

[64] JOELSONS, Marcela. O legítimo interesse do controlador no tratamento de dados pessoais e o teste de proporcionalidade europeu: desafios e caminhos para uma aplicação no cenário brasileiro. **Revista de Direito e as Novas Tecnologias**, v. 8/2020, p. 1-26, jul. - set. 2020. Disponível em: https://revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad6adc50000017a5a0f5e2cbc441364&docguid=I924c2dd0e10a11eaad20d1cf72cae2ef&hitguid=I924c2dd0e10a11eaad20d1cf72cae2ef&spos=3&epos=3&td=3&context=84&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1. Acesso em 29 jun. 2021. (Paginação da versão eletrônica difere da versão impressa). p. 13.

autorizada", sendo necessário que o controlador pondere os interesses e direitos envolvidos e que, uma vez que se conclua que há um legítimo interesse, uma série de requisitos especiais devem ser observados. "Uma eventual interpretação por demais ampla da cláusula do legítimo interesse acabaria por descreditar a própria regra, além de pôr em xeque a sua constitucionalidade, por violação ao direito fundamental à intimidade e vida privada", de acordo com ela [65].

Neste sentido, Bruno Ricardo Bioni, Marina Kitayama e Mariana Rielli ressaltam que o legítimo interesse pode não ser uma base legal "vantajosa" para o controlador, haja vista que os requisitos estabelecidos pela LGPD para a se garantir a aplicabilidade do legítimo interesse claramente criam um ônus argumentativo reforçado em relação a alguns dos princípios da legislação, como finalidade, necessidade e transparência[66].

Ademais, segundo a já mencionada autora Marcela Joelsons:

> (...) a Autoridade Nacional terá papel fundamental na implementação da Lei Geral de Proteção de Dados, pois garantirá a aplicação da lei às circunstâncias fáticas com segurança jurídica, elaborando normas, regulamentos e orientações sobre a interpretação da nova legislação. Além disso, poderá estabelecer parâmetros para a aplicação da Lei em cada setor ou mercado em respeito às características e aos diferenciais de cada atividade, objetivando que as ações sejam mais eficazes e respeitem os direitos fundamentais dos titulares e dos agentes econômicos.
>
> A Autoridade Nacional deverá garantir a desburocratização e o esclarecimento sobre a existência do legítimo interesse do controlador em casos concretos e de acordo com os setores e players que utilizam comumente os dados em suas atividades empresariais, de modo célere e desjudicializado. Caberá também a esse órgão a verificação da ocorrência de abusos de direito e contrariedade aos valores maiores do ordenamento jurídico, com a aplicação das competentes sanções.[67]

Desta feita, é importante monitorar as atividades da ANPD, para que se possa identificar os posicionamentos do órgão a respeito de tal base legal.

---

[65] MENDES, Laura Schertel. Marco jurídico para a cidadania digital: uma análise do projeto de lei 5.276/2016. **Revista de Direito Civil Contemporâneo**, v. 9/2016, p. 1-11, 2016. Disponível em:https://revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad6adc60000017a59fb751882d39242&docguid=I2a8eb400a3a711e69ab7010000000000&hitguid=I2a8eb400a3a711e69ab7010000000000&spos=1&epos=1&td=1&context=16&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1. Acesso em 29 jun. 2021. (Paginação da versão eletrônica difere da versão impressa). p. 6-7.

[66] BIONI, Bruno; KITAYAMA, Marina; RIELLI, Mariana. **O Legítimo Interesse na LGPD**: quadro geral e exemplos de aplicação. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021. Disponível em: https://conteudo.dataprivacy.com.br/ebook-legitimo-interesse. Acesso em 26 jun. 2021. p. 28.

[67] JOELSONS, Marcela. O legítimo interesse do controlador no tratamento de dados pessoais e o teste de proporcionalidade europeu: desafios e caminhos para uma aplicação no cenário brasileiro. **Revista de Direito e as Novas Tecnologias**, v. 8/2020, p. 1-26, jul. - set. 2020. Disponível em: https://revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad6adc50000017a5a0f5e2cbc441364&docguid=I924c2dd0e10a11eaad20d1cf72cae2ef&hitguid=I924c2dd0e10a11eaad20d1cf72cae2ef&spos=3&epos=3&td=3&context=84&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1. Acesso em 29 jun. 2021. (Paginação da versão eletrônica difere da versão impressa). p. 16-17.

3.3 Teste de ponderação do legítimo interesse

Como destacam Bruno Ricardo Bioni, Marina Kitayama e Mariana Rielli, o teste de ponderação do legítimo interesse aplicado no contexto do RGPD (também conhecido como "LIA", do inglês *legitimate interest assessment)* possui variações quanto a sua estruturação – há versões que subdividem o teste em três fases (como a do *Information Commissioner Office* do Reino Unido[68]) e outras que determinam a existência de quatro fases (como a do antigo Grupo de Trabalho do Artigo 29[69])[70].

Independente da estrutura adotada, o propósito de tal teste é buscar um equilíbrio entre os interesses envolvidos, quais sejam, o do titular dos dados e o do controlador que deseja tratar suas informações (ou de terceiros), buscando, como destaca Marcela Joelsons, uma forma eficaz de solucionar este impasse, "que consiga englobar a proteção da privacidade do titular dos dados e ao mesmo tempo permita a circulação das informações que são essenciais para o mercado econômico"[71].

