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

VICTOR BERNARDI MARTINO

O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS: as adaptações do Estado e do Setor Financeiro no Brasil

BRASÍLIA

2022

VICTOR BERNARDI MARTINO

O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS: as adaptações do Estado e do Setor Financeiro no Brasil

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

Orientador(a): Professor Dr. José Levi do Amaral Junior

BRASÍLIA

2022

VICTOR BERNARDI MARTINO

O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS: as adaptações do Estado e do Setor Financeiro no Brasil

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

Orientador(a): Professor Dr. José Levi do Amaral Junior

BRASÍLIA, 10 DE DEZEMBRO DE 2022

BANCA AVALIADORA

_____

JOSÉ LEVI DO AMARAL JUNIOR

_____

Professor(a) Avaliador(a)

AGRADECIMENTOS

Sou grato aos vivos, porquanto estão vivos. Aos mortos, porque já estiveram vivos. À vida que antes não existia, e que hoje me toca em todas as horas, de meu filho, Julio. À minha companheira, Luisa Ramos Caetano. À minha mãe, Maria Alice Bernardi Martino Cotrim. Aos meus dois pais, Julio Cesar Martino e Donizeti Diogenes Cotrim. À Matrioska, Amelia Paes de Almeida Bernardi. Aos colegas de Data Privacy Office e Risk Management da EY Brasil, pelo conhecimento e oportunidades. Ao meu líder profissional Nuno Vieira, pelo reconhecimento e confiança. Ao meu Professor-orientador nesse projeto, Dr. José Levi do Amaral Junior, por perseverar acreditando no desenvolvimento desse trabalho e pelas diretrizes objetivas e precisas. Ao Núcleo de Pesquisa Jurídica- NPJ do CEUB por contemplar o que seria melhor para a entrega desse trabalho.

Vocês, o povo, têm o poder — o poder de criar máquinas, o poder de criar felicidade! Vocês, o povo, têm o poder de fazer desta vida livre e bela, de fazer desta vida uma aventura maravilhosa. - Discurso em “O Grande Ditador” (1940) de Charles Chaplin

RESUMO

O direito a proteção de dados se aperfeiçoou no mundo e, recentemente no Brasil, tornou-se direito fundamental expresso no rol de direitos fundamentais individuais da Constituição da República Federativa do Brasil de 1988 (CRFB/88). O presente trabalho visa a demonstração de que a positivação de tal direito em uma Constituição de classificação formal não ‘e à toa, senão um dever do poder constituinte derivado reformador, notadamente o Poder Legislativo, sobretudo em tempos em que o encontro entre os avanços tecnológicos e as necessidades humanas pelo encurtamento da distancias no pós-pandemia atingiram um planalto. Os riscos estão agravados, desde a ameaça aos direitos da personalidade dos indivíduos, por sua autodeterminação informativa, como cunhada no direito alemão, até a manipulação comportamental dos indivíduos em temas sensíveis, a exemplo do resultado dos pleitos eleitorais e a ordem do Estado Democrático. Objetos específicos do presente trabalho são os recentes acordos de cooperação entre o Governo Federal do Brasil e entidades de representação civis dos bancos, para compartilhamento de dados de milhões de brasileiros, na contramão da Lei Geral de Proteção de Dados (LGPD) e da proteção de dados como direito fundamental. Os riscos operacionais de tais acordos são diversos, com destaque a não formalização dos limites do uso desses dados, sua finalidade e, como hipótese, dúvida se tais dados podem ser utilizados para arquitetura de perfis de comportamento de consumo de maneira a manipular o comportamento das pessoas titulares de dados a consumirem mais do que consumiriam e, por vezes, do que poderiam em termos de poder de consumo. A utilização de dados dessa maneira incorreria na ausência do princípio da autodeterminação informativa, o que influencia não somente a dignidade e o comportamento dos indivíduos, como da sociedade em geral.

Palavras-chave: LGPD; proteção de dados pessoais; monetização de dados; direitos fundamentais.

SUMÁRIO

INTRODUÇÃO

A atenção à proteção aos dados pessoais é tema de grande consideração nas pautas dos órgãos estatais de todos os Poderes, nas corporações empresariais, organizações sociais em todas as nações.

Se antes a privacidade estava em voga nas aflições da sociedade, a partir de conflitos dirigidos ao mundo físico, ainda que, em alguns casos, houvessem de uma vigia social por câmeras, a discussão evolui de patamar. A preocupação hoje não está mais com os acessos a imagens ou dados objetivos das pessoas em si, mas em como esses dados são utilizados para o desenho de perfis.

O desenho de perfis sociais, possibilitado pela mineração de dados em massa, permite à governos e empresas mais do que a identificação de pessoas e seus comportamentos, mas também a definição de seus comportamentos, a partir do que lhes é ofertado em contrapartida à obtenção de seus dados. Os comportamentos de um indivíduo abrangem os seus hábitos de consumo, ideológicos, culturais e, portanto, integram a sua autodeterminação.

A autodeterminação informativa, termo cunhado pela Corte Constitucional alemã, em decisão que marcou o direito à proteção de dados na década de 70, revela desde aquele momento que o desenvolvimento de tecnologias da informação para armazenamento e tratamento de dados em massa era tema sensível a ser tutelado pelas nações-estado. Houve então evoluções geracionais do direito à proteção dados, até se atracar ao no porto do consentimento.

Os princípios da dignidade da pessoa humana e de sua personalidade deveriam prevalecer sobre os interesses de um mercado de consumo extremamente racional e de um modelo governamental extremamente controlador. Não obstante tenham em suas ações finalidades claras: aumento de margens de receitas e melhor atendimento ao público, respectivamente – esses interesses não devem preponderar sobre preceitos fundamentais.

Em consequência da magnitude do problema, o direito à proteção de dados foi positivado em diversos países. O Supremo Tribunal Federal decidiu em favor do reconhecimento do direito à proteção de dados como fundamental em 2017, no caso que envolvia os bancos de dados do Instituto Brasileiro de Geografia e Estatística. Seguidamente, em 2018, o direito foi positivado com a Lei Geral de proteção de Dados (LGPD). Mais além, diante da incerteza sobre tal direito estar abarcado ou não como direito fundamental, como sub-rogado do direito à privacidade, promulgou-se em 2022 sua emenda constitucional, integrando o rol expresso de direitos fundamentais na Constituição Federal de 1988.

No entanto, passa que, assim como para outros direitos, a proteção de dados pode ser relativizada. A necessidade de trocas de dados pessoais em transações, seja com o público ou entre particulares, para fins de certificação da legitimidade e de confiabilidade, faz com que o limiar entre o gerenciamento legítimo e ilegítimo de dados pessoais seja estreito.

Sem embargos à LGPD apresentar estrutura e conteúdo robustos como espelho de arcabouços legais relativos à matéria construídos ao longo de décadas em ordenamentos nacional e estrangeiros, há ainda certa insegurança jurídica sobre como serão conduzidos temas como o papel do órgão de fiscalização – a Autoridade Nacional de Proteção de Dados – e como efetivamente avaliará a atuação do Estado e das Corporações.

Um caso recente, é o acordo do Governo brasileiro junto a Federação Brasileira de Bancos (FEBRABAN), para compartilhamento do seu banco de dados central públicos com os bancos associados. Outrossim, objetiva-se nesta monografia confrontar os requisitos da LGPD com o plano de Open Finance, estágio atual do que antes se denominava *Open Banking*, seguidamente de *Open Investiment*.

A respeito do acordo de compartilhamento de dados entre o Governo Federal e a FEBRABAN, tem-se como fim analisar a legalidade e constitucionalidade do ato administrativo que deu ensejo ao negócio jurídico.

No caso do *Open Finance, a* finalidade é analisar as possibilidades lógico-jurídicas para além do já comportado consentimento dos indivíduos quando da cessão de seus dados.

CAPÍTULO I. PROTEÇÃO DE DADOS COMO DIREITO FUNDAMENTAL

A proteção de dados ganha força normativa constitucional em 2022, a partir do histórico explorado adiante, que percorre as noções dos direitos preexistentes: do direito a propriedade e o direito à privacidade, passando por analises principiológicas, até as visões de supremas cortes na Europa e no Brasil.

1. A PROTEÇÃO DE DADOS PESSOAIS E SUA FORMAÇÃO COMO DIREITO

A formação do direito à proteção dos dados pessoais requer considerações sobre a origem do direito à privacidade. (MENDES, 2014)

Os debates acerca do direito à privacidade decorreram da insurgência de novas técnicas e instrumentos tecnológicos que passaram a se infiltrar na vida privada, com a divulgação ampla e irrestrita de fatos relativos à vida dos indivíduos. Assim, em sua origem, o direito à privacidade possui um viés extremamente individualista.

Em seu desenvolvimento a partir de uma visão da common law, o direito à privacidade, diferenciou-se por uma definição relacionada à inviolabilidade da personalidade, e não mais à proteção da propriedade privada. (MENDES, 2014)

Posteriormente, o direito à privacidade na Europa foi delineado pelo não impede da publicação do que é de interesse público, nem de tudo o que seja privado, pois os atos do Estado são regidos por lei. Além disso, a divulgação de dados sem causa de danos não gera direito a reparação, e o consentimento do titular dos dados e a ausência de dolo não geraria violação ao direito à privacidade. (MENDES, 2014)

No século XX, com a revolução tecnológica após a Segunda Guerra Mundial, a visão sobre o direito à privacidade como um direito restrito ao indivíduo, o que não poderia lhe ser mitigado, passou a ser notado como garantia ao indivíduo, a partir de seu controle direto sobre suas informações. Nesse sentido, esse direito fundamental ganhou espaço com uma conotação mais democrática, sobre uma sociedade internacional atingida diuturnamente pela informatização de seus dados, de modo a carecer de proteção legal.

Na década de 70, passou-se então a ser notada maior preocupação de diversos países com a proteção de dados em si, período em que foram produzidas legislações, julgadas causas e editados acordos internacionais em favor do direito à proteção de dados baseados no conceito do direito à personalidade relativa aos dados pessoais. Como contrapartida à corrida de governos e empresas pelo processamento e armazenamento de dados massivos, foram promulgadas as primeiras leis específicas para proteção de dados na Europa e nos Estados Unidos. (MEDES, 2014, p. 29)

Como desenvolvimento do embrião concebido a partir de leis e tratados dessa natureza, deu-se início a um pensamento global sobre o conceito de privacidade sublinhado pela proteção de dados pessoais, destacando-se as convenções e diretrizes da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) e do Conselho Europeu.

O marco para o entendimento sobre o direito à proteção de dados e controle do indivíduo é oriundo da Corte Constitucional Alemã, que decidiu sobre a lei de censo desse país - que normatiza os atos de órgão da Administração Pública voltados a pesquisas, tais quais as realizadas pelo Instituto Brasileiro de Geografia e Estatística (IBGE) – oportunidade em que foi cunhada a expressão “autodeterminação informativa”.

A “autodeterminação informativa” como concebida pela Corte Alemã, defrontava precipuamente a não participação decisória sobre que dados os cidadãos cederiam, como seriam tratados, por quanto tempo seriam armazenados, qual a finalidade de sua detenção. Baseou-se o Tribunal no princípio da dignidade da pessoa humana e no livre desenvolvimento da personalidade, e delineou, assim, a proteção de dados como direito subjetivo fundamental. Tal decisão constitucional incidiu sobre o poder legislativo, que passou a legislar nos parâmetros constitucionais assim concebidos.

Nessa miríade, é notável a proteção de dados pessoais como uma dimensão do direito à privacidade. Consequentemente, ambas partilham dos mesmos fundamentos: a tutela da personalidade e da dignidade da pessoa humana. (LAURA, p.35)

A evolução da proteção de dados pessoais frente aos novos paradigmas

Ainda atual, a obra pioneira do sec. XX de Castells (1999) já falava sobre novas tecnologias da informação que, àquela época, já estavam “integrando o mundo em redes globais de instrumentalidade”, interferindo significativamente nas estruturas sociais. (MENKE, 2021)

A ampliação da complexidade do sistema industrial, a burocratização dos setores público e privado, a transformação das ciências sociais e da tecnologia da informação, o certo é que nos tornamos a sociedade que mais já gerou dados.

(SCHERTEL, p.32). Em decorrência, foi exigido que o Direito se desenvolvesse de forma a proteger os riscos aos sujeitos dos dados.

O valor intrínseco que justifica a necessidade do desenvolvimento de normas que protejam os dados das pessoas está em que, entre sujeito e sociedade, imperam os seus dados como intermediários das relações. Nessa posição, os dados pessoais possuem enorme capacidade de causar danos e prejuízos à personalidade individual, caso informações sejam divulgadas ou armazenadas de forma inadequada. (LAURA in DONEDA, p.33)

Haja vista os motivos pelos quais os dados pessoais são coletados, é notório o risco de mitigação de direito à privacidade ou à personalidade. Corporações e governos de diversos posicionamentos políticos visaram ao uso de um sistema global burocratizado e tecnológico para analisar, investigar, negociar e administrar, não apenas a partir do armazenamento desses dados, mas também por meio de seu tratamento, com o intuito de desenharem perfis informativos de cada pessoa e seu comportamento consumerista, laboral ou cidadão. (MENDES, 2014) O desenho de perfis tornou possível tomar decisões com maior capilaridade e influenciar o comportamento econômico, político e social dos indivíduos.

