Centro Universitário de Brasília - UniCEUB
Faculdade de Ciências Jurídicas e Sociais - FAJS

LETÍCIA SALVADOR SANTOS TAVARES

PANORAMA SOBRE A PROTEÇÃO DE DADOS DIANTE DA DIGITALIZAÇÃO DAS INFORMAÇÕES BANCÁRIAS

BRASÍLIA

2020

LETÍCIA SALVADOR SANTOS TAVARES

PANORAMA SOBRE A PROTEÇÃO DE DADOS DIANTE DA DIGITALIZAÇÃO DAS INFORMAÇÕES BANCÁRIAS

Artigo científico apresentado 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: Ricardo Leite

BRASÍLIA

2020

LETÍCIA SALVADOR SANTOS TAVARES

PANORAMA SOBRE A PROTEÇÃO DE DADOS DIANTE DA DIGITALIZAÇÃO DAS INFORMAÇÕES BANCÁRIAS

Artigo científico apresentado 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).

BRASÍLIA, 2020.

BANCA EXAMINADORA

_____

Professor Orientador

_____

Professor Avaliador

PANORAMA SOBRE A PROTEÇÃO DE DADOS DIANTE DA DIGITALIZAÇÃO DAS INFORMAÇÕES BANCÁRIAS DE CONSUMIDORES

Letícia Salvador Santos Tavares [i]

RESUMO

O presente trabalho pretende apresentar um panorama sobre a proteção de dados, inclusive os bancários na era digital e mostrar alguns desafios a serem enfrentados pelo poder público. O objetivo desta pesquisa é propor uma análise acerca do conceito de coleta, armazenagem e utilização de dados, e demonstrar a necessidade de adaptação da legislação já que a sociedade está cada vez mais digitalizada. O método utilizado foi a pesquisa bibliográfica e doutrinária, e almeja-se a confirmação da hipótese através de um processo lógico dedutivo. Por meio dessa análise, estima-se confirmar a hipótese de que a era da digitalização tem trazidos enormes desafios para que um, ou outro Estado, consiga realmente proteger os indivíduos do uso indevido das informações pessoais, e, no caso brasileiro, a jurisprudência é divergente sobre o sigilo e compartilhamento de dados a depender do ente que a requisita. Concluiu-se, portanto, que ainda há um longo caminho para que se encontre uma forma eficiente de controle da rede mundial de computadores, e a forma que as informações pessoais, bancárias e fiscais, sejam de fato e de direito protegidas, sem que haja a violação da privacidade por parte do Estado ou o risco de utilização indevida por qualquer agente público ou particular no processo de transmissão.

Palavras-chaves: Proteção. Dados. Sigilo. Bancário. Privacidade. Digital.

INTRODUÇÃO

Este artigo tem como objetivo apresentar um panorama acerca da proteção de dados de consumidores, com foco aos dados bancários diante da digitalização das informações e como a legislação específica sobre o tema tem regulado os procedimentos. O artigo está dividido em três partes incluindo as considerações finais. Na primeira parte, expõe-se um panorama sobre a história da proteção de dados, o histórico sobre a coleta de dados e como os escândalos de multinacionais e escândalos de troca de dados foram determinantes para a criação de leis para proteger os indivíduos da coleta e utilização indevida de dados de pessoas, com a consequente edição e publicação da Lei Geral de Proteção de Dados no âmbito do ornamento jurídico pátrio. Na segunda parte, aprofunda-se sobre a questão do sigilo

[i] Bacharel do curso de Direito pela Faculdade de Ciências Jurídicas e Sociais-FAJS – (leticia.tavares@sempreceub.com)

bancário, direito à privacidade e sociedade da informação digital, conceitua os termos privacidade, sigilo bancário e sociedade na forma que foram construídas na legislação pátria e a necessidade de suas adaptações à era digital. Na terceira parte, encerra-se com a apresentação dos desafios da proteção de dados bancários na sociedade digital, com a demonstração das formas e dos conceitos relativos a como as instituições bancárias e o Banco Central do Brasil tem regulado o assunto de proteção de dados, especialmente os de informações bancárias com a digitalização dos meios de comunicação. Por fim, as considerações finais apresentam a conclusão deste trabalho.

1 HISTÓRIA DA PROTEÇÃO DE DADOS

Engana-se quem pensa que a sociologia é uma área voltada apenas ao estudo das relações sociais físicas ou movimentos populares e comportamento humano presencial. A sociologia, como instrumento de estudo da interação humana, inevitavelmente levaria o estudo das relações humanas por meio da internet. Jan van Dijk, um importante sociólogo holandês da Universidade Twente, utilizou o termo "sociedade em rede" na sua obra "*De Netwerkmaatschappij"* (A Sociedade em Rede, em tradução própria) de 1999 (ano original da publicação), seguindo termos e ideias da obra teorizada pelo sociólogo espanhol Manuel Castells em 1996, na obra "A Sociedade em Rede", primeira de uma trilogia chamada de "A Era da Informação" (*The Rise of Networking Society – The Information Age: Economy, Society and Culture*).

Esse termo, segundo Van Dijk, refere-se à uma sociedade como um coletivo em que as redes sociais, juntamente com a mídia, constroem a forma de organização social nos âmbitos individuais, organizacionais e sociais. O autor propõe várias premissas e, delas, algumas reflexões inquietantes. Entre elas, uma seria se a expansão da internet poderia representar uma "Revolução Digital", pois representaria uma nova mudança na forma e no jeito de se comunicar (VAN DIJK, 2012).