Considerando a forma como a LGPD regulou o legítimo interesse, é possível afirmar que a estrutura do teste de ponderação nela prevista pode ser dividida em quatro fases, as quais podem ser segmentadas em duas etapas, de acordo com Bruno Ricardo Bioni:

> A primeira, que compreende as três primeiras fases, em que quem vai fazer o juízo de valor da legitimidade do interesse é o controlador e/ou terceiro. A segunda, que é onde está alocada a quarta fase, para que haja uma espécie de contraditório e ampla defesa por parte do próprio titular e entidades representativas do seu interesse. Esse último momento do teste cumpre uma função de extrema importância que é assegurar voz à outra parte cujo interesse

---

[68] De acordo com parecer do órgão, o teste de ponderação compreende a fase de teste da finalidade, da necessidade e do balanceamento. (UK INFORMATION COMMISSIONER Office. Guide to the General Data Protection Regulation (GDPR). 02 ago. 2018. Disponível em: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf. Acesso em 30 jun. 2021. p. 82.)

[69] De acordo com o posicionamento do órgão, a avaliação deve levar em consideração diversos fatores, que podem ser agrupados em quatro fases, quais sejam, a avaliação do legítimo interesse, do impacto sobre os titulares dos dados, o equilíbrio provisório e salvaguardas adicionais implementadas para prevenção de impacto indevido. (ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion on 06/24 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. Disponível em: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Acesso em 30 jun. 2021. p. 33.)

[70] BIONI, Bruno; KITAYAMA, Marina; RIELLI, Mariana. **O Legítimo Interesse na LGPD**: quadro geral e exemplos de aplicação. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021. Disponível em: https://conteudo.dataprivacy.com.br/ebook-legitimo-interesse. Acesso em 26 jun. 2021. p. 39.

[71] JOELSONS, Marcela. O legítimo interesse do controlador no tratamento de dados pessoais e o teste de proporcionalidade europeu: desafios e caminhos para uma aplicação no cenário brasileiro. **Revista de Direito e as Novas Tecnologias**, v. 8/2020, p. 1-26, jul. - set. 2020. Disponível em: https://revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad6adc50000017a5a0f5e2cbc441364&docguid=I924c2dd0e10a11eaad20d1cf72cae2ef&hitguid=I924c2dd0e10a11eaad20d1cf72cae2ef&spos=3&epos=3&td=3&context=84&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1. Acesso em 29 jun. 2021. (Paginação da versão eletrônica difere da versão impressa). p. 14.

> deve ser sopesado ao do agente de tratamento de dados, em linha com um dos fundamentos da LGPD: a autodeterminação informacional.
>
> (...)
>
> O mérito dessa divisão é arquitetar um circuito decisório que considera não apenas o juízo de valor a ser realizado pelo agente de tratamento de dados, mas, também, pelo próprio titular ou representantes de seu direito. Daí a importância em ter uma fase dedicada a destacar e reforçar os princípios que dariam voz a quem deve ter seus interesses sopesados. Por fim, destaca-se, ainda, que esses quatro passos refletem exatamente a estrutura do art. 10 e a escolha do legislador brasileiro em não fazer um transplante legal daquilo que vinha sendo desenvolvido, com algumas variações, no contexto europeu. (...)[72].

A primeira de tais fases seria a verificação da legitimidade do interesse, conforme art. 10 *caput* e I da LGPD, sendo necessário avaliar se a finalidade (razão) para a qual se deseja realizar o tratamento é legítima (lícita) e se o interesse (o benefício advindo do tratamento) está devidamente consubstanciado em uma situação concreta, de acordo com o já mencionado autor Bruno Ricardo Bioni[73] – caso a finalidade seja vedada por lei ou norma infralegal, ou o interesse seja meramente especulativo (e assim, não específico), deve-se concluir pela não aplicabilidade de tal base legal.

A segunda, de acordo com tal autor, seria a análise da necessidade do tratamento, nos termos do art. 10, §1º, da norma. Neste momento, deve-se avaliar se os dados que se pretende tratar de fato são necessários para que se alcance a finalidade desejada (ou seja, se não há pretensão de tratamento de dados excessivos e se não há outros meios para se alcançar tal finalidade, que sejam menos invasivos e não exijam esforço desproporcional), bem como a necessidade de utilização da base legal do legítimo interesse, ou seja, se não é possível realizar o tratamento com fundamento em outra das bases legais previstas no art. 10 da LGPD[74].

A terceira fase, de acordo com ele, seria a do balanceamento, prevista no art. 10, II, da LGPD. Esta seria a principal fase do teste de proporcionalidade e nela devem ser avaliadas a compatibilidade entre o tratamento pretendido e as legítimas expectativas do titular dos dados, considerando a finalidade para a qual os dados foram inicialmente tratados[75]. Esta necessidade de compatibilidade está diretamente relacionada à boa-fé, prevista no *caput* do art. 6º da LGPD

---

[72] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 3ª ed. Rio de Janeiro: Forense, 2021. p. 243-244.
[73] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2ª ed. Rio de Janeiro: Forense, 2020. p. 236.
[74] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2ª ed. Rio de Janeiro: Forense, 2020. p. 236-237.
[75] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2ª ed. Rio de Janeiro: Forense, 2020. p. 237.

como um norte para os demais princípios, segundo Bruno Ricardo Bioni, Marina Kitayama e Mariana Rielli.[76]

A boa-fé objetiva, de acordo com Judith Costa-Martins, consiste em nada mais que um "modelo de conduta social, arquétipo ou standard jurídico, segundo o qual cada pessoa deve ajustar a própria conduta a esse arquétipo, obrando como obraria um homem reto: com honestidade, lealdade, probidade"[77].