Não obstante o avanço tecnológico tenha alavancado a capacidade de armazenamento e tratamento de dados pessoais, não é razoável considerar que deva prevalecer sobre o do direito à privacidade e à proteção de dados. Por outro lado, também não é razoável que o desenvolvimento tecnológico deva se restringir em absoluto pelos direitos eventualmente ameaçados. (MENDES, 2014). Outrossim, não é correto ponderar que os fatores e interesses que deram causa ao avanço da tecnologia da informação anulem o seu valor nas relações humanas hoje.

Em comparação, nas décadas de 60 e 70 se discutiu persistentemente o risco de esgotamento de recursos naturais em prol do desenvolvimento econômico aliado à superpopulação do mundo, como se não fosse possível encontrar um ponto de equilíbrio entre os recursos disponíveis e as demandas. Sobreveio, então, o movimento de desenvolvimento sustentável, o qual equaliza essas questões. No mesmo sentido, a proposta de (GARFINKEL, 2000) é que o desenvolvimento e utilização de tecnologias seja harmonizado com a garantia de privacidade pessoal.

As **Gerações do direito à proteção de dados**

Bobbio (2004) observa sobre a evolução dos direitos fundamentais:

> Não nascem todos de uma vez. Nascem quando devem ou podem nascer. Inicialmente, a urgência era pela garantia da liberdade do indivíduo. Posteriormente, outras necessidades emergiram, representando importantes ferramentas à compreensão da sociedade e das soluções jurídicas a se seguirem.

MENKE (2021, p. 2) propõe que a maneira pela qual se deva analisar a possibilidade de um direito como a proteção de dados pessoais merecer o status de um direito fundamental autônomo é identificar a sua maturidade frente às gerações dos direitos fundamentais:

> Compreender, uma a uma, essas gerações, e observar o estágio atual em que se encontram, é tarefa exigida a se identificar a necessidade e a viabilidade de incluir o direito à proteção de dados pessoais na lista de direitos fundamentais autônomos.

Os direitos fundamentais denominados de primeira geração - fase inaugural do constitucionalismo no ocidente, consolidada ao final do século XVII (Revolução Francesa contra o Estado Absolutista - Liberdade, Igualdade, Fraternidade,) - apontam para a ideia de liberdade negativa clássica, buscando promover a separação entre sociedade e Estado (impor limites à forca estatal), dizem respeito ao direito à vida, à propriedade, à inviolabilidade de domicílio, à liberdade de expressão e à participação política e religiosa.

Sec. XIX e XX, somou-se aos direitos fundamentais o entendimento sobre os direitos políticos: liberdade do indivíduo a partir da ideia de participação na tomada de decisões. Assim avançou-se com relação ao entendimento por direitos que extrapolassem a isenção negativa do Estado, dando espaço à segunda geração.

A primeira geração das normas de proteção de dados pessoais surgiu na década de 70, como reação ao processamento eletrônico de dados nas Administrações Públicas e nas Empresas Privadas, bem como às ideias de centralização dos bancos de dados em gigantes bancos de dados nacionais.

impulso para o surgimento de normas europeias na década de 70 foi o contexto generalizado do Estado Social, em que governos necessitavam armazenar dados dos cidadãos com a finalidade de administrar os serviços públicos.

Segunda geração: direitos sociais e econômicos (ou de igualdade): O Estado deveria intervir para garantir as liberdades individuais, especialmente com relação à saúde, educação, alimentação, trabalho, moradia, lazer e segurança.

Segunda geração de normas de proteção de dados pessoais suscita uma controvérsia bastante interessante, relacionada à efetividade do consentimento do cidadão e do real exercício de sua liberdade de escolha, em um contexto no qual a não disponibilização dos dados pode acarretar a sua exclusão social. Por um lado, no âmbito do Estado Social, é muito difícil assegurar-se a liberdade informacional sem comprometer as funções dessa complexa burocracia que necessita de dados dos cidadãos para planificar. Por outro, também na relação entre privados é difícil se verificar o exercício do direito à privacidade informacional, na medida em que tal exercício poderá impedir o acesso do indivíduo a determinadas facilidades do mercado de consumo, que o fornecedor está disposto a conceder somente em troca de suas informações pessoais.

Na Terceira Geração, após Segunda Guerra Mundial, direitos transindividuais e direcionados à Globalização, ligados aos valores da fraternidade e solidariedade: voltados ao desenvolvimento, paz, meio ambiente, direito de propriedade sobre o patrimônio comum da humanidade e ao direito de comunicação.

A terceira geração de normas de proteção de dados pessoais é marcada pela decisão do Tribunal Constitucional alemão 40, de 1983, que declarou a inconstitucionalidade de parte da Lei do Censo. Na ocasião, o Tribunal reinterpretou a Lei Federal de Proteção de Dados Pessoais alemã à luz da Lei Fundamental de Bonn e declarou que os cidadãos possuem o direito à autodeterminação informativa, radicalizando a ideia do controle do indivíduo no processamento de seus dados. A principal diferença em relação à segunda geração de normas é que a participação do cidadão no processamento de seus dados passa a ser compreendida como um envolvimento contínuo em todo o processo, desde a coleta, o armazenamento e a transmissão e não apenas como a opção entre “tudo ou nada”.

Com o transcurso do tempo, novos direitos se juntam aos já delineados e, embora haja divergências doutrinárias, em razão de sua abstração, parcela importante de estudiosos do tema, capitaneada pelo jurista Bonavides, posiciona-se no sentido de haver ainda outras gerações. em: BONAVIDES, Paulo. Curso de Direito Constitucional. 15.ed. São Paulo. Malheiros, 2004. p. 569.

MENKE (2021, pg. 4) - “O direito fundamental à proteção de dados estaria inserido em uma dessas novas gerações de direitos fundamentais - na quarta, ou até mesmo na quinta, ambas objeto de divergência doutrinária."

Ao mencionar a quarta geração, Bonavides diz: “Deles depende a concretização da sociedade aberta ao futuro, em sua dimensão de máxima universalidade, para a qual parece o mundo inclinar-se no plano de todas as relações de convivência (...) Tao somente com eles será legítima e possível a globalização política `` em: BONAVIDES, Paulo. Curso de Direito Constitucional. 15.ed. São Paulo. Malheiros, 2004. p. 571 - 572.

A Quarta geração tem origem, nesse sentido, nos direitos à democracia, à informação e ao pluralismo. E’ justamente nesse cenário que emerge de uma sociedade globalizada, dinâmica e volátil, que parece repousar o direito fundamental à proteção de dados pessoais” A quarta geração de normas buscou resolver esses problemas apresentados nos períodos anteriores por meio de duas soluções. Primeiramente, algumas das normas visaram fortalecer a posição dos indivíduos, tornando mais efetivo o seu autocontrole sobre os dados pessoais. Isso foi possível, por exemplo, a partir da previsão de “no faulta compensation” para reclamações individuais a respeito da violação à proteção de dados pessoais, que se deu na Alemanha, com a emenda à Lei Federal de Proteção de Dados alemã, sendo que norma semelhante já existia na legislação da Noruega em menor extensão.

Em outros casos, as normas retiraram da esfera do controle do indivíduo determinados assuntos, por compreenderem que alguns temas relativos aos dados pessoais são tão relevantes para o cidadão que merecem ser extremamente protegidos, não podendo estar na esfera de disposição individual. Tal pode ser observado na proibição, total ou parcial, imposta para o tratamento dos dados pessoais considerados sensíveis, que são aqueles cujo tratamento tem grande potencial de acarretar discriminação, tais como os dados relativos à etnia, opção sexual, opinião política e religião. (p.43)

Ressalta-se que os direitos fundamentais originalmente contavam com aspecto vertical, no qual o titular passa a ter instrumentos capazes de se opor aos arbítrios do Estado frente a possíveis abusos. Entretanto, preocupação e necessidade similares sugiram em relação aos arbítrios cometidos por particular, dando espaço à horizontalização direito fundamental, vinculando a esses direitos não apenas o Estado, mas também os particulares, em suas relações privadas. Movimento que

surgiu ao se perceber que o poder em sociedade já não era de exclusividade do Estado. É um direito tão importante quanto a privacidade (e não apenas seu consectário)

Desde a sua origem, a disciplina da proteção de dados desenvolveu-se e alterou-se substancialmente, em razão das transformações econômicas, sociais e tecnológicas das últimas quatro décadas.

Regulamento Setorial

Outra característica bastante interessante da quarta geração de normas de proteção de dados pessoais consiste no fato de que, em diversos países, normas gerais sobre a proteção de dados são complementadas com normas setoriais. Tal fato tem como finalidade ampliar a proteção do indivíduo nos diversos setores em que é possível o tratamento dos seus dados pessoais, de modo que a legislação possa contemplar as diversas especificidades setoriais.

2. LEI GERAL DE PROTEÇÃO DE DADOS E NORMAS EXTERNAS INFLUENTES

Com o acesso facilitado da internet, seja nas residências, seja nos smartphones, as barreiras geográficas tornaram-se irrelevantes, fazendo com que informações fiquem ao alcance de internautas do outro lado do planeta em questão de segundos.

Devido a essa facilidade de tráfego de informações, torna-se cada vez mais complexa a previsão da provável utilização desses dados, quem os utilizarão, por quanto tempo e para qual finalidade. Essa preocupação fez com que diversos países criassem mecanismos legais orientando sobre uso de dados pessoais, criação de autoridades fiscalizadoras de proteção de dados pessoais e sanções para ilícitos cometidos na utilização destes.

Hannah Arendt, em “A condição humana” (1958) discorre sobre a importância da propriedade privada, cujas paredes ofereceriam “o único refúgio seguro contra o mundo público comum”.

Em “Era da Vigilância Liquida”, Zygmunt Bauman (2014) alerta a propriedade privada já não é suficiente para a inviolabilidade do indivíduo, pois a exposição se faz possível por meio da tecnologia, inclusive e especialmente pelo acesso a dados pessoais.

O conferido tratamento autônomo à disciplina da proteção de dados pessoais no Brasil é fruto de uma tendência consolidada em diversos ordenamentos jurídicos estrangeiros cuja principal consequência foi a formação das bases para elevar-se a proteção de dados à categoria de direito fundamental. (DONEDA, 2011, p.96)

Dessa forma, mesmo antes da edição da Lei Geral de Proteção de Dados Pessoais no ordenamento brasileiro, já era possível perceber, a partir das normas em comento, a formação de um sistema de proteção de dados pessoais, ao qual incorporou-se grande parte dos princípios relativos à proteção de dados pessoais já padronizados na seara internacional (MENDES, 2014. p.160)

O aumento na troca de informações entre as fronteiras nacionais surge como decorrência do estabelecimento de um mercado global, pelo que a proteção de dados tem, desde então, tornando-se uma questão que permeia o cenário internacional, sobretudo a partir da década de 1980. (ROOS, 2006. p.103)

Nesse sentido, importa compreender que a significativa convergência internacional estabelecida em torno de determinados princípios relativos ao tratamento de dados: diferentes ordenamentos jurídicos têm adotado uma série de princípios básicos de proteção de dados, com sutis diferenças entre eles. (MENDES, 2014. p.68)

Esse quadro comum de princípios é denominado “Fair information Practice Principles(FIPPs)”**,** cuja origem remonta à década de 70, sendo que seu surgimento ocorre de forma quase simultânea nos Estados Unidos, Inglaterra e na Alemanha. (CATE, 2009, p.343)

FAIR INFORMATION PRACTICE PRINCIPLES: instrumentos básicos internacionais e transnacionais que norteia a atividade de tratamento de dados, com princípios básicos, com objetivos de especificar limitações ao tratamento de dados, além de viabilizar que o indivíduo detenha condições de controlar o fluxo de suas informações

Tais princípios encontram expressão, em especial, com a edição de dois instrumentos internacionais: a Convenção de Estrasburgo e as *guidelines* da Organização para a Cooperação e Desenvolvimento Econômico - OCDE, no início da década de 1980. De acordo com a doutrina pátria, é possível elaborar uma síntese desses princípios (DONEDA, 2011. p. 100)

As duas *guidelines* emitidas pela OCDE: 1) proteção da privacidade e 2) fluxo transfronteiriço de dados pessoais - princípios a serem seguidos pelas legislações sobre o tema, “no intuito de criar um ambiente regulatório uniforme e, por conseguinte, permitir o livre fluxo de informações" (BIONI, 2019. p.118 - 119)

LGPD (Brasil) *versus* GPDR (União Europeia)

Convergências: a) princípios elencados pelas legislações (influência do consenso transnacional); b) modelo ex-ante de proteção (controlador só está autorizado a tratar dados caso amparado por base legal); c) papel da accountability nos dois modelos regulatórios.

Contudo em que pese a LGPD tenha elencado o princípio da accountability, não prevê os procedimentos a serem realizados para que os relatórios, selos e códigos de boas condutas sejam efetivamente utilizados pelos agentes de tratamento.

A Lei deixa o encargo de regulação para a Autoridade Nacional de Proteção de Dados Pessoais.

LGPD e RGPD tem muito em comum, quando tratam da estruturação de diretrizes para a transferência de dados pessoas. A semelhança do Regulamento Europeu, a lei brasileira estabelece três regimes para tutelar a transferência internacional de dados: “a) a declaração de existência de grau de proteção de dados adequado; b) a existência de garantia de cumprimentos dos preceitos da LGPD; c) derrogações especificas do regime da LGPD (CARVALHO, 2019. p.624)

Fazendo uma interseção entre o direito comunitário europeu e o brasileiro, o RGPD seria um código de proteção de dados que conta uma quantidade maior de dispositivos e com uma espécie de exposição de motivos, ao passo que a LGPD seria uma lei mais enxuta e sem pistas interpretativas deixadas por parte do legislador”, BIONI, Bruno R., MENDES, Laura Schertel. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral brasileira de Proteção de Dados: mapeando convergências na direção de um nível de equivalência. In. FRAZAO, Ana; TEPEDINO, Gustavo, OLIVA, Milena Donato (Coord.) Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. São Paulo: Thomson Reuters Brasil, 2019.p. 806.

A legislação europeia é resultado de longa construção na área da proteção de dados. Possui 173 considerandos e 99 artigos.

A LGPD brasileira foi elaborada com grande inspiração europeia. Mas possui 65 artigos e não apresenta orientações interpretativas.

A técnica legislativa é uma das maiores divergências entre as legislações.

Por fim, LGPG aborda em seu texto a temática relativa à transferência internacional de dados, coloca o país em posição competitiva com outras nações que já disciplinaram, em legislações especifica, critérios para que tal fluxo ocorra - algo extremamente necessário, seja em razão da globalização econômica, como também pelo fato de que transações envolvendo dados pessoais muito dificilmente deixam de ter dimensão internacional relevante (CARVALHO, 2019. p. 623)

Constitucionalização

Não existem mais dados irrelevantes diante do processamento eletrônico e ubíquo de dados na sociedade da informação. Considerando que os dados pessoais são projeções diretas da personalidade, qualquer tratamento de dados acaba por influenciar a representação da pessoa na sociedade, podendo afetar a sua personalidade e, portanto, tem o potencial de violar os seus direitos fundamentais (BIONI, Bruno R. MENDES, Laura Scherer. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral Brasileira de Proteção de Dados: mapeando convergências na direção de um nível de equivalência. In. FRAZAO, Ana; TEPEDINO, Gustavo, OLIVA, Milena Donato (Coord.) Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. São Paulo: Thomson Reuters Brasil, 2019.p. 811)

Antecedentes Normativos

Inicialmente, o sistema brasileiro de proteção de dados era composto por normas esparsas que exigiam uma interpretação sistemática, ou seja, coordenada de todo o ordenamento jurídico a fim de efetivar a proteção.

Nota-se uma progressão do sistema a cada nova norma publicada, tentando tornar o tratamento mais seguro e igualitário, bom como preservando a intimidade por meio dos dados sensíveis, buscando trazer mais inclusão social por meio da neutralidade da rede, coibir abusos perpetrados pela livre iniciativa, entre tantos outros direitos aos indivíduos. O referido sistema foi unificado com o advento da LGPD.

Normas esparsas relativas à proteção de dados no ordenamento jurídico brasileiro:

- art. 5, incisos X e XII, da CF 88
- Cód. de Defesa do Consumidor (Lei 8078/1997): art. 43, caput e §§2o e 3o
- Lei de arquivos públicos (Lei 8159/1991): art. 4o
- Lei de Habeas Data (Lei 9.507/1997): art. 7o I, II e III
- Decreto 6.135/2007, art.8o
- Decreto 6.425/2008, art.6o
- Decreto 6.523/2008, art. 11
- Lei do Cadastro Positivo (lei 12.414/11): art. 5o, I, III e §4o e art. 3o, §3o)

- Lei do Acesso à Informação (Lei 12.527/2011): art. 8o §2o
- Lei do Marco Civil da Internet (Lei 12.965/2014): art. 19, §2o e art. 3o

Lei do Marco Civil da Internet definiu direitos e responsabilidades na utilização dos meios digitais, decorrendo seu texto de amplo debate público com contribuições da sociedade civil, da comunidade empresarial, de cidadãos comuns, bem como de representantes das áreas técnicas e acadêmica. A supracitada norma estabeleceu a edição futura de lei específica sobre a proteção de dados pessoais (art. 19, §2o). Também elencou no art. 3o, como princípios do uso da internet no Brasil: garantia da liberdade de expressão, comunicação e manifestação de pensamento, proteção da privacidade, proteção dos dados pessoais, preservação e garantia da neutralidade de rede e a responsabilização dos agentes de acordo com suas atividades. Princípios estes relacionados aos princípios contidos na LGPD. Proteção de Dados como Direito Fundamental - informações de https://www.serpro.gov.br/menu/noticias/noticias-2022/protecao-de-dados-pessoais-como-um-direito-fundamental

O Congresso Nacional promulgou em 10/02/2022 a Emenda Constitucional n° 115, de 2022, proveniente da PEC n° 17 de 2019. Ela altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais aos cidadãos e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais, além de organizar e fiscalizar o tema nos termos da lei.

A importância dos direitos à privacidade e proteção de dados pessoais estar elencado no art. 5º da Constituição Federal é que os direitos fundamentais são garantias com o objetivo de promover a dignidade humana e de proteger os cidadãos. O direito à privacidade e à proteção de dados pessoais é essencial à vida digna das pessoas, principalmente nesse contexto de total inserção na vida digital.

Os direitos previstos no Título II - Dos Direitos e Garantias Fundamentais da Constituição da República Federativa do Brasil elencam um rol de direitos e garantias individuais e coletivas nos aspectos sociais, econômicos e políticos considerados indispensáveis ao exercício da cidadania pelos brasileiros.

O texto constitucional proporciona uma proteção tão diferenciada aos direitos fundamentais que não é possível apresentar Proposta de Emenda à Constituição (PEC) tendente a aboli-los, por afronta ao princípio democrático.

A proteção de dados pessoais, com perspectiva de direito fundamental, incorpora à esfera jurídica do titular mais um mecanismo de proteção aos direitos de personalidade, com foco na imagem e na honra da pessoa natural. Importante destacar que qualquer pessoa, natural ou jurídica, privada ou pública, possui o dever de zelar pelos dados pessoais dos titulares, assumindo os riscos e podendo sofrer sanções caso não aplique as proteções necessárias para evitar o uso inadequado ou fraudulento dos dados pessoais.

As mudanças trazidas pela inclusão da proteção de dados pessoais como um direito fundamental são o fortalecimento de um direito que, até então, não se conhecia sua devida extensão, provocando equívocos quanto a quem pertencem os dados pessoais e o reconhecimento, tanto pelo Estado quanto pela sociedade, que a proteção de dados pessoais é necessária para o livre e pleno desenvolvimento da personalidade.

A LGPD cria o papel do Encarregado de Dados Pessoais para intermediar as solicitações dos titulares dos dados pessoais, com a pessoa natural ou jurídica responsável pelo tratamento destes dados. A lei obriga as entidades públicas a darem ampla publicidade dos contatos do Encarregado de Dados Pessoais para que não haja dúvida a quem direcionar as solicitações.

Os Princípios que fundamentam a LGPD:

Privacidade, liberdade, neutralidade, autodeterminação.

Princípios de proteção de dados expressos no art. 6º da LGPD:

Boa Fé**,** finalidade**,** adequação, necessidade, livre Acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização, prestação de contas.

A autodeterminação informativa está na Lei Geral de Proteção de Dados (LGPD), Lei 13.709 /2018, em seu art. 2o, inciso II. Para MENKE (2021), é possível dizer, que dos fundamentos presentes no art. 2o da LGPD, a autodeterminação informativa é aquele guarda, juntamente com o respeito à privacidade, a relação mais

próxima com a disciplina de proteção de dados pessoais. Isso porque consiste no único presente no rol dos incisos dos dispositivos que tem sua origem atrelada a esta matéria, que nos dias de hoje ganhou contornos de autonomia.

São exemplos de normas da primeira geração, no âmbito europeu, as leis do Estado alemão de Hesse (1970), a Lei de Dados da Suécia (1973), o Estatuto de Proteção de Dados do Estado alemão de Rheinland-Pfalz (1974) e a Lei Federal de Proteção de Dados da Alemanha (1977). Nos EUA, foram aprovados nesse mesmo período o Fair Credit Reporting Act (1970), com foco na regulação dos relatórios de crédito dos consumidores, e o Priva Act. (1974), aplicável à administração pública. (LAURA, p. 29)

Legislações nacionais se seguiram importantes instrumentos internacionais e transnacionais que contribuíram para a consolidação de um conceito de privacidade ligado à proteção de dados pessoais. Destacam-se, nesse contexto, a Convenção 108 do Conselho da Europa (1981), as Diretrizes da OCDE para a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais (1980) e a Diretiva Europeia 95/46/CE relativa à proteção de dados pessoais (1995).

Na evolução do conceito de privacidade, a decisão do Tribunal Constitucional alemão, no julgamento da “Lei do Recenseamento de População, Profissão, Moradia e Trabalho” de 25-3-1982, é considerada uma referência. Nesse julgamento histórico, o Tribunal radicalizou o conceito do livre controle do indivíduo sobre o fluxo de suas informações na sociedade e decidiu pela inconstitucionalidade parcial da referida lei, ao argumentar a existência de um direito à “autodeterminação informativa” (informationelle Selbstbestimmung) com base nos artigos da Lei Fundamental que protegem a dignidade humana e o livre desenvolvimento da personalidade, respectivamente, Art. 1 I GG e Art. 2 I GG9

3. A VISÃO DO STF E CONSTITUCIONALIZAÇÃO DO DIREITO À PROTEÇÃO DE DADOS

A Emenda Constitucional nº 115, de 2022, inclui no texto constitucional a competência privativa da União legislar sobre proteção de dados pessoais. O Congresso Nacional buscou evitar que surgissem diplomas legislativos estaduais e municipais tratando o tema de forma diversa, o que poderia dificultar a adequação de produtos e serviços decorrente da diversidade legal, por tratarem assuntos correlatos de formas muito distintas. Dada a importância da proteção de dados pessoais, é necessária uma legislação nacional uniforme capaz de centralizar as questões mais relevantes.

O marco no ordenamento jurídico brasileiro, o caso do IBGE, em que posicionamento adotado pelo STF em abril de 2020, quando do julgamento da Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387/DF*, também chamado de Caso IBGE: BRASIL. Supremo Tribunal Federal. Medida Cautelar em Ação Direta de Inconstitucionalidade 6.387. Requerente: Conselho Federal da Ordem dos Advogados do Brasil - CFOAB. Relatora: Min. Rosa Weber. Brasília, 24 de abril de 2020. Disponível em http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165.

Na oportunidade, a decisão foi reproduzida nas Ações Diretas de Inconstitucionalidade - ADIs 6388, 6389, 6390 e 6393, tendo em vista igualmente impugnarem a validade constitucional da MP.

Proposta pelo CFOAB, a ADI fazia frente à Medida Provisória 954, de 17 de abril de 2020, que determinava a empresas de telefonia fixa e móvel que compartilhassem dados não anonimizados de milhões de usuários com o IBGE. A lista de informações envolvia nomes, números de telefones e endereços dos consumidores, pessoas físicas e jurídicas.

A liminar que suspendeu a MP foi concedida em abril de 2020, em razão da ausência de indicação expressa de sua finalidade e demonstração do interesse público que se visava alcançar, além de não explicitar como e para que fim seriam utilizados os dados coletados. Ainda conforme o entendimento da relatora, Ministra Rosa Weber, permitir a liberação de dados de pessoas naturais e jurídicas por empresas de telefonia ao IBGE poderia causar “danos irreparáveis à intimidade e ao

sigilo da vida privada de mais de uma centena de milhão de usuários". O voto de Rosa Weber menciona as origens do direito à privacidade e cita o artigo The right to privacy, de Samual D. Warren e Louis Brandeis.

Sobre a decisão do STF no caso IBGE, "comparável ao julgamento da Corte constitucional alemã de 1983 que, de forma pioneira, estabeleceu o conceito de autodeterminação informativa naquele país, posteriormente influenciando e moldando os debates internacionais sobre proteção de dados." (MENDES, Laura Schertel). Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais. JOTA, São Paulo, 10 maio 2020.

O direito à privacidade veda a comunicação de tudo que é privado, pois se isso acontecer sob a guarda da lei, como, por exemplo, em um Tribunal ou em uma Assembleia Legislativa, não há violação desse direito (MENDES, 2014, p. 28)

4. LEI GERAL DE PROTEÇÃO DE DADOS: COMPETÊNCIAS DOS PODERES E ÓRGÃOS

A Autoridade Nacional de Proteção de Dados é o órgão federal responsável por dar efetividade à LGPD no País. As principais competências da ANPD são zelar, implementar e fiscalizar o cumprimento da LGPD, além de orientar e explicar para a população como a Lei Geral de Proteção de Dados Pessoais é aplicada no Brasil.