Ao fazer menção a tal conceito, "o legislador brasileiro amarrou duplamente os conceitos jurídico-indeterminados da legítima expectativa e do legítimo interesse a um elemento bastante tradicional da cultura jurídica brasileira.", conforme apontam Bruno Ricardo Bioni, Marina Kitayama e Mariana Rielli.[78]

Ainda na terceira fase, deve-se avaliar a forma como os titulares dos dados pessoais que se pretende tratar serão impactados, em especial no que diz respeito a eventuais repercussões negativas sobre seus direitos e liberdades fundamentais. É pertinente, em relação a tal avaliação, fazer menção ao entendimento do Grupo de Trabalho do Artigo 29, segundo o qual é necessário levar em consideração as consequências positivas e as negativas do tratamento pretendido – as quais podem incluir potenciais decisões ou ações futuras por parte de terceiros, bem como situações em que tratamento possa levar à exclusão ou à discriminação de pessoas e à difamação ou, de forma mais ampla, situações em que haja o risco de se causar dano à reputação, ao poder de negociação ou à autonomia do titular dos dados[79].

A quarta e última fase do teste de ponderação do legítimo interesse, prevista no art. 10, §§ 2º e 3º da LGPD, consistiria na adoção de salvaguardas para transparência e minimização dos riscos aos titulares dos dados, segundo Bruno Ricardo Bioni. De acordo com o autor:

> Não é porque o legítimo interesse prescinde do consentimento do titular que a atividade de tratamento de dados deve ser opaca. Pelo contrário, reforça-se d.1) o dever de transparência. Objetiva-se, com isso, franquear ao cidadão d.2) poder de tomada de decisão para se opor a tal atividade de tratamento de dados (opt-out), podendo optar por estar fora do que considera ser incompatível com as suas legítimas expectativas. E, por fim. Isso porque a legítima expectativa é também dele titular e é nesse momento que pode levantar a sua voz para controlar seus dados a posteriori, d.3) o controlador

---

[76] BIONI, Bruno; KITAYAMA, Marina; RIELLI, Mariana. **O Legítimo Interesse na LGPD**: quadro geral e exemplos de aplicação. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021. Disponível em: https://conteudo.dataprivacy.com.br/ebook-legitimo-interesse. Acesso em 26 jun. 2021. p. 30.
[77] MARTINS-COSTA, Judith. **A boa-fé no direito privado**. São Paulo: Ed. RT, 1999. p. 24.
[78] BIONI, Bruno; KITAYAMA, Marina; RIELLI, Mariana. **O Legítimo Interesse na LGPD**: quadro geral e exemplos de aplicação. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021. Disponível em: https://conteudo.dataprivacy.com.br/ebook-legitimo-interesse. Acesso em 26 jun. 2021. p. 30.
[79] ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion on 06/24 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. Disponível em: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Acesso em 30 jun. 2021. p. 37.

> deve adotar ações que mitiguem os riscos do titular dos dados (v.g., anonimização dos dados), sendo este o sentido da previsão da eventual necessidade elaboração de relatório de impacto à privacidade na LGPD[80].

Percorridas tais etapas, o controlador deve tomar o cuidado de documentar a realização do teste, para que esteja apto a prestar contas da adoção de tal base legal, em atendimento ao disposto no art. 37 da LGPD.

---

[80] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2ª ed. Rio de Janeiro: Forense, 2020. p. 238.

4 O USO DO LEGÍTIMO INTERESSE COMO BASE LEGAL PARA O TRATAMENTO DE DADOS PESSOAIS NO ÂMBITO DA PRESTAÇÃO DE SERVIÇOS DE PAGAMENTO

O mercado de meios de pagamento é classificado como uma plataforma multilateral, ou um sistema de dois lados, como apontam Claudia Bruschi e Adalto Gonçalves, os quais explicam que:

> Uma plataforma multilateral fornece bens ou serviços a dois ou mais grupos distintos de clientes que precisam uns dos outros de alguma forma e que confiam em uma plataforma para intermediar transações entre eles. Plataformas multilaterais geralmente reduzem os custos de transação e, portanto, facilitam as trocas mutualmente benéficas. Eles [sic] tendem a surgir quando há algum valor em obter múltiplos lados juntos, mas os custos de transação ou outros obstáculos ficam no caminho.[81]

Neste setor, muitas vezes as instituições mantêm relacionamento contratual diretamente com um grupo de clientes, mas não com o outro – o qual, não obstante, usufrui dos benefícios da plataforma, ainda que indiretamente. Assim, instituições de pagamento credenciadoras[82] e instituições subcredenciadoras[83], usualmente, mantêm relação contratual com os usuários recebedores (pessoas jurídicas ou pessoas físicas), ao passo que instituições emissoras de moeda eletrônica[84] e instituições emissoras de instrumentos pós-pagos[85] mantêm relação com os usuários pagadores (pessoas físicas ou jurídicas titulares de contas de pagamento ou de instrumentos pós-pagos, os bem conhecidos cartões de crédito).

---

[81] BRUSCHI, Cláudia. GONÇALVES, Adalto. **Regulação em Meios de Pagamento**: Contratos de Interoperabilidade ou Participação? INSPER. 26 jun. 2018. Disponível em https://www.insper.edu.br/wp-content/uploads/2018/10/Interoperabilidade_ou_Participacao_em_Meios_de_Pagamento.pdf. Acesso em 28 jun. 2021.

[82] Instituição de pagamento que, sem gerenciar conta de pagamento, (i) habilita recebedores para a aceitação de instrumento de pagamento emitido por instituição de pagamento ou por instituição financeira participante de um mesmo arranjo de pagamento; e (ii) participa do processo de liquidação das transações de pagamento como credor perante o emissor, de acordo com as regras do arranjo de pagamento, conforme Resolução BCB nº 80/2021 (art. 3º, III).

[83] Participante do arranjo de pagamento que habilita usuário final recebedor para a aceitação de instrumento de pagamento emitido por instituição de pagamento ou por instituição financeira participante de um mesmo arranjo de pagamento, mas que não participa do processo de liquidação das transações de pagamento como credor perante o emissor, conforme Circular BCB nº 3.682/2013 (art. 2º, VIII).