O inciso XIX delimita a figura da Autoridade Nacional de Proteção de Dados, que é órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da lei. Foi formalmente instituída por meio da Medida Provisória 869/2018.

A MEDIDA PROVISÓRIA Nº 1.124, DE 13 DE JUNHO DE 2022 Altera a Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais, transforma a Autoridade Nacional de Proteção de Dados em autarquia de natureza especial e transforma cargos em comissão.

A ANPD se articula com outras entidades e órgãos públicos a fim de garantir o cumprimento de sua missão institucional, atuando como órgão central de interpretação da LGPD e do estabelecimento de normas e diretrizes para a sua implementação. (https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes-2013-anpd)

A LGPD determina, por exemplo, no art. 55-J, XXIII, que a ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com maior eficiência e promover o adequado funcionamento dos setores regulados. Da mesma forma, no art. 55-J, XXI, a LGPD determina que a ANPD deve comunicar às autoridades competentes as infrações penais das quais tiver conhecimento.

Nesse sentido, a ANPD já celebrou acordos de cooperação técnica com a Secretaria Nacional do Consumidor do Ministério da Justiça e da Segurança Pública, com o Conselho Administrativo de Defesa Econômica - CADE, com o Tribunal Superior Eleitoral – TSE e com o NIC.br. Clique aqui para consultar a íntegra dos acordos de cooperação técnica celebrados. A ANPD também desenvolve ações em

cooperação com outros órgãos públicos com vistas à proteção dos dados pessoais dos titulares.

É importante observar que a aplicação das sanções previstas na LGPD compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública, conforme o art. 55-K.

4.1. JUDICIALIZAÇÃO DA PROTEÇÃO DE DADOS PESSOAIS

Em seu trabalho, Souto[1] constata que as demandas sociais possuem uma dinâmica mais célere do que a resposta legal e judicial, que costuma vir a posteriori. No caso específico de proteção de dados, por se tratar de temática altamente entrelaçada com recursos tecnológicos cada vez mais avançados, a ausência de parâmetros legais robustos e compatíveis com a complexidade envolvida traz inúmeros impactos, não só para os indivíduos como para a própria justiça.

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

No contexto europeu, de acordo com Zanatta (2020)[2], faz parte da cultura utilizar-se em larga escala da esfera administrativa para a apreciação de demandas relativas aos interesses difusos na proteção de dados, com fundamento no art. 80 do GDPR: O titular dos dados tem o direito de mandatar um organismo, organização ou associação sem fins lucrativos, que esteja devidamente constituído ao abrigo do direito de um Estado-Membro, cujos objetivos estatutários sejam do interesse público e cuja atividade abranja a defesa dos direitos e liberdades do titular dos dados no que

[1] SOUTO, Leticia Soares. Open Banking e a Lei Geral De Proteção De Dados – LGPD, Segurança Jurídica e Transparência das Informações: p. 33 e seguintes. Brasília, Centro Universitário de Brasília 2020.
[2] ZANATTA, Rafael A. F. Tutela coletiva e coletivização da proteção de dados pessoais. Temas atuais de proteção de dados: p. 345 a 373. São Paulo: Thomson Reuters Brasil, 2020.

respeita à proteção dos seus dados pessoais, para, em seu nome, apresentar reclamação, exercer os direitos previstos nos artigos 77.o, 78.o e 79.o, e exercer o direito de receber uma indemnização referido no artigo 82.o, se tal estiver previsto no direito do Estado-Membro.

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

Zanatta[3] destaca, ainda, em seu artigo, alguns exemplos de grande repercussão de casos que foram judicializados no Brasil em temas de proteção de dados:

Ano: 2016

Autor(es): MPF/PI

Réu: Google Fundamentação: Coleta de dados (Gmail) sem consentimento informado, violando Marco Civil da Internet e CDC

Danos morais coletivos: R$ 1.000.000,00 (um milhão de reais) Resultado: Improcedente (1ª Instância).

Ano: 2017

Autor: MP/RJ e Defensoria Pública

Réu: Fetranspor

Fundamentação: Cessão ilegal (sem licitação) do serviço público de Bilhete Único a empresa privada. Comercialização indevida de dados pessoais dos usuários de transporte público.

Valor: R$ 260.000.000,00 (duzentos e sessenta milhões de reais)

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

Resultado: Liminar concedida ao autor

Ano: 2018

Autor: MPDFT

Réu: Banco Inter

Fundamentação: Incidente de segurança e exposição ilegal de informações financeiras de clientes

Valor: R$ 10.000.000,00 (dez milhões de reais)

Resultado: ACP encerrada após assinatura de Termo de Ajuste de Conduta e repasse de recursos ao Fundo de Direitos Difusos

---

Ano: 2018

Autor: Instituto Brasileiro de Defesa do Consumidor Réu: Via-Quatro (concessionária da Linha Amarela – Metrô/SP)

Fundamentação: Tratamento de dados biométricos sem informação adequada e sem consentimento

Valor: R$ 100.000.000,00 (cem milhões de reais)

Resultado: Liminar concedida, com efeito suspensivo

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

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

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

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

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

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

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

> Sob a ótica da Lei Geral de Proteção de Dados Pessoais – LGPD fica claro que a empresa ré faz tratamento de dados pessoais de forma totalmente ilegal/irregular gerando prejuízos aos titulares dos dados pessoais.
>
> Sob a mesma ótica, ajuizou outra ação civil pública o MPDFT, com pedido de tutela de urgência, em face de fornecedor flagrado comercializando bancos de dados pessoais no site de comércio eletrônico Mercado Livre.[4]

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

> Tal prática, portanto, está em patente confronto com o princípio constitucional da inviolabilidade do sigilo de dados, insculpido no artigo 5º, XII, da Constituição Federal e o fundamento do respeito à privacidade, previsto no artigo 2º, I, da Lei Geral de Proteção de Dados Pessoais, sem prejuízo de outros Diplomas Legais aplicáveis à espécie, a demonstrar a probabilidade do direito invocado. O perigo de dano, por sua

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

> vez, dessai da persistente violação à privacidade dos titulares dos dados, a tornar impositiva a suspensão do comércio erigido pelo réu [...] (grifo nosso).

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

CAPÍTULO II. A ADAPTAÇÃO DO SETOR PRIVADO À NOVA NORMA

A concretização do direito a proteção de dados exigiu que os setores publico e privado se preocupassem em se adaptar e responder as suas correspondentes obrigações. Sistemas de ganhos de valor e vantagem sobre dados os quais antes não previam necessidade de garantia de direitos da sociedade civil, houveram de formular soluções para que pudessem continuar atuando com ganhos sobre tratamento de dados massivo. Temas como a monetização de dados e *open banking* adviram nesse sentido. No entanto, permanecem latentes os riscos de desobediência a obrigações legais sobre o direito a proteção de dados nas relações dos particulares entre si e nas relações entre sociedade civil e governos, como será observado no caso das instituições financeiras brasileiras e o Governo Federal em acordos de cooperação.

5. A MONETIZAÇÃO DE DADOS APÓS A LGPD

A monetização de dados é a capitalização de referências informativas de indivíduos com o intuito de gerar ou agregar valor as linhas de produção por meio de maior previsibilidade das necessidades e expectativas de consumo, de modo a gerar maior economicidade. Na era da informação em curso, baseada em uma sociedade de consumo, as bases de dados são valiosas fontes de recurso. No entanto, as bases de dados não alcançam o objetivo da economicidade e alavancagem de valor *de per si*. São necessários cruzamentos de informações por meio de *data analytics* sobre *big data,* que permitam a conversão de um grande volume de dados em informações precisas e especificas, com valor monetário plausível correspondente, e que permitam a racionalização da cadeia produtiva, ao modo *just in time*, isto ‘e, sem a necessidade de formação de estoque permanente de produtos, por exemplo. Assim, diminui-se os custos com retenção de estoque, por exemplo. Alcança-se, assim, a razão maior num sistema capitalista, o seu excedente, o lucro.

Big data contempla a captação, armazenamento, processamento e capitalização de dados. O tratamento do grande volume de dados possibilita o direcionamento de publicidade de acordo com o perfil de uso de programas e aplicações. O próprio padrão de comportamento do usuário, tais como o padrão e preferencias de consumo, desde os movimentos e cliques do cursor na tela, são dados que podem ser capturados e utilizados para fins de definição dos locais de inserção de propagandas na tela onde captasse maior atenção do consumidor, por exemplo. Outras utilidades do tratamento desses dados são a definição do tipo de propaganda e produto a serem apresentados, de maneira a influenciar o comportamento de consumo.

Assim, a monetização de dados reflete o valor da vantagem que se adquire com a utilização na geração de informações pela economicidade, assertividade e abrangência da produção, além da definição dos perfis de consumo dos usuários. Organizações que não se valerem de tal vantagem, certamente terão dificuldades de se manter no mercado (GUIMARAES, 2018).

Na medida em que a monetização de dados avança em prol da personalização de comunicações e serviços, deu-se necessária a edição de lei que protegesse o direito a autodeterminação informativa e a intimidade dos indivíduos. Se, de um lado, os setores público e privado prezam pela customização das informações e arquitetura

de perfis de consumo rumo a eficiência e economicidade, do outro lado do balcão, os indivíduos devem ter a garantia de que o direito à privacidade seja observado, não apenas com o intuito se utilizar dados pessoais de forma a garantir que o indivíduo não seja incomodado pela má gestão dos dados. Mais que isso, busca-se evitar que o cidadão seja transformado em números e projeções mercadológicos, desconsiderando-se seus aspectos subjetivos e, por consequente, sua intimidade (LIMBERGER, 2008, p. 219). O direito a intimidade tratada por Limberger (2008) no tocante a proteção de dados tem forte correlação com a autodeterminação informativa nativa do direito alemão, princípio do direito a proteção de dados.

Os indivíduos atualmente têm pouco ou quase nenhum controle sobre o rastreio da circulação de seus dados pessoais inseridos na *internet* ou disponibilizados para organizações. Chiara Teffé (2017, p. 122) propõe que "a velocidade da circulação da informação é inversamente proporcional à capacidade de seu controle, retificação e eliminação."

Por outro lado, houve evolução da consciência dos indivíduos sobre a entrega indiscriminada, excessiva e voluntária de seus dados pessoais, precipuamente após notáveis escândalos de má gestão de dados pessoais por agentes de tratamento.

Para além do volume e qualidade de dados pessoais compartilhados por indivíduos-titulares dos dados, e para além da qualidade da gestão dos dados por agentes de tratamento, a monetização de dados se apresenta como um fator que ultrapassa alguns limites ético-morais. Ademais, alguns desses limites podem influir em questões-chave da economia, da política e até mesmo da democracia como forma de governo, como para Aristóteles[5].

O caso envolvendo a extinta Cambridge Analytica e o Facebook 'e um bom exemplo. Enquanto o Facebook tão somente pretendia monetizar os dados de seus usuários, valendo-se dos respectivos aceites de termos e condições generalistas de privacidade de dados que lhes apresentava, donde constava autorização livre e

[5] ARISTÓTELES. Política. Tradução do grego, introdução e notas do Prof. Mário da Gama Kury. 3 ed.. Brasília: UNB, 1997. 317p.. ISBN: 85230001109.

irrestrita de uso e transferência dos dados pelo seu cessionário (Facebook), a Cambridge Analytica, ao adquirir os dados por determinado valor monetário, utilizou-se deles para prestar serviços de inteligência e manipulação de perfis. Tal conduta por parte da empresa inglesa influenciou diretamente a opinião publica quanto aos pleitos eleitorais dos Estados Unidos e quanto ao referendo da saída do Reino Unido da Uniao Europeia, o Brexit.

Assim, consiste em problema maior para a coleta de volume massivo a forma como serão tratadas as informações e como se garantira sua proteção. Alguns sítios da internet apresentam política de privacidade e proteção de dados dos clientes, porém de maneira generalista, sem especificações sobre percurso dos dados, armazenamento, finalidade ou tempo de permanência antes do descarte. Tal abertura possibilita que dados sejam monetizados por mais tempo do que sequer teriam sido autorizados pelo seu titular a serem armazenados.

Os dados pessoais de um indivíduo são disponíveis, assim como se reflete na Lei Geral de Proteção de Dados por meio do consentimento, por exemplo. A Lei visa garantir a liberdade do titular a fim de que decida sobre sua privacidade, isto ‘e desde que seja uma decisão livre, voluntária e consentida, a disponibilidade dos dados pessoais ‘e a regra.

Ao passo que as relações entre particulares compõem continuamente como sujeitos temas éticos e jurídicos antes mencionados, o setor publico tem como desafio observar como lidar com essas relações jurídicas e como garantir a soberania estatal.

Pierre Levy (1999, p. 312) discorre sobre o caráter desterritorializante do ciberespaço. Por sua constatação, entende que o mundo virtual, onde acontecem negócios jurídicos antes detidos pelos Estados e devidamente controlados por meio de alfandegas e fiscalizações, vem desde a solidificação do mundo das redes a limitar a atuação estatal. O ciberespaço permite facilmente que reste ineficaz qualquer controle estatal sobre as informações oriundas de serviços ou outras relações jurídicas, desde que os servidores podem estar pulverizados, em paraísos de dados, ou nos antípodas – isto ‘e, em local onde a jurisdição estatal não alcance, nem mesmo em termos de direito internacional. Bem mais, as leis, normas e regulamentações de um determinado Estado restariam inférteis de efeitos sobre tais relações.

Extrai-se do anteposto, que haveria preocupação primordial por parte dos estados-nação em se estabelecer a quais regramentos de ordenamentos jurídicos estariam sujeitas às operações de monetização de dados pessoais internacionais. Com o tema se preocupam, como já mencionado, órgãos internacionais como a OCDE. Outrossim, ao se alcançar um parâmetro legal adequado, não somente o haveria maior segurança jurídica interna como também haveria maior segurança a ordem soberana estatal.

Nesse arcabouço, a segurança cibernética se faz a maior aliada da manutenção da soberania de um país. O que leva a permear uma das maiores tecnologias utilizadas atualmente para o tema, o *blockchain*[6], definido por uma cadeia de dados bloqueada por validações em cadeia, a qual duplica os dados por uma rede aberta, de modo que todas as pessoas na *blockchain* possam ver suas atualizações simultaneamente e todas as atualizações sejam validadas através de um processo de verificação pública, sem a necessidade de um banco centralizado de dados como controle.

A tecnologia *blockchain* vem sendo utilizada pelo governo brasileiro em processos gradativamente, e um campo de utilização ‘e para acesso a transações de dados entre particulares como controlador.

[6] Blockchain - o que é e qual sua importância? Disponível em: https://www.sas.com/pt_br/insights/analytics/blockchain.html. Acesso em: 9 mar. 2020.

6. OPEN FINANCE E A LGPD

6.1. A implementação do Open Banking no Brasil

Segundo Domingues e Paravela (2021)[7], o Open Banking, surgiu no Reino Unido e iniciou o seu processo de criação, por meio de sua autoridade reguladora concorrencial em 2016 e se expandiu para outros países. O Open Banking conta com recomendações da OCDE, refletindo em temas de interesse econômico entre países signatários e aspirantes.

Por conseguinte, o Banco Central do Brasil (BC) divulgou os requisitos fundamentais para a implementação no país, isto é, definição dos objetivos, definições, escopos do modelo, estratégias de regulação e as ações para a implementação.

O objetivo exposto como motivo foi o de aumentar a eficiência no mercado de crédito e de pagamentos no país, de forma a promover um ambiente de negócios mais inclusivo e competitivo, mas que preservasse a segurança do sistema financeiro, bem como a proteção do consumidor. A possibilidade de que o sistema financeiro aberto – tradução livre de *Open Banking* – comportasse acesso compartilhado entre as instituições financeiras aos dados pessoais de consumidores, permitiria a oferta de produtos e serviços bancários especializados para cada cliente, trazendo a objetivada eficiência e competitividade.

O Open Banking no Brasil evoluiu para outras fases, nominadas *Open Investment* e *Open Finance*. No mercado financeiro brasileiro, há o desenvolvimento por parte de entidades que não tem são financeiras, mas adentraram no mercado como atividade secundaria, como ‘e o caso das empresas de varejo, que desenvolveram cartões de crédito com marca própria, sistemas próprios de pagamentos e até concessão de créditos como bancos comerciais comuns – entidades com devida autorização de funcionamento para tais finalidades pelo Banco Central do Brasil (BC). Isto posto, se, num primeiro momento, o Open Banking contemplava somente bancos tradicionais e bancos propriamente ditos, nas fases de

[7] DOMINGUES, Juliana Oliveira; PARAVELA, Tatyana Chiari. OPEN BANKING: A IMPLEMENTAÇÃO DO SISTEMA FINANCEIRO ABERTO NO BRASIL NA PERSPECTIVA DO CONSUMIDOR. Revista da PGBC – V. 15 – N. 2 – Dez. 2021. ARTIGOS

Open Investment e Open Finance foram abarcadas todas as instituições com algum tipo de serviço financeiro prestado aos consumidores. Isto ‘e dizes que todas essas entidades puderam compartilhar dados entre si.

Por enquanto, apenas as instituições financeiras autorizadas pelo BC podem atuar no sistema financeiro aberto; entretanto, a tendência mundial demonstra que é apenas questão de tempo para que o Open Banking também esteja disponível para além do mercado financeiro, atingindo as gigantes da tecnologia. Há que se ressaltar que as bigtechs já possuem em grande medida a detenção dos dados pessoais, porém não financeiros, dos consumidores devido a sua inserção que já é sólida no mercado digital. Futuramente, caso elas possuam os dados pessoais financeiros dos consumidores, podemos ver seu poder de mercado se expandir, com eventual monopólio em diversos mercados.

A propulsão para o desenvolvimento de projetos globais de sistemas abertos de dados foi justamente a necessidade de se garantir acesso a informações de indivíduos num contexto de iminência de promulgações de normas legais sobre proteção de dados. Para se responder a essa barreira de acesso a informações de consumidores e livre compartilhamento por parte do sistema financeiro, criou-se o *Open Banking*, quase como que uma cartilha para que os consumidores consentissem com o compartilhamento de seus dados. Como apresentado ao longo do presente trabalho, a palavra consentimento ‘e de suma importância para fins legais e principiológicos do direito a proteção de dados, de modo que a implementação do *Open Banking* – ou *Open Finance* – visou, além do desenvolvimento de mercados, o desenvolvimento de mercados seguros juridicamente.

Da Resolução Conjunta 1/2020 do Banco Central do Brasil, o artigo 3º, os objetivos do Open Banking: i) incentivar a inovação; ii) promover a concorrência; iii) aumentar a eficiência do Sistema Financeiro Nacional e do Sistema de Pagamento Brasileiro; e, por fim iv) promover a cidadania financeira.

Ainda da Resolução conjunta, o princípio da reciprocidade é tentativa de aumentar a concorrência do mercado financeiro, assegurando que as instituições participantes do sistema financeiro aberto tenham também a obrigação de transmitir as informações dos clientes, desde que de forma consentida, para outras instituições. Destarte, todos os bancos que queiram receber as informações de outros

consumidores devem também estar dispostos a compartilhar as informações de seus clientes quando requerido.

O artigo 11 da Resolução 1/2020 impõe que o consumidor terá acesso aos dados que tenham sido compartilhados com as outras instituições, dado que corrobora

6.2. A proteção dos dados do consumidor no Open Banking e possíveis reflexos

Embora haja argumentos sobre os benefícios que o *Open Banking* oferece, é imperioso que a construção do arcabouço regulatório também seja capaz de garantir a proteção do consumidor, precipuamente no que tange à proteção de dados pessoais.

Nesse sentido, a Secretaria Nacional do Consumidor firmou Acordo de Cooperação Técnica (Senacon) com a Autoridade Nacional de Proteção de Dados (ANPD), em 2021, de modo a fortalecer a preocupação e a atividade interinstitucional nos temas que vão envolver a portabilidade de dados do consumidor, de modo a privilegiar as investigações de incidentes de segurança.

Nessa perspectiva, é importante que os consumidores se sintam seguros com relação ao sistema eletrônico e ao banco de dados, principalmente considerando os diversos ataques cibernéticos que ocorreram nos últimos tempos.

Luiz Sergio Vieira (2020)[8], CEO da EY, lembra que:

> Na pandemia do coronavírus, os brasileiros aceleraram sua digitalização, e um dos setores mais impactados com esse movimento foi o financeiro. Segundo o estudo Future Consumer Index, realizado pela EY com 1.112 consumidores entre maio e junho, 46% dos entrevistados aumentaram o uso de meios digitais para pagamento. Além disso, 59% passaram a usar mais o banco online. O impulso à digitalização deu-se claramente pelo fato de que a mudança em nossos hábitos ocorreu do dia para a noite. Evitamos o acesso às lojas físicas, diminuímos o uso de cédulas de dinheiro e intensificamos o pagamento de produtos e serviços pelo celular. Estamos nos adaptando a essas mudanças e aprendendo a fazer escolhas que levam em conta esse novo momento das nossas vidas.

Em 2019, o BC decidiu criar o sistema, inspirado pela Inglaterra, onde o movimento acontecia com êxito. E, em um ano, foi formado todo o arcabouço

[8] VIEIRA, Luiz Sergio. As melhores estratégias para conquistar clientes com a entrada em vigor do open banking. Site: https://www.ey.com/pt_br/audit/as-melhores-estrategias-para-conquistar-clientes-com-a-entrada-e. Data: 18 de setembro de 2020. Acessado em 20/09/2022.

regulatório para isso. Mas somente a regulação não é suficiente para dar impulso ao open banking.

Tão importante quanto o ambiente regulatório favorável é atrair consumidores para o sistema aberto. Isso porque a regulação está construída em cima do consentimento do cliente, ou seja, só funcionará se ele optar por aderir ao novo sistema para, depois, suas informações poderem ser compartilhadas. Mas, para haver consentimento, é necessário, primeiro, que haja sentimento positivo do cliente: ele precisa estar disposto a mudar. Neste sentido, um outro estudo da EY, o Open Banking Opportunity, mostrou que há espaço para as empresas financeiras. No Brasil, 33% dos entrevistados estão positivos com a introdução do open banking, colocando o Brasil na 4ª posição de sentimento favorável de clientes na comparação com outros 12 países.

Essa predisposição, aliada à regulação e à transformação digital impulsionada pela covid-19, criou o ambiente perfeito para a consolidação do open banking. No entanto, é preciso entender como o sistema financeiro aberto vai inspirar esse sentimento positivo — por exemplo, por meio de educação financeira, quais medidas antifraude e de respeito à privacidade de dados podem ser tomadas pelas instituições bancárias. Desse modo, será visto na prática o quanto os consumidores estarão abertos ou não a adotarem o novo modelo.

São eles: ter na palma da mão as informações e os produtos que eu preciso; resolver minhas questões financeiras quando quiser; possibilidade de customizar o serviço do jeito que me agrada e pagar menos (ou ter a percepção de que se paga menos) por serviços financeiros. O ponto crucial para o sucesso do open banking é que a sua adoção será maior quanto maior forem as garantias do consumidor em relação à privacidade e gestão de risco de terceiros sobre seus dados financeiros.

Outra característica da digitalização bancária e do open banking é que são atraídas para o sistema financeiro as empresas que historicamente não atuavam nessa indústria. Os maiores varejistas têm oferecido serviços financeiros a seus clientes, seja por meio de um serviço próprio, seja em parceria com alguma instituição bancária tradicional. Entre as ofertas estão os meios de pagamento online e as carteiras digitais que vêm ganhando espaço para além dos já tradicionais cartões de crédito com marca própria.

E não são só eles: até mesmo empresas B2B já aderiram a esse movimento. Com muito capital para investir, podem mudar drasticamente a maneira como se relacionam com revendedores, pontos de venda e clientes finais. Como exemplo, uma grande distribuidora de combustível tem oferecido plataformas de pagamento no posto não apenas para facilitar o processo de abastecimento do carro, mas para ter acesso ao comportamento do cliente e fideliza-lo com promoções e descontos.

6.3. OPEN BANKING: UM MODELO BASEADO EM API

O sistema financeiro se insere na tendência do aumento exponencial de dados capturados dos usuários e do tratamento desses dados para a realização de análises comportamentais e definição de perfis de consumo com o objetivo de oferecer produtos e serviços, conforme se extrai do trabalho de Souto (2020)[9]

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

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

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

Para compreender a proposta do open banking é importante entender que este é um modelo de negócio fundamentado em tecnologia e ciência de dados, que propõe

[9] SOUTO, Leticia Soares. Open Banking e a Lei Geral De Proteção De Dados – LGPD, Segurança Jurídica e Transparência das Informações: p. 30 e seguintes. Brasília, Centro Universitário de Brasília 2020.

a utilização de APIs (*Application Programming Interfaces*) para a integração de softwares e compartilhamento de informações entre diferentes instituições.

Esse tipo de estrutura é caracterizado pela flexibilidade na gestão de uso, design, além de convergir com o processo de inovação. O nível de abertura da API está diretamente relacionado ao seu potencial alcance e a sofisticação de suas funcionalidades. A proposta de open banking se baseia na troca de informações por APIs abertas. Ou seja, uma API que permite a possibilidade de acesso por terceiros, de fora da organização.

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

6.3.1. OPEN BANKING NO BRASIL

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

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

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

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

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

A proposta do open banking, na visão da autarquia, seria facilitar esse processo de escolha, na busca do consumidor por produtos e serviços financeiros mais adequados à sua realidade e expectativa.

Cabe aqui frisar que as instituições financeiras do Brasil estão sujeitas à Lei Complementar nº 105/2001 (Lei do Sigilo Bancário) e, de acordo com essa norma, as informações referentes a operações ativas e passivas, serviços prestados e grande parte dos dados pessoais dos clientes devem ser especialmente protegidos contra quaisquer acessos, comercializações ou publicizações indevidas, salvo as exceções expressamente previstas na referida Lei Complementar.