[84] Instituição de pagamento que gerencia conta de pagamento de usuário final, do tipo pré-paga, disponibiliza transação de pagamento que envolva o ato de pagar ou transferir, com base em moeda eletrônica previamente aportada nessa conta, converte tais recursos em moeda física ou escritural, ou vice-versa, podendo habilitar a aceitação da moeda eletrônica com a liquidação em conta de pagamento por ela gerenciada, conforme Resolução BCB nº 80/2021 (art. 3º, I).

[85] Instituição de pagamento que gerencia conta de pagamento de usuário final pagador, do tipo pós-paga, e disponibiliza transação de pagamento com base nessa conta, conforme Resolução BCB nº 80/2021 (art. 3º, II).

Neste cenário, conforme salienta Felipe Schvartzman,[86] há situações em que o tratamento de dados pessoais será necessário e não será viável que a instituição de pagamentos responsável pelo tratamento colete o consentimento dos titulares de tais dados ou se utilize de outras bases legais para justificá-lo.

Em muitos casos, as instituições de pagamento poderão valer-se das bases legais de execução do contrato ou de procedimentos preliminares a pedido do titular ou cumprimento de obrigação legal ou regulatória, descritas nos subitens do subcapítulo 2.5 deste trabalho, mas, em determinados casos, o tratamento não poderá ser enquadrado em tais bases.

Em situações concretas em que não seja possível a utilização das demais bases legais previstas na LGPD, tais instituições deverão realizar um teste de proporcionalidade do legítimo interesse, para avaliarem a possibilidade de utilização de tal base legal – sendo necessário documentá-lo, para cumprimento de seus deveres de responsabilidade e de prestação de contas.

Assim, tais instituições deverão ponderar, na situação concreta: se a finalidade para a qual os dados pessoais serão tratados é lícita; se o tratamento será adequado para o atendimento da finalidade; se de fato não há outras bases legais aplicáveis (sendo que, neste mercado, será pertinente avaliar com especial cuidado a possibilidade de se utilizar a base legal do cumprimento de obrigação legal ou regulatória); se não há outros meios, menos intrusivos, para se alcançar a finalidade pretendida (que não exijam um esforço desproporcional); quais são as legítimas expectativas do titular em relação ao tratamento de seus dados pessoais; e quais seriam as medidas de mitigação de riscos passíveis de adoção para a garantia dos direitos e liberdades fundamentais dos titulares.

Sem prejuízo da necessidade de avaliação das situações concretas, é possível apresentar alguns exemplos de hipóteses em que a adoção do legítimo interesse como base legal de tratamento, a princípio, pode ser pertinente, tais como: o processamento de uma transferência de recursos[87]; a coleta, o cruzamento e a análise de dados pessoais para a prevenção a fraudes[88];

---

[86] SCHVARTZMAN, Felipe. Lei Geral de Proteção de Dados Pessoais e riscos cibernéticos: coexistência de normas no mercado de meios de pagamento. In: COHEN, Gabriel Luiz Schvartzman (Coord.). **Direito dos Meios de Pagamento**. São Paulo: Quartier Latin, 2020, p. 396.

[87] Aqui, vale destacar que embora possa parecer intuitivo que o processamento de uma transferência de recursos possa ser realizado com fundamento na base legal da execução de contrato a pedido do titular, tal entendimento seria incorreto, haja vista que caso o usuário recebedor seja uma pessoa física, seus dados pessoais serão tratados, mas ele (o titular de tais dados) não terá solicitado a realização da transação à instituição de pagamento.

[88] É pertinente fazer referência à Consideranda 47 do GDPR, que prevê expressamente que "o tratamento de dados pessoais estritamente necessário aos objetivos de prevenção e controlo da fraude constitui igualmente um interesse legítimo do responsável pelo seu tratamento" e a qual é mencionada nas Diretrizes 06/2020 do Comitê Europeu de Proteção de Dados, relativas à sobre a interação entre a Segunda Diretiva Serviços de Pagamento e o RGPD (COMITÊ EUROPEU PARA A PROTEÇÃO DE DADOS. Diretrizes 06/2020 relativas ao consentimento na sobre a interação entre a Segunda Diretiva Serviços de Pagamento e o RGPD.

“os esforços para prevenção de crimes financeiros e usos indevidos de cartões de crédito”, como aponta Felipe Schvartzman[89]; bem como a exigência de cadastro dos clientes para acesso a conteúdos relacionados aos serviços prestados, no âmbito de uma ação de *marketing* que visa a promover as atividades da instituição, como ilustram Bruno Ricardo Bioni, Marina Kitayama e Mariana Rielli[90].

Versão 2.0. 15 dez. 2020. Disponível em: https://edpb.europa.eu/system/files/2021-06/edpb_guidelines_202006_psd2_afterpublicconsultation_pt.pdf. Acesso em: 28 jun. 2021. p. 12).

[89] SCHVARTZMAN, Felipe. Lei Geral de Proteção de Dados Pessoais e riscos cibernéticos: coexistência de normas no mercado de meios de pagamento. In: COHEN, Gabriel Luiz Schvartzman (Coord.). **Direito dos Meios de Pagamento**. São Paulo: Quartier Latin, 2020. p. 401.

[90] BIONI, Bruno; KITAYAMA, Marina; RIELLI, Mariana. **O Legítimo Interesse na LGPD**: quadro geral e exemplos de aplicação. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021. Disponível em: https://conteudo.dataprivacy.com.br/ebook-legitimo-interesse. Acesso em 26 jun. 2021. p. 57.

5 CONCLUSÕES

As atividades da indústria de meios de pagamento como um todo e das instituições de pagamento, especificamente, desenvolvem-se em um cenário de intensa coleta, processamento e compartilhamento de dados pessoais. Por esta razão, normas setoriais anteriores ao advento da LGPD já tangenciavam a temática da proteção de tais dados.