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

§ 3o Não constitui violação do dever de sigilo:

I – a troca de informações entre instituições financeiras, para fins cadastrais, inclusive por intermédio de centrais de risco, observadas as normas baixadas pelo Conselho Monetário Nacional e pelo Banco Central do Brasil;

II - o fornecimento de informações constantes de cadastro de emitentes de cheques sem provisão de fundos e de devedores inadimplentes, a entidades de proteção ao crédito, observadas as normas baixadas pelo Conselho Monetário Nacional e pelo Banco Central do Brasil;

III – o fornecimento das informações de que trata o § 2o do art. 11 da Lei no 9.311, de 24 de outubro de 1996;

IV – a comunicação, às autoridades competentes, da prática de ilícitos penais ou administrativos, abrangendo o fornecimento de informações sobre operações que envolvam recursos provenientes de qualquer prática criminosa;

V – a revelação de informações sigilosas com o consentimento expresso dos interessados;

VI – a prestação de informações nos termos e condições estabelecidos nos artigos 2o, 3o, 4o, 5o, 6o, 7o e 9 desta Lei Complementar.

VII - o fornecimento de dados financeiros e de pagamentos, relativos a operações de crédito e obrigações de pagamento adimplidas ou em andamento de pessoas naturais ou jurídicas, a gestores de bancos de dados, para formação de histórico de crédito, nos termos de lei específica. (grifo nosso)

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

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

Conforme observado por Thomaz (2020):

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

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

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

7. ACORDOS DE ACESSO A BANCOS DE DADOS PESSOAIS

BASES LEGAIS (ALEM DA LGPD):

1) LEI Nº 13.019, DE 31 DE JULHO DE 2014.

Art. 1º Esta Lei institui normas gerais para as parcerias entre a administração pública e organizações da sociedade civil, em regime de mútua cooperação, para a consecução de **finalidades de interesse público e recíproco**, mediante a execução de **atividades ou de projetos previamente estabelecidos** em planos de trabalho **inseridos em termos de colaboração**, em termos de fomento ou em acordos de cooperação.

Art. 2º Para os fins desta Lei, considera-se:

VIII-A - acordo de cooperação: instrumento por meio do qual são formalizadas as parcerias estabelecidas pela administração pública com organizações da sociedade civil para a consecução de **finalidades de interesse público e recíproco que não envolvam a transferência de recursos financeiros.**

2) LEI Nº 13.444

Art. 1º É criada a Identificação Civil Nacional (ICN), com o objetivo de identificar o brasileiro em suas relações com a sociedade e com os órgãos e entidades governamentais e privados.

ACORDOS DE COOPERAÇÃO:

1) Acordo de Cooperação FEBRABAN

Espécie: Acordo de Cooperação que entre si celebram a união, por intermédio do Ministério da Economia, representada pela Secretaria de Governo Digital – SGD e a FEBRABAN.

Objeto: Estabelecer parceria entre a SGD/ME e a FEBRABAN, visando ao uso das APIs de Identidade Digital pelos Bancos, em caráter de degustação experimental, para fins de Identidade Digital e aderência à identificação segura de seus Usuários, por

meio da franquia específica de validações, conforme previsto neste Acordo de Cooperação.

Despesa: O presente Acordo não contempla repasse de recursos financeiros entre os partícipes.

Prazo de vigência: O prazo de vigência deste Acordo de Cooperação será de seis meses prorrogáveis por igual período. Prorrogado em 12 de janeiro de 2022.

Data de Assinatura: 20 de julho de 2021.

2) Acordo de Cooperação ABBC

ACORDO DE COOPERAÇÃO Nº 27/2021

Espécie: Acordo de Cooperação que entre si celebram a união, por intermédio do Ministério da Economia, representada pela Secretaria de Governo Digital - SGD, e a Associação Brasileira de Bancos - ABBC

Objeto: Estabelecer parceria entre a SGD/ME e a ABBC, visando ao uso das APIs de Identidade Digital pelos Bancos, em caráter de degustação experimental, para fins de Identidade Digital e aderência à identificação segura de seus Usuários, por meio da franquia específica de validações, conforme previsto neste Acordo de Cooperação.

Despesa: O presente Acordo não contempla repasse de recursos financeiros entre os partícipes.

Prazo de vigência: O prazo de vigência deste Acordo de Cooperação será de 1 (um) ano, a partir da data de publicação do extrato deste Acordo de Cooperação no Diário Oficial da União, podendo ser prorrogado, nas condições previstas no art. 55 da Lei nº 13.019, de 2014, e art. 21 do Decreto nº 8.726, de 27 de abril de 2016, mediante Termo Aditivo.

Data de Assinatura: 5 de janeiro de 2022.

A disponibilização de informações pelo Governo Federal às entidades bancárias representadas pela mencionada Associação violaria a privacidade de dados de 117 milhões de cidadãos brasileiros, direito protegido pela Lei Geral de Proteção de Dados Pessoais (Lei nº 13.079/18).

A Autoridade Nacional de Proteção de Dados - ANPD - não teria sido comunicada dos acordos celebrados, nem teria se pronunciado quanto a esta questão, nem sobre a adequação dos seus termos à Lei. Entretanto, a ANPD se manifestou, a posteriori, em favor da regularidade dos acordos.

O Tribunal de Contas da União – TCU – também teve o entendimento pela regularidade dos acordos de cooperação em apreço.

8. LACUNAS NO DIREITO À PROTEÇÃO DE DADOS DO CIDADÃO E CONSUMIDOR

8.1. HIPERVULNERABILIDADE DO TITULAR DE DADOS

Em diversos ramos do direito, pode-se observar um esforço do Estado na tentativa de minimizar as assimetrias decorrentes da própria dinâmica social inerente ao contexto em que as relações se estabelecem e de trazer mais equilíbrio entre as partes. Nas palavras de Bioni (2020) et Souto (2020)[10], é quando entra em cena:

> O paradigma protetivo que reconhece a posição de vulnerabilidade de certos grupos, dedicando-lhes normas especiais para tutelá-los na exata medida de suas fraquezas. Isso pode ser facilmente percebido nas normas de direito do trabalho e do direito do consumidor. E deve balizar também os aspectos do direito digital, onde se faz necessário o cuidado do legislador na percepção da vulnerabilidade do indivíduo frente ao mercado, que usa as informações como ativos de grande valor, e também em relação a indivíduos mal-intencionados, que atuam à margem ética e legal em nome de interesses escusos diversos.

Conforme trazido por Sarlet e Ferreira Neto apud Facchini Neto e Demoliner (2019), há na sociedade atual: um absoluto descontrole no manuseio, na armazenagem e no acesso dos dados pessoais que estão pulverizados na Internet, o que acaba por fragmentar o nosso senso de privacidade e de personalidade, tornando-nos vulneráveis em relação ao que os demais pensam e falam sobre nossa esfera individual e sobre o nosso passado.

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

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

[10] SOUTO, Leticia Soares. Open Banking e a Lei Geral De Proteção De Dados – LGPD, Segurança Jurídica e Transparência das Informações: p. 21 e seguintes. Brasília, Centro Universitário de Brasília 2020.

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

Para além disso, adentrando ao viés subjetivo da conduta humana, destacam Facchini Neto e Demoliner (2019) que a maior parte dos indivíduos: Não tem paciência (até porque desconhece os riscos) para ler as "políticas de privacidade". Simplesmente 'clica' no botão da 'aceitação' porque de outra forma não conseguiria "criar sua conta" e/ou "perfil" nas redes sociais. E tudo o que mais quer é "participar desse mundo virtual", onde a imagem vale mais do que a realidade. Tudo é urgente, tudo é feito em instantes e ler os "termos de aceitação" – através do qual vende (ou melhor, doa) "sua alma", abrindo mão da sua valiosa privacidade – pode tomar muito tempo e energia, que seriam mais bem utilizados, sob a ânsia do momento, se destinados para postar a próxima selfie ou compartilhar o próximo 'meme'.

Um exemplo de repercussão mundial que demonstra a vulnerabilidade do titular de dados e os riscos atrelados ao uso de informações obtidas por meio de redes sociais foi o caso envolvendo as empresas Cambridge Analytica e Facebook em 2015[11] que, porém, só veio à tona em meados de 2018. No episódio, dados pessoais de mais de oitenta e sete milhões de usuários da rede social foram usados, sem o prévio consentimento dos titulares, por analistas de dados da Cambridge Analytica para construir perfis e modelos de comportamento a fim de influenciar eleitores e direcionar a campanha de determinado candidato à presidência dos Estados Unidos, nas eleições que ocorreram no ano de 2016 (LAPAIRE, 2018).

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

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

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

uma multa equivalente a US$ 5 bilhões de dólares, contabilizando a maior penalidade já aplicada na história da FTC.[12]

A consequência desse tipo de uso indevido dos dados das pessoas, notadamente quanto à finalidade de modificar resultados eleitorais, de acordo com a visão de Martins e Tateoki (2019): obscurece a transparência em torno da pessoa do candidato, notadamente suas ideias e propostas. Com efeito, a transparência em torno do candidato é pedra angular do sistema, visto que é ela que permite ao eleitor fazer sua escolha de forma livre e, sobretudo, consciente. Assim, em um cenário de manipulação do eleitor por propaganda eleitoral direcionada a grupos ou perfis pré-selecionados, a qualidade do voto, como expressão do exercício da cidadania, é severamente prejudicada.

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

Referenciando a perspectiva trazida por Blum (2018), nota-se que o respeito à privacidade do indivíduo tem se distanciado da perspectiva restrita da ótica do segredo e se aproximado cada vez mais da ideia de controle dos dados pelo seu titular: A preocupação que antes era voltada para a tutela do direito a ser deixado só e do direito ao recato, agora está menos voltada à privacidade de certos dados (porque as pessoas sabem que há um certo grau de publicidade) e mais focada no uso destes dados, no fato de o indivíduo poder controlar a forma de coleta, organização e uso das informações.

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

[12] MUNDO CONECTADO. Disponível em: https://mundoconectado.com.br/noticias/v/9883/facebook-vai-pagar-us5-bilhoes-para-encerrar-investigacao-sobre-o-caso-cambridge-analytica. Acessado em: 20/09/2022.

Descumprimento de Preceito Fundamental nº 130 pelo Supremo Tribunal Federal, que derrubou a Lei de Imprensa em 2009: Silenciando a Constituição quanto ao regime da internet (rede mundial de computadores), não há como se lhe recusar a qualificação de território virtual livremente veiculador de ideias e opiniões, debates, notícias e tudo o mais que signifique plenitude de comunicação. (STF - ADPF: 130 DF, Relator: Min. CARLOS BRITTO, Data de Julgamento: 30/04/2009, Tribunal Pleno, Data de Publicação: DJe-208 DIVULG 05-11-2009 PUBLIC 06-11-2009 EMENT VOL-02381-01 PP-00001) (grifo nosso)

Por outro lado, conforme Denardis apud Borges (2019): ao mesmo tempo em que é possível assegurar tais direitos, a internet também apresenta-se como solo fértil para a violação de valores como proteção da propriedade intelectual (...) ciberataques e ameaças à segurança dos próprios. Diante disso, a capacidade de proteger o ciberespaço passa a ser requisito para que qualquer país possa proteger direitos, executar operações de comércio internacional e desenvolver funções públicas essenciais. (grifo nosso) Consolidado o entendimento de que os dados pessoais devem ser protegidos como extensão natural do direito à privacidade, e, considerando o expressivo aumento do volume da troca de informações, da quantidade de dados publicados especialmente nas redes sociais e do interesse econômico na obtenção desses dados pelas empresas, fez-se necessário o estabelecimento de alguns meios de mitigação da vulnerabilidade e dos riscos para os indivíduos que são titulares dessas informações.

Um desses mecanismos, previsto na LGPD, é a anonimização de dados, que consiste em um processo onde o vínculo entre o dado e seu respectivo titular é quebrado, de maneira que não seja possível realizar a associação entre um e outro.

E isso pode ser feito basicamente por meio de quatro espécies possíveis: supressão, generalização, randomização e pseudonimização (BIONI, 2020). Foge ao escopo deste trabalho explorar as formas de anonimização de dados, bastando para o objetivo proposto apenas explicar que a pseudonimização, a exemplo do GDPR, também é trazida pela LGPD como uma forma de mascarar os dados, onde o controlador teria a capacidade de recombinar esse conjunto de dados e novamente identificar o indivíduo. No entanto, conforme versa o §4º do art. 13 da Lei nº 13.709/2018, essa informação adicional capaz de reunir os elementos e montar o

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

Para compreender melhor essas estruturas, é relevante mencionar Machado e Doneda (2018) que argumentam que, do ponto de vista da técnica legislativa e da política de proteção de dados, há duas principais abordagens para a definição de dado pessoal: reducionista e expansionista. Na primeira abordagem, o dado pessoal é tido como: a representação de fatos sobre pessoa identificada, isto é, representação referente a alguém que se conhece e individualiza em meio a certo grupo ou coletividade. O processo de identificação aí operado é possível a partir de elementos informativos chamados identificadores.

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

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

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

Os dados acima evidenciam a persistência de uma conduta inadequada de algumas empresas e o engajamento da sociedade ao buscar a proteção legal no tratamento de seus dados, mas imediatamente também trazem uma reflexão necessária à realidade brasileira: uma vez que o país conta com quase oitenta milhões de processos judiciais em tramitação[13], quais serão as consequências das lacunas e conceitos indeterminados presentes na LGPD para o judiciário brasileiro?

8.2. A INSUFICIENTE PROTEÇÃO DE DADOS NO BRASIL

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

Em artigo, José Renato Gaziero Cella e Rafael Copetti[14], delineia-se que, frente a situações como a descrita o item anterior, possível destacar que o decreto é marcado por uma grande lacuna e não contribui satisfatoriamente para o tema, já que não menciona em nenhum momento o termo “dados pessoais” – optando por falar em “dados cadastrais” e “dados individualizados”.

A especificação da finalidade e a limitação do uso são princípios básicos de leis internacionais dessa matéria e do Projeto de Lei para a Proteção de Dados Pessoais que tramita perante o Congresso Nacional[15]. A noção subjacente é a de que o uso de informações pessoais deve servir à finalidade comunicada na coleta e a outros propósitos compatíveis, nos limites do consentimento do indivíduo.

Com efeito, a finalidade integra os princípios enumerados por Rodotà (2008, p. 60) como norteadores da proteção de dados pessoais, quais sejam:

- princípio da correção na coleta de dados e no tratamento das informações;
- princípio da exatidão dos dados coletados, acompanhado pela obrigação de sua utilização;
- princípio da finalidade da coleta de dados, que deve poder ser conhecida antes que ocorra a coleta, e que especifica na relação entre os dados colhidos e a finalidade perseguida (princípio da pertinência); na relação entre a finalidade da coleta e a utilização dos dados (princípio da utilização não-abusiva); na eliminação ou na transformação em dados anônimos das informações que não são mais necessárias (princípio do direito ao esquecimento);
- princípio da publicidade dos bancos de dados que tratam as informações pessoais, sobre os quais deve existir um registro público;
- princípio do acesso individual, com a finalidade de conhecer quais são as informações coletadas sobre si próprio, obter a sua cópia, obter a correção daquelas erradas, a integração daquelas incompletas, a eliminação daquelas coletadas ilegitimamente;

[14] GAZIERO, José Renato Cella e COPETTI, Rafael. Compartilhamento de Dados Pessoais e a Administração Pública Brasileira. Revista de Direito, Governança e Novas Tecnologias. e-ISSN: 2526-0049| Maranhão | v. 3 | n. 2 | p. 39 – 58 | Jul/Dez. 2017.

[15] Projeto de Lei no 5.276/2016, disponível em http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378. Acesso em 05/09/2022.

- princípio da segurança física e lógica da coleta dos dados.

É por isso que um programa de compartilhamento de dados não pode só ser justificado em termos de eficiência de gestão do Estado, como o governo até agora o fez. Ele precisa instituir garantias aos indivíduos afetados, sob pena de já nascer em descompasso com as discussões mais recentes sobre proteção de dados pessoais, que inclusive vê ocorrendo no Congresso Nacional.

Ressalte-se que, independentemente da definição de privacidade que se adote, deve-se ter uma ampliação da tutela da esfera privada dos sujeitos em virtude do tipo e quantidade de informações que são coletas e, como consequência, gerado um dano ao indivíduo.

Para melhor exemplificação, Rodotà (2008, p. 129) traz efeitos do panorama tecnológico essenciais à privacidade, e a define de forma singela como “o direito de manter o controle sobre as próprias informações” (RODOTÀ, 2008, p. 92):

a) impõe como direito fundamental;

b) especifica-se como direito à autodeterminação informativa e, mais precisamente, como direito a determinar as modalidades de construção da esfera privada na sua totalidade;

c) apresenta-se, por fim, como precondição da cidadania na era eletrônica e, como tal, não pode ser confiada unicamente à lógica da autorregulamentação ou das relações contratuais.

A justificativa trazida pelo autor para estipular tais características inerentes à privacidade é a de que “a descrição de um novo panorama tecnológico e as transformações que traz consigo, se apresentam como um caminho que deve ser percorrido para à plena compreensão dos efeitos sociais resultantes das tecnologias da informação e da comunicação” (RODOTÀ, 2008, p. 127).

Ou seja, “como vivemos em um mundo onde as informações estão divididas com uma pluralidade de sujeitos e a coleta de informações que anteriormente era realizada através de cessões vindas de relações interpessoais e agora ocorre através de transações abstratas, passa-se de um mundo no qual o problema era o controle do fluxo das informações que saiam de dentro da esfera privada em direção ao exterior, para um mundo no qual o problema é o controle das informações que entram,

tal como demonstra a autodeterminação do direito de não saber, pela atribuição dos indivíduos do poder de recusar interferências em sua esfera privada" (RODOTÀ, 2008, p. 128).

Todavia, assumindo os efeitos e seguindo os aspectos da privacidade trazidos por Rodotà, a definição do direito à privacidade compatível com a era moderna-tecnológica se dá como o direito fundamental à autodeterminação e ao controle informativo, decidindo, em sua totalidade, os dados informativos que constroem, adentram e saem da esfera privativa, apresentando-se como precondição da cidadania na era moderna, não sendo restrito à lógica da auto-regulamentação ou das relações contratuais, justificando-se à compreensão dos efeitos sociais resultantes das tecnologias da informação e da comunicação e de um conjunto de condicionamentos.

Porém, como "vivemos em um mundo no qual aumenta o valor agregado das informações pessoais, onde a referência ao valor da pessoa em si e de sua dignidade passou a ser secundário em relação à transformação da informação em mercadoria" (RODOTÀ, 2008, p. 128), o desafio para aplicação do direito à privacidade é constante.

Informações de todos os tipos são coletadas mediante programas ou objetos de interação social. Seja pelo computador ou pelo smartphone, o acesso à uma rede social ou a algum sítio eletrônico da internet, na maioria das vezes se realiza uma pequena coleta de dados por meio de cookies[16] de quem o está utilizando ou acessando para com algum objetivo proposto (expressamente) pelos desenvolvedores, e aceito (tácita ou expressamente) pelos usuários.

> O aumento da quantidade de informações pessoais coletadas por instituições públicas e privadas através de aplicativos de smartphones ou no acesso em rede, de forma geral, visa sobretudo à dois objetivos: por parte dos poderes púbicos, a aquisição de elementos necessários à gestão de programas de intervenção, e o desenvolvimento de estratégias empresariais privadas; conjuntamente ao controle da conformidade da população à gestão política dominante ou aos comportamentos prevalecentes (RODOTÀ, 2008, p. 28).

[16] "Um cookie é um pequeno texto que os sites podem enviar aos navegadores, anexado a qualquer conexão. Nas visitas posteriores o navegador reenvia os dados para o servidor dono do cookie. Um cookie é transmitido até que perca a validade, que é definida pelo site. Os sites geralmente usam os cookies para distinguir usuários e memorizar preferências." http://br.mozdev.org/firefox/cookies. Acesso em 28.out. 2016.

Assim, a caracterização da organização social como uma sociedade com bases na acumulação e circulação das informações torna-se clara, trazendo novas situações e tipos de poder. Este, contudo, problemático ao ser legitimado e fundado na informação. Tais desafios dão-se, “primeiramente, em virtude e a dificuldade de individualizar certos tipos de informações das quais o cidadão estaria disposto a renunciar definitivamente a controlar o seu tratamento e a atividade dos sujeitos que a utilizam, pois publicidade e controle não são termos contraditórios, como são publicidade e sigilo. Em segundo lugar, a nova situação determinada pelo uso de computadores no tratamento das informações pessoais faz-se mais difícil caracterizar o cidadão como simples ‘fornecedor de dados’, sem que a ele caiba algum poder de tutela e tratamento dessas informações (RODOTÀ, 2008, p. 36).

> As informações coletadas, além fazer as organizações públicas e privadas capazes de planejar e executar os seus programas, ainda permitem o surgimento de novas concentrações de poder ou o fortalecimento de poderes já existentes” (RODOTÀ, 2008, p. 37).

Daí a importância da proteção jurídica da privacidade, da vida privada ou da intimidade, cuja definição é trazida por Doneda (2006, p. 101):

Ao se tratar da privacidade, há de se fazer antes de tudo um esclarecimento inicial sobre a terminologia utilizada. A profusão de termos utilizados pela doutrina brasileira para representa-la, propriamente ou não, é considerável; além de ‘privacidade’ propriamente dito, podem ser lembrados os termos: vida privada, intimidade, segredo, sigilo, recato, reserva, intimidade da vida privada, e outros menos utilizados, como ‘privatividade’ e ‘privaticidade’, por exemplo. O fato de a doutrina estrangeira apontar igualmente para uma multiplicidade de alternativas certamente contribui, induzindo juristas brasileiros a experimentar diversas destas.

De acordo com Limberger (2007, p. 116), a intimidade como direito fundamental tem sua gênese na “[…] dignidade humana e está vinculado à própria personalidade, sendo seu núcleo central. Como direito que é da expressão da própria pessoa, desfruta da mais alta proteção constitucional”. Para a autora, “[…] As exigências do mundo tecnológico atual fizeram com que o direito tutelasse essa nova face da intimidade. A intimidade deriva da dignidade humana, é um direito fundamental que integra a personalidade. Das relações da informática e a intimidade se desenvolve a autodeterminação informativa. […]” (LIMBERGER, 2007, p. 119).

Para Rodotá (1995, p. 122), a privacidade é “[…] o direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada […]”.

No direito brasileiro, o direito à privacidade pode ser entendido como um direito da personalidade de matiz constitucional, com expressa previsão no artigo 5º, inciso X, da Constituição da República.

Infraconstitucionalmente, a proteção da privacidade se consubstancia na cláusula geral estabelecida no artigo 21 do Código Civil. Ainda, destaca-se que as previsões legislativas específicas para a proteção de dados são escassas. Tem-se, na Lei Federal no 8.078/1990 - Código de Defesa do Consumidor, a regulamentação dos bancos de dados e cadastros de consumidores em único dispositivo, o artigo 43. Além disso, há a regulamentação do chamado cadastro positivo pela Lei Federal no 12.414/2011, 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.

No presente estudo, assim se define privacidade: [...] um direito fundamental, em sentido amplo, capaz de recepcionar em seu bojo a proteção da vida privada, da intimidade, da imagem, da honra e dos direitos-base vinculados ao conceito de direitos de privacidade na internet, significa dizer que, na contemporaneidade, o direito de navegar na internet com privacidade, o direito de monitorar quem monitora, o direito de deletar dados pessoais e o direito de proteger a identidade online devem ser tutelados, explícita e expressamente, como um dos pilares de garantia da eficácia do direito fundamental à privacidade em sentido amplo. (FORTES, 2015, p. 188).

A proteção dos dados no sistema normativo da União Europeia (UE) é tratada por meio de um sistema de regulamentos e diretivas, na qual é possível encontrar aspectos pioneiros no regramento da matéria. Há registro de legislações, por exemplo, na Alemanha e Suécia desde a década de 1970. Portugal, em 1976, e, posteriormente, Espanha, em 1978, foram os primeiros países a elevar a proteção em nível constitucional, trazendo previsões expressas nas suas respectivas Cartas.

Atualmente, as Diretivas 95/46/CE e 2002/58/CE, e Regulamento 45/2001, trazem diretrizes para os países integrantes da UE. Ganham destaque também os

Relatórios e Comunicações de acompanhamento da implantação e eficiência das normativas (FORTES, 2015, p. 132-133).

Cabe mencionar que desde o início de 2012, foi formada a Comissão Europeia para regulamentação sobre a proteção de dados pessoais. Entre os objetivos expostos, há referência de que:

La Comisión europea quiere modernizar la legislación europea de protección de datos para garantizar la intimidad de los consumidores y hacerla compatible con la libre circulación de datos en la UE . [...]

Las empresas sólo estarán autorizadas a enviar información personal fuera de la UE a países con un nivel similar en sus sistemas de protección de datos. Se trata además de mejorar y simplificar los mecanismos de transferencia internacional de datos. [...]

El objetivo de la nueva estrategia es consolidar un enfoque común en toda la UE. Las divergencias actuales no permiten determinar con nitidez la legislación aplicable en cada caso. Por eso es necesario armonizar las normas y reforzar el poder de las autoridades de protección de datos con el principio de cooperación y coordinación. (COMISIÓN EUROPEA, 2010).

Referidas premissas servem ao mesmo tempo como alerta à constante mutação e evolução da tecnologia e da forma como os dados podem ser armazenados e manipulados. É importante, ainda, considerar a facilidade do intercâmbio de informações e procurar meios para que essa circulação atenda a requisitos de segurança e preservação da privacidade.

A utilização dos recursos tecnológicos alterou significativamente a circulação, a forma de compartilhamento e o armazenamento de dados. A digitalização de documentos e o arquivamento de informações em bancos de dados digitais é cada vez mais significativo.

Nesse contexto, a proteção de dados pessoais nos sistemas jurídicos em geral necessita de uma análise mais criteriosa, principalmente no sistema jurídico brasileiro, no qual não se tem uma legislação específica acerca da proteção dos dados pessoais.