Considerando que a LGPD entrou em vigor no mês de setembro de 2020 e que, a partir de agosto de 2021, a ANPD poderá aplicar sanções administrativas substanciais, é importante avaliar as hipóteses de tratamento de dados pessoais previstas na LGPD, para se identificar quais seriam as bases legais para o tratamento realizado no âmbito das atividades de tais instituições.

A norma estabelece uma série de hipóteses autorizativas para o tratamento de dados pessoais – o consentimento do titular e outras nove hipóteses que o dispensam, entre as quais está o interesse legítimo do controlador ou de terceiros.

A redação da maioria das bases de tratamento previstas na legislação é quase autoexplicativa, mas isto não pode ser dito a respeito do interesse legítimo, uma vez que a terminologia adotada é ampla e carregada de subjetividade – o que faz com que o adequado manejo desta base legal de tratamento de dados pessoais seja um desafio, haja vista que ainda não há orientações da ANPD quanto a sua utilização, inexistindo consenso a respeito de como a norma deve ser interpretada.

Assim, este trabalho se propôs a analisar os limites do legítimo interesse do controlador ou de terceiros para o tratamento de dados pessoais previsto na Lei nº 13.709/2018, para que se pudesse identificar os casos em que o tratamento de dados pessoais pelas instituições de pagamento poderá justificar-se pelo legítimo interesse – ficando dispensada a obtenção do consentimento dos titulares de tais dados (as pessoas físicas às quais os dados dizem respeito).

A LGPD representa não só uma mudança legislativa, mas uma mudança de cultura em relação à tutela da privacidade e dos dados pessoais em nosso país, que deverá observar como fundamentos o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas físicas.

A norma, que foi fortemente inspirada no GDPR, apresenta uma série de conceitos relevantes, tais como o de dados pessoais, o de dados pessoais sensíveis, o de tratamento e o de

agentes de tratamento de dados pessoais – sendo que alguns destes conceitos são novos (como o de dados pessoais sensíveis) e outros já constavam em nosso ordenamento jurídico (como o de dados pessoais, que já constava no Marco Civil da Internet e é bastante semelhante ao adotado no GDPR).

Entre as bases legais previstas na LGPD, é possível apontar cinco como as mais relevantes para as operações de tratamento de dados pessoais desenvolvidas no âmbito das atividades das instituições de pagamento: o consentimento, o cumprimento de obrigação legal ou regulatória, a execução de contrato a pedido do titular dos dados e o legítimo interesse do controlador ou de terceiros.

As discussões sobre a inclusão desta última base legal na norma intensificaram-se na segunda consulta pública ao Anteprojeto de Lei de Proteção de Dados Pessoais, mas o conceito do legítimo interesse já estava previsto há décadas no direito comunitário europeu, cujas normas (entre as quais o GDPR) são, em grande medida, tidas como as melhores práticas internacionais de proteção de dados pessoais – sendo possível a utilização das orientações das autoridades de proteção de dados europeias como referência para interpretação de questões controversas a respeito desta base legal, até que haja orientações da ANPD sobre o tema.

Em tal âmbito, o legítimo interesse foi consagrado enquanto hipótese autorizativa para o tratamento de dados pessoais, quando da edição da Diretiva 95/46/EC do Parlamento Europeu e Conselho da União Europeia, que foi substituída pelo GDPR. Nos termos da norma vigente é necessário não só ponderar os interesses dos envolvidos, mas também avaliar a existência de expectativas razoáveis dos titulares de dados pessoais quanto à realização do tratamento, baseadas na relação entre o titular e o controlador, realizar uma criteriosa avaliação quanto à possibilidade razoável de o titular dos dados prever, no momento e no contexto em que os dados pessoais são coletados, que esses poderão vir a ser tratados com a finalidade em questão; e informar ao titular quais são os interesses legítimos do controlador ou de terceiros que justificam o tratamento para uma determinada finalidade – devendo tal avaliação ser formalizada em documento específico, para atendimento do princípio da responsabilidade.

De acordo com a LGPD, o tratamento de dados pessoais pode ser realizado quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais e desde que observados os requisitos previstos no art. 10.

Para avaliar a possibilidade de aplicação desta base legal, o controlador deverá realizar um teste de ponderação. Tal teste compreende quatro etapas: a verificação da legitimidade do interesse (concretude do interesse e da finalidade, bem como a licitude da finalidade); a

necessidade (tanto do tratamento, ou seja, avaliação de quais são os dados que se pretende tratar e da possibilidade de se alcançar a finalidade pretendida por outros meios ou com a utilização de menos dados; quanto da utilização do legítimo interesse como base legal, diante da inexistência de outras bases legais mais apropriadas para a situação concreta); o balanceamento (compatibilidade entre o tratamento pretendido e as legítimas expectativas do titular dos dados, considerando a finalidade para a qual os dados foram inicialmente tratados; bem como a forma como os titulares dos dados pessoais que se pretende tratar serão impactados, em especial no que diz respeito a eventuais repercussões negativas sobre seus direitos e liberdades fundamentais); e a adoção de salvaguardas para transparência e minimização dos riscos aos titulares. Percorridas tais etapas, o controlador deve tomar o cuidado de documentar a realização do teste, para que esteja apto a prestar contas da adoção de tal base legal, em atendimento ao disposto no art. 37 da LGPD.

Por atuarem em uma indústria classificada como uma plataforma multilateral, as instituições de pagamentos muitas vezes mantêm relacionamento contratual diretamente com um grupo de clientes, mas não com o outro – o qual, não obstante, usufrui dos benefícios da plataforma, ainda que indiretamente. Neste cenário, muitas vezes, em situações concretas, o tratamento de dados pessoais será imprescindível e não será viável que a instituição responsável pelo tratamento colete o consentimento dos titulares de tais dados ou se utilize de outras bases legais para justificá-lo.

Nestas situações, conclui-se que as instituições de pagamento deverão realizar o teste de ponderação do legítimo interesse e documentá-lo. Sem prejuízo da necessidade de avaliação caso a caso, é possível apresentar alguns exemplos de hipóteses em que a adoção do legítimo interesse como base legal de tratamento, a princípio, pode ser pertinente, tais como: o processamento de uma transferência de recursos; a coleta, o cruzamento e a análise de dados pessoais para a prevenção a fraudes; os esforços para prevenção de crimes financeiros e usos indevidos de cartões de crédito; bem como a exigência de cadastro dos clientes para acesso a conteúdos relacionados aos serviços prestados, no âmbito de uma ação de marketing que visa a promover as atividades da instituição.

REFERÊNCIAS

ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion on 06/24 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. Disponível em: <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdfhttp://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf>. Acesso em 30 jun. 2021.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. ANPD abre consulta pública sobre norma de fiscalização. 28 maio. 2021. Disponível em https://www.gov.br/anpd/pt-br/assuntos/noticias/confira-linha-do-tempo-com-as-principais-acoes-da-anpd. Acesso em 01 jun. 2021.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Confira linha do tempo sobre principais ações da ANPD. 14 abr. 2021. Disponível em https://www.gov.br/anpd/pt-br/assuntos/noticias/confira-linha-do-tempo-com-as-principais-acoes-da-anpd. Acesso em 01 jun. 2021.

BIONI, Bruno; KITAYAMA, Marina; RIELLI, Mariana. **O Legítimo Interesse na LGPD**: quadro geral e exemplos de aplicação. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021. Disponível em: https://conteudo.dataprivacy.com.br/ebook-legitimo-interesse. Acesso em 26 jun. 2021.

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

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 3ª ed. Rio de Janeiro: Forense, 2021.

BRAGA, Fabio de Almeida. Aplicabilidade da Lei de Sigilo Bancário na Atuação dos Instituidores de Arranjos e das Instituições de Pagamento. In: COHEN, Gabriel Luiz Schvartzman (Coord.). **Direito dos Meios de Pagamento**. São Paulo: Quartier Latin, 2020.

BRUSCHI, Cláudia. GONÇALVES, Adalto. **Regulação em Meios de Pagamento**: Contratos de Interoperabilidade ou Participação? INSPER. 26 jun. 2018. Disponível em https://www.insper.edu.br/wp-content/uploads/2018/10/Interoperabilidade_ou_Participacao_em_Meios_de_Pagamento.pdf. Acesso em 28 jun. 2021.

COMITÊ EUROPEU PARA A PROTEÇÃO DE DADOS. Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pt.pdf. Acesso em: 20 jun. 2021.

COMITÊ EUROPEU PARA A PROTEÇÃO DE DADOS. Diretrizes 06/2020 relativas ao consentimento na sobre a interação entre a Segunda Diretiva Serviços de Pagamento e o RGPD. Versão 2.0. 15 dez. 2020. Disponível em: https://edpb.europa.eu/system/files/2021-06/edpb_guidelines_202006_psd2_afterpublicconsultation_pt.pdf. Acesso em: 28 jun. 2021.

CRESPO, Danilo Leme; FILHO, Dalmo Ribeiro. A evolução legislativa brasileira sobre a proteção de dados pessoais: a importância da promulgação da Lei Geral de Proteção de Dados Pessoais. **Revista de Direito Privado**. v. 98, p. 1-20. mar – abr 2019. Disponível em https://revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad6adc600000179f81daabd6fc295cb&docguid=I98c1d5d04a0611e9b1d8010000000000&hitguid=I98c1d5d04a0611e9b1d8010000000000&spos=2&epos=2&td=102&context=136&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1. Acesso em 10 jun. 2021. (Paginação da versão eletrônica difere da versão impressa).

DOMO, INC. **Data never sleeps 8.0.** Domo, 2020. Disponível em https://www.domo.com/learn/data-never-sleeps-8. Acesso em 06 dez. 2020.

JOELSONS, Marcela. O legítimo interesse do controlador no tratamento de dados pessoais e o teste de proporcionalidade europeu: desafios e caminhos para uma aplicação no cenário brasileiro. **Revista de Direito e as Novas Tecnologias**, v. 8/2020, p. 1-26, jul. - set. 2020. Disponível em: https://revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad6adc50000017a5a0f5e2cbc441364&docguid=I924c2dd0e10a11eaad20d1cf72cae2ef&hitguid=I924c2dd0e10a11eaad20d1cf72cae2ef&spos=3&epos=3&td=3&context=84&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1. Acesso em 29 jun. 2021. (Paginação da versão eletrônica difere da versão impressa)

KAMARA, Irene; DE HERT, Paul. Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach**. Brussels Privacy Hub Working Paper**, v. 4, n. 12, ago. 2018. Disponível em: https://ssrn.com/abstract=3228369. Acesso em 27 jun. 2021.

LEMOS, Ronaldo. O Marco Civil como símbolo do desejo por inovação no Brasil. In: LEITE, George Salomão; LEMOS, Ronaldo (Coord.). **Marco Civil da Internet**. São Paulo: Atlas, 2014.

LEONARDI, Marcel. Legítimo Interesse. In: **Revista do Advogado**, nº 144. Novembro, 2019, Lei Geral de Proteção de Dados Pessoais.

LIMA, Caio César Carvalho. Do tratamento de dados pessoais. In: MALDONADO, Viviane Nobrega; BLUM, Renato Opice (Coord.). **Comentários ao GDPR**: Regulamento Geral de Proteção de Dados da União Europeia, 2ª ed. São Paulo: RT, 2019.