Ao contrário da legislação encontrada em países da Europa, não há no sistema jurídico brasileiro, por exemplo, uma autoridade responsável e independente,

dedicada a preservar o consentimento e o uso de dados pessoais mediante a supervisão do cumprimento das obrigações dos responsáveis pelo tratamento de dados, as quais possuem previsão específica (GALINDO, 2013, p. 136).

De acordo com a normativa europeia, em caso de descumprimento, qualquer cidadão pode reclamar à autoridade de proteção dos dados, a qual estará apta a instaurar procedimento administrativo e aplicar sanções ao responsável. Referida característica, conforme Galindo (2013, p. 137), é relevante, pois: ...se completó este cuadro de derechos y obligaciones con la atribución legal a la autoridad de protección de datos de su obligación de velar por el cumplimiento de las medidas conducentes a evitar la modificación de los datos personales por la utilización de las técnicas de seguridad de las TIC consideradas más adecuadas en cada momento.

A existência de autoridade responsável pela proteção dos dados, com atribuições claras e voltadas a não transgressão dos dados pessoais, afigura-se, portanto, um relevante mecanismo.

A autodeterminação informativa é um direito que orienta até hoje a proteção de dados pessoais na Alemanha e exerce grande influência em países do sistema jurídico romano-germânico. “Concebido como um direito fundamental (...), o direito à autodeterminação informativa proporciona ao indivíduo o controle sobre suas informações” (DONEDA, 2006, p. 196-197).

Em um julgamento (BverfGE 65,1) emblemático do Tribunal Constitucional Federal da Alemanha, de 15 de dezembro de 1983, averiguou-se a constitucionalidade da lei que ordenava o recenseamento geral da população, com dados sobre a profissão, moradia e local de trabalho para fins estatísticos.

Segundo o Tribunal Constitucional Federal da Alemanha, em virtude das condições do moderno processamento de dados, o direito geral da personalidade contido no artigo 2 I GG, em conjugação com o artigo 1 I GG, passa a abranger a proteção do indivíduo contra levantamento, armazenagem, uso e transmissão irrestritos de seus dados pessoais, que somente podem ser utilizados, em princípio, com sua autorização. Essa norma consubstancia um direito geral à autodeterminação sobre a informação, que somente é restringível se houver a contraposição de um interesse predominante da coletividade (SCHWABE, 2005, p. 233-235).

Na construção dessa norma concreta, o Tribunal Constitucional Federal da Alemanha considerou que o direito ao livre desenvolvimento da personalidade abrange o poder do indivíduo de decidir, por si próprio, quando, quais e em que limites os fatos pessoais serão revelados, poder que, diante da evolução tecnológica atinente ao processamento automático de dados, depende de uma proteção especialmente intensa (SCHWABE, 2005, p. 237).

A faculdade contemporânea e futura de armazenamento ilimitado, transmissão instantânea e consulta irrestrita de dados atentaria contra a autodeterminação individual, uma vez que não mais possibilitaria a determinação, com segurança, de quais informações sobre a sua pessoa são conhecidas, nem por quem são acessadas, inibindo substancialmente a liberdade de planejar ou decidir com autodeterminação (SCHWABE, 2005, p. 237).

Esse direito à autodeterminação informativa, porém, não é absoluto, mas restrito quanto às informações de interesse geral predominante, quer dizer, limitável excepcionalmente quando imprescindível para a consecução de um interesse público. Tais restrições exigem uma base constitucional que possibilite o conhecimento, pelo cidadão, de forma clara e reconhecível, dos pressupostos e da extensão das limitações, atendendo ao princípio da transparência do Estado de Direito (SCHWABE, 2005, p. 237-239).

O núcleo da autodeterminação informativa, enquanto relacionada ao aspecto básico do direito à intimidade, constitui-se na faculdade que a pessoa detém de escolher sobre a divulgação e a revelação de informações que diretamente a ela se referem.

Para Doneda (2006, p. 201) a terminologia mais adequada é tão somente “proteção de dados pessoais”, pois estaria englobada tanto a problemática da privacidade quanto a da informação, que teria como ponto de referência os direitos da personalidade e estaria isenta de uma acepção patrimonialista ou contratual, ao mesmo tempo em que não remonta ao direito à liberdade em uma acepção demasiadamente ampla.

A crítica do jurista citado reside basicamente em três fatores. O primeiro é acerca da correta definição do que seja autodeterminação, pois em determinado

sentido poderia dar ao indivíduo a oportunidade de controlar as informações que lhe digam respeito dentro de parâmetros quase ilimitados (DONEDA, 2006, p. 198).

Já para uma segunda leitura, em chave liberal, a autodeterminação concentrar-se-ia no ato do consentimento da pessoa para o tratamento de seus dados pessoais e assumiria contornos negociais, afastando a matéria do âmbito dos direitos da personalidade (DONEDA, 2006, p. 198).

Por fim, outro fator seria a possibilidade de se ter a impressão de que as pessoas teriam um direito de propriedade sobre suas informações, o que as transportaria para o campo das situações patrimoniais (DONEDA, 2006, p. 198-199).

Outro aspecto a ser delimitado é a importância da existência de um órgão responsável pela proteção dos dados pessoais. Trata-se de órgão com diversas atribuições sociais, políticas e jurídicas, pois, como se observa em experiências europeias, além de fiscalizar, controlar e aplicar sanções à violação dos dados pessoais, cabe a promoção de ações educativas e de informação tanto para cidadãos quanto para órgãos públicos.

É preciso delimitar as atribuições, estrutura, composição e observar uma autonomia financeira e política a esse órgão. A vinculação a órgãos governamentais e ligados ao Poder Executivo não é desejável. Ainda, a dependência ao Poder Legislativo, Judiciário ou outros da estrutura jurídico-administrativa (Ministério Público, por exemplo) também podem comprometer a segurança dos dados, notadamente pelo interesse em determinadas demandas. O novo órgão deve ter autonomia e meios efetivos de executar sanções aos infratores, além de organizar as políticas para a conscientização quanto à utilização e guarda de dados pessoais.

Ademais, sua composição deverá ser híbrida e seus integrantes oriundos de diversos segmentos sociais. Ao mesmo tempo em que é importante que se tenha um órgão com conhecimentos técnicos acerca da criação e manutenção de banco de dados é importante que haja uma interdisciplinaridade em seu Conselho administrativo.

Nesse sentido, referidos integrantes poderão advir de diferentes áreas do conhecimento contribuindo para uma melhor regulamentação da legislação protetiva e adequação à realidade das relações sociais e institucionais.

Ao falar sobre a independência de uma autoridade de proteção de dados, Doneda (2006, p. 393) afirma que referida característica pressupõe a presença de "mecanismos de nomeação de seus membros, geralmente limitando a discricionariedade na sua escolha (através, por exemplo, da exigência de determinada formação ou atuação profissional)", além "da incompatibilidade de sua atuação com outras atividades, atuais ou mesmo pregressas (e também futuras [...]), além da limitação temporal de seu cargo" (DONEDA, 2006, p. 393).

Ainda, a independência pressupõe "a ausência de ingerência governamental sobre seus atos, que se pode obter situando tais órgãos fora de uma posição hierárquica em relação ao governo" (DONEDA, 2006, 393-394).

Além da especificidade referente à matéria e da função de velar pelo fiel cumprimento e respeito à lei, interpretando-a e aplicando-a, o ente independente deve ser dotado de poderes para inspecionar e aplicar sanções. É preciso que os responsáveis pelos arquivos mantenham referido órgão informado acerca das características de seu banco, além de, sendo o caso, quando requisitados, deem acesso aos dados que nele constam.

CONSIDERAÇÕES FINAIS

As informações disponibilizadas pela Secretaria de Governo Digital – SGD, ligada ao Ministério da Economia até a feitura do presente trabalho, até o momento são insuficientes para que se conclua, de forma definitiva, acerca da legalidade e legitimidade do tratamento de dados pessoais sensíveis no escopo dos referidos Acordos de Cooperação.

Entretanto, é possível observar que os acordos dizem respeito ao tratamento de dados pessoais sensíveis, que envolvem o Poder Público e mais de 220 instituições privadas, que nos termos do art. 27 deveria terem sido comunicados à ANPD, que até o momento não se pronunciou quanto a esta questão e nem mesmo quanto à adequação dos mesmos à Lei.

É muito evidente a falta de transparência e em consequência dela a incerteza quanto ao cumprimento dos fundamentos, de diversos princípios e hipóteses legais de tratamento estabelecidos na LGPD. Por fim, como visto na definição legal de tratamento de dados, a “eliminação” é uma espécie de tratamento. A eliminação, também conforme a lei, consiste na exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

A “eliminação dos dados pessoais” é um direito do titular. Segundo a Lei, consideradas algumas exceções, “Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades (...)” não fica claro para a sociedade, como, após um ano de degustação, as instituições participantes do convênio vão garantir a eliminação dos dados pessoais que porventura tenham consumido, ou mesmo, se eles serão ou não compartilhados entre a administração pública e as instituições privadas e em que termos.

É urgente:

1. investigar a legalidade de acordo de cooperação 027/2021 entre a Secretaria de Governo Digital – SGD, vinculada ao Ministério da Economia e a Associação Brasileira de Bancos (ABBC) e o acordo de colaboração 016/2021 entre a Secretaria de Governo Digital – SGD, vinculada ao Ministério da Economia e a FEBRABAN e que foi renovado em janeiro de 2022,

2. Acionar a Autoridade Nacional de Proteção de Dados - ANPD, a quem compete a fiscalização administrativa, a Secretaria Nacional do Consumidor (Senacon), a Justiça Eleitoral e as comissões internas do Congresso Nacional para que se pronunciem e o assunto seja tratado com o devido cuidado, além de investigar a legalidade,

3. Solicitar a suspensão da execução dos acordos de cooperação acima citados até que as investigações sejam concluídas e as autoridades competentes se pronunciem.

Caberia aos órgãos e entidades abaixo:

- MP: Fiscalizar e Investigar.
- ANPD: Regulamentar, Fiscalizar e emitir Parecer pela (ir) regularidade com ou sem ressalvas.
- TCU: Fiscalizar e emitir Parecer pela (ir) regularidade dos acordos de cooperação.
- STF: Apreciação, por provocação, em linha com a CRFB/88, seja por bases dos direitos a privacidade e a propriedade, seja pelo direito a proteção de dados como direitos fundamentais.
- Governo Federal: Análise mais cautelosa dos acordos firmados em relação a LGPD e a proteção de dados como direito fundamental.
- Bancos: Análise de riscos: fazer acordos notadamente em desconformidade com a LGPD junto ao Governo de plantão não gera escusa de consciência ou entendimento de que atos administrativos seriam presumidamente impostos, porquanto acordos de cooperação estão no âmbito das parcerias, regidas pelo princípio da livre iniciativa.

REFERÊNCIAS BIBLIOGRÁFICAS

BIONI, Bruno R., MENDES, Laura Schertel. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral brasileira de Proteção de Dados: mapeando convergências na direção de um nível de equivalência. In. FRAZAO, Ana; TEPEDINO, Gustavo, OLIVA, Milena Donato (Coord.)

BOBBIO, Noberto. A Era dos Direitos. 9. ed. Rio de Janeiro: Elsevier, 2004

GARFINKEL, Simson. Database Nation: the death of privacy in the 21th Century. California: O'Reilly Media, 2000.

MENDES, Laura Schertel. Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais. Site: https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020. Acessado em: 25/09/2022. JOTA, São Paulo, 10 maio 2020.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014 – (Série IDP: linha de pesquisa acadêmica)

MELLO, Alexandre Schmitt da Silva, ... [et al.]. Lei geral de proteção de dados: aspectos relevantes ; organizado por Fabiano Menke e Rafael de Freitas Valle Dresh.

Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. Sao Paulo: Thomson Reuters Brasil, 2019.p. 806.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS: Site https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes-2013-anpd acessado em: 25/06/2022

LEI Nº 13.019, DE 31 DE JULHO DE 2014 – LEI DE PARCERIAS PÚBLICO PRIVADAS EM REGIME DE COOPERAÇÃO. Site: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l13019.htm. Acessado em 25/09/2022.

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018 - LEI GERAL DE PROTEÇÃO DE DADOS. Site: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acessado em 25/09/2022.

https://www12.senado.leg.br/ril/edicoes/59/235/ril_v59_n235_p11.pdf.

LÈVY, Pierre. Cybercultura. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 1999.

LIMBERGER, Têmis. Proteção de dados Pessoais e comércio eletrônico: os desafios do século XXI, São Paulo: Vozes, 2008

Open Banking - Guia de implementação da versão 2.0 das APIs de dados cadastrais e transacionais. Site: https://openbankingbrasil.atlassian.net/wiki/spaces/OB/pages/61636643/Guia+de+implementa+o+v2.0+-+Dados+cadastrais+e+transacionais Acessado em: 25/09/2022.

Banco Nacional de Desenvolvimento – Open Finance - Transparência. Site: https://www.bndes.gov.br/wps/portal/site/home/transparencia/open-finance. Acessado em: 25/09/2022.

Revista da Procuradoria Geral do Banco Central: Open Banking - a implementação do sistema financeiro aberto no Brasil na perspectiva do consumidor. Site: https://revistapgbc.bcb.gov.br/revista/article/view/1133/70. Acessado em 25/09/2022.