MARTINS-COSTA, Judith. **A boa-fé no direito privado**. São Paulo: Ed. RT, 1999. p. 24.

MENDES, Laura Schertel. Marco jurídico para a cidadania digital: uma análise do projeto de lei 5.276/2016. **Revista de Direito Civil Contemporâneo**, v. 9/2016, p. 1-11, 2016. Disponível em:https://revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad6adc60000017a59fb751882d39242&docguid=I2a8eb400a3a711e69ab7010000000000&hitguid=I2a8eb400a3a711e69ab7010000000000&spos=1&epos=1&td=1&context=16&crumb-

action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1. Acesso em 29 jun. 2021. (Paginação da versão eletrônica difere da versão impressa)

MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor**, v. 79, p. 1-26, 2011. Disponível em: https://revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad6adc60000017a5a98d7c0a617e29d&docguid=I1977b2a0008911e1968d00008558bdfc&hitguid=I1977b2a0008911e1968d00008558bdfc&spos=7&epos=7&td=7&context=294&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1. Acesso em 02 jun. 2021.

NERY JUNIOR, Nelson; Nery, Rosa Maria de Andrade. **Código Civil anotado e legislação extravagante**. 2. ed. rev. e ampl. São Paulo: Ed. RT, 2004.

OLIVEIRA, Ricardo; COTS, Márcio. **O legítimo interesse e a LGPDP**: Lei Geral de Proteção de Dados Pessoais. 1ª ed. São Paulo: RT, 2020.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais**: comentários à Lei 13.709/2018 (LGPD). 2ª ed. São Paulo: Saraiva Educação, 2020.

ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT. Guidelines on the Protection of Privacy and Transborder Flows of Personal, of September 23rd, 1980. 23 set. 1980. Disponível em: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Acesso em 26 jun. 2021

QUINELATO, Pietra Daneluzzi. A proteção de dados pessoais no âmbito das *startups*. In: OIOLI, Erik Frederico (Coord.). **Manual de direito para startups**. 2ª ed. São Paulo: RT, 2020.

SCHVARTZMAN, Felipe. Lei Geral de Proteção de Dados Pessoais e riscos cibernéticos: coexistência de normas no mercado de meios de pagamento. In: COHEN, Gabriel Luiz Schvartzman (Coord.). **Direito dos Meios de Pagamento**. São Paulo: Quartier Latin, 2020.

THE ECONOMIST. The world's most valuable resource is no longer oil, but data. **The Economist**. 06 maio 2017. Disponível em https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em 06 dez. 2020.

UK INFORMATION COMMISSIONER Office. Guide to the General Data Protection Regulation (GDPR). 02 ago. 2018. Disponível em: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdfhttps://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf). Acesso em 30 jun. 2021.

VAINZOF, Rony. Comentários ao art. 5º. In: MALDONADO, Viviane Nobrega; BLUM, Renato Opice (Coord.). **LGPD**: Lei Geral de Proteção de Dados comentada, 2ª ed. São Paulo: RT, 2019.

VAINZOF, Rony. Dados pessoais, tratamento e princípios. In: MALDONADO, Viviane Nobrega; BLUM, Renato Opice (Coord.). **Comentários ao GDPR – Regulamento Geral de Proteção de Dados da União Europeia**, 2ª ed. São Paulo: RT, 2019.

VIGGIANO, Giuliana. Google atinge "supremacia quântica", que promete revolucionar a computação. **Galileu**, 23 out. 2019. Disponível em https://revistagalileu.globo.com/Tecnologia/noticia/2019/10/google-atinge-supremacia-quantica-que-promete-revolucionar-computacao.html. Acesso em 14 dez. 2020.

VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11º. In: BIONI, Bruno et al (Coords.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Grupo GEN, 2020.

LEGISLAÇÃO

BANCO CENTRAL DO BRASIL. Circular nº 3.681, de 4 de novembro de 2013. Dispõe sobre o gerenciamento de riscos, os requerimentos mínimos de patrimônio, a governança de instituições de pagamento, a preservação do valor e da liquidez dos saldos em contas de pagamento, e dá outras providências. **Banco Central do Brasil**, Brasília, DF, 4 nov. 2013. Disponível em: https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/48839/Circ_3681_v9_L.pdf. Acesso em 01 jun. 2021.

BANCO CENTRAL DO BRASIL. Circular nº 3.682, de 4 de novembro de 2013. Aprova o regulamento que disciplina a prestação de serviço de pagamento no âmbito dos arranjos de pagamentos integrantes do Sistema de Pagamentos Brasileiro (SPB), estabelece os critérios segundo os quais os arranjos de pagamento não integrarão o SPB e dá outras providências. **Banco Central do Brasil**, Brasília, DF, 4 nov. 2013. Disponível em: https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/48838/Circ_3682_v18_L.pdf. Acesso em 01 jun. 2021.

BANCO CENTRAL DO BRASIL. Circular nº 3.978, de 23 de janeiro de 2020. Dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil visando à prevenção da utilização do sistema financeiro para a prática dos crimes de "lavagem" ou ocultação de bens, direitos e valores, de que trata a Lei nº 9.613, de 3 de março de 1998, e de financiamento do terrorismo, previsto na Lei nº 13.260, de 16 de março de 2016. **Banco Central do Brasil**, Brasília, DF, 23 jan. 2020. Disponível em: https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50905/Circ_3978_v2_L.pdf. Acesso em 01 jun. 2021.

BANCO CENTRAL DO BRASIL. Resolução nº 80, de 25 de março de 2021. Disciplina a constituição e o funcionamento das instituições de pagamento, estabelece os parâmetros para ingressar com pedidos de autorização de funcionamento por parte dessas instituições e dispõe sobre a prestação de serviços de pagamento por outras instituições autorizadas a funcionar pelo Banco Central do Brasil. **Banco Central do Brasil**, Brasília, DF, 25 mar. 2021. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=80. Acesso em 01 jun. 2021.

BRASIL. Constituição da República Federativa do Brasil de 1988. **Palácio do Planalto Presidência da República**, Brasília, DF, 5 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 01 jun. 2021.

BRASIL. Decreto nº 7.962, de 15 de março de 2013. Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico. **Palácio do Planalto Presidência da República**, Brasília, DF, 15 mar. 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D7962.htm. Acesso em 01 jun. 2021.

BRASIL. Decreto nº 8.771, de 11 de maio de 2016. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. **Palácio do Planalto Presidência da República**, Brasília, DF, 23 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm. Acesso em 01 jun. 2021.

BRASIL. Lei Complementar nº 105, de 10 de janeiro de 2001. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. **Palácio do Planalto Presidência da República**, Brasília, DF, 10 jan. 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm. Acesso em 01 jun. 2021.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Palácio do Planalto Presidência da República**, Brasília, DF, 11 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em 01 jun. 2021.

BRASIL. Lei nº 9.613, de 3 de março de 1998. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências. **Palácio do Planalto Presidência da República**, Brasília, DF, 3 mar. 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9613.htm. Acesso em 01 jun. 2021.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Palácio do Planalto Presidência da República**, Brasília, DF, 10 jan. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em 01 jun. 2021.

BRASIL. Lei nº 12.414, de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. **Palácio do Planalto Presidência da República**, Brasília, DF, 9 jun. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em 01 jun. 2021.

BRASIL. Lei nº 12.865, de 9 de outubro de 2013. Autoriza o pagamento de subvenção econômica aos produtores da safra 2011/2012 de cana-de-açúcar e de etanol que especifica e o financiamento da renovação e implantação de canaviais com equalização da taxa de juros; dispõe sobre os arranjos de pagamento e as instituições de pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB); autoriza a União a emitir, sob a forma de colocação direta, em favor da Conta de Desenvolvimento Energético (CDE), títulos da dívida pública mobiliária federal; estabelece novas condições para as operações de crédito rural oriundas de, ou contratadas com, recursos do Fundo Constitucional de Financiamento do Nordeste (FNE); altera os prazos previstos nas Leis nº 11.941, de 27 de maio de 2009, e nº 12.249, de 11 de junho de 2010; autoriza a União a contratar o Banco do Brasil S.A. ou suas subsidiárias para atuar na gestão de recursos, obras e serviços de engenharia relacionados ao desenvolvimento de projetos, modernização, ampliação, construção ou reforma da rede integrada e

especializada para atendimento da mulher em situação de violência; disciplina o documento digital no Sistema Financeiro Nacional; disciplina a transferência, no caso de falecimento, do direito de utilização privada de área pública por equipamentos urbanos do tipo quiosque, trailer, feira e banca de venda de jornais e de revistas; altera a incidência da Contribuição para o PIS/Pasep e da Cofins na cadeia de produção e comercialização da soja e de seus subprodutos; altera as Leis nºs 12.666, de 14 de junho de 2012, 5.991, de 17 de dezembro de 1973, 11.508, de 20 de julho de 2007, 9.503, de 23 de setembro de 1997, 9.069, de 29 de junho de 1995, 10.865, de 30 de abril de 2004, 12.587, de 3 de janeiro de 2012, 10.826, de 22 de dezembro de 2003, 10.925, de 23 de julho de 2004, 12.350, de 20 de dezembro de 2010, 4.870, de 1º de dezembro de 1965 e 11.196, de 21 de novembro de 2005, e o Decreto nº 70.235, de 6 de março de 1972; revoga dispositivos das Leis nºs 10.865, de 30 de abril de 2004, 10.925, de 23 de julho de 2004, 12.546, de 14 de dezembro de 2011, e 4.870, de 1º de dezembro de 1965; e dá outras providências. **Palácio do Planalto Presidência da República**, Brasília, DF, 9 out. 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12865.htm. Acesso em 01 jun. 2021.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Palácio do Planalto Presidência da República**, Brasília, DF, 23 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 01 jun. 2021.

BRASIL. Lei nº 13.260, de 16 de março de 2016. Regulamenta o disposto no inciso XLIII do art. 5º da Constituição Federal, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista; e altera as Leis n º 7.960, de 21 de dezembro de 1989, e 12.850, de 2 de agosto de 2013. **Palácio do Planalto Presidência da República**, Brasília, DF, 16 mar. 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13260.htm. Acesso em 01 jun. 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). **Palácio do Planalto Presidência da República**, Brasília, DF, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 01 jun. 2021.

CONSELHO MONETÁRIO NACIONAL. Resolução nº 4.282, de 4 de novembro de 2013. Estabelece as diretrizes que devem ser observadas na regulamentação, na vigilância e na supervisão das instituições de pagamento e dos arranjos de pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB), de que trata a Lei nº 12.865, de 9 de outubro de 2013. **Banco Central do Brasil**, Brasília, DF, 4 nov. 2013. Disponível em: https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/48841/Res_4282_v1_O.pdf. Acesso em 01 jun. 2021.

COUNCIL OF EUROPE. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. **European Treaty Series**. Estrasburgo. 28 jan. 1981. Disponível em https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37. Acesso em: 26 jun. 2021

UNIÃO EUROPEIA. Directiva (UE) nº 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. **Jornal Oficial das Comunidades Europeias**, Luxemburgo, 23 nov. 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT. Acesso em: 26 jun. 2021.

UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados**). Jornal Oficial da União Europeia**, Bruxelas, 04 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=PT. Acesso em: 17 jun. 2021.