Certamente o autor não se enganou quando teorizou em 1991 que a internet viria a transformar a comunicação face a face. Para explicar melhor, o autor utilizou como base a conceituação de sociedade de massas (do período moderno), onde esse termo se tornou "sociedade em rede" (VAN DIJK, 2012) ou "sociedade da informação",

como alguns autores, como André Abelha e Alexandre Junqueira Gomide se referem no seu artigo sobre o assunto vindouro desta pesquisa, sobre a Lei Geral de Proteção de Dados (ABELHA; GOMIDE, 2019). A sociedade em rede para Van Dijk, portanto, traria a mudança de que a sociedade, por meio das novas mídias, teria instrumentos de direcionamento da estrutura e da organização de relacionamentos (VAN DIJK, 2012).

Essa abordagem acerca da sociedade da informação, se fez precisa, pois atualmente as comunicações, identificações e interações entre as pessoas se tornam cada vez mais digitais em diversos aspectos do dia-a-dia, com a utilização de aplicativos. Esses aplicativos de acesso individual ou de acesso coletivo, demandam que o sujeito preste informações pessoais, como o nome, cadastro de pessoa física, data de nascimento, informações sobre familiares etc. E exatamente por essa necessidade de prestar informações, que a lei brasileira teve que atentar-se à coleta de dados. Destaca-se que essa abordagem será melhor trabalhada em capítulo posterior.

Para entender melhor esse tema, relata-se momentos históricos internacionais que repercutiram para se pensar em legislações para proteger os dados dos cidadãos. Um dos casos mais conhecidos é o da *Cambridge Analytica* e do *Facebook* (THE GUARDIAN, 2018), que tiveram milhares de dados vazados de seus clientes e utilizados para fins comerciais (venda), o caso das *fake news* durante o plebiscito da saída do Reino Unido da União Europeia (apelidado de *Brexit*), e os escândalos de manipulação eleitoral durante a campanha presidencial de Donald Trump que, segundo a análise de Roncolato, fizeram a União Europeia se mobilizar (RONCOLATO, 2018).

No ano de 1960, nos Estados Unidos e alguns países europeus, começaram os primeiros processamentos de dados em larga escala de forma centralizada. Essa centralização de processamento se deu em razão da proteção de dados, pois se pensava que um único centro de processamento de dados poderia controlar, armazenar e proteger as informações com mais eficiência. Nos Estados Unidos a proteção de dados voltou-se para o setor de crédito e na Europa se voltou para bancos de dados eletrônicos.

Com a criação da Comunidade Econômica Europeia (CEE), foi demandado à época a criação de uma legislação única para a questão de tratamento de dados. Contudo, pelo Tratado de Maastricht (1992), as regulações da União Europeia devem e levam em consideração as particularidades jurídicas de seus integrantes, o que demandaria um longo período de estudos de viabilidade para os membros. Em 1995 foi criada a primeira norma jurídica sobre processamento de dados, a Diretiva 95/46/EC, que estabeleceu procedimentos para a proteção de dados pessoais de cidadãos europeus no âmbito da União Europeia (PLUGAR, 2019).

Já em 2011, o *European Data Protection Supervisor* (EDPS), publicou Opinião (instrumento de emissão de parecer para regulações no âmbito da União Europeia) onde deixava claro a necessidade de aperfeiçoamento da legislação do bloco sobre a proteção de dados pessoais. No ano seguinte, em 2012, o Conselho Europeu *(European Counsil - EC)* apresentou proposta ao parlamento europeu para endurecer as normas regulatórias sobre a privacidade e economia digital. Os anos de 2012 e 2013 foram marcados por debates sobre a proposta, que foi alvo de críticas e apoiadores por todo o mundo (VIDOR, 2019).

Em 2014 o Parlamento Europeu (*European Parliament*) deu apoio para a criação de uma regulação geral sobre proteção dados, que à época foi chamada de *General Data Protection Regulation* (GDPR). Já em 2015 o Conselho Europeu e o Parlamento Europeu firmaram acordo sobre a legislação para que seguissem os tramites legislativos de aprovação (VIDOR, 2019).

A União Europeia em 27 de abril de 2016 regulou a proteção de dados de cidadãos, empresas e governos dos seus membros por meio da *General Data Protection Regulation* (GDPR) ou *Regulation* 2016/679 da União Europeia, que estabeleceu regras para coleta, armazenamento e utilização de dados de cidadãos da união europeia, que deveria ser seguida pelos seus membros e por qualquer outra organização que venha a utilizar os dados de empresas, governos e cidadãos.

No Brasil, o tema restou materializado pela Lei 13.709/2018, uma legislação recente, mas que trouxe um grande panorama regulatório e conceitual sobre dados e a forma que se deverá observar a coleta, proteção, utilização e o armazenamento de dados pessoais dos consumidores. As transformações e exigências da nova lei a

deixaram com um longo *vacatio legis* (24 meses), já que a lei aprovada em 2018 só entrará em vigor no mês de agosto de 2020.

A legislação brasileira não trata a coleta de dados apenas em serviços digitais, mas sim por qualquer pessoa, física ou jurídica (pública ou privada), que trabalhe com coleta de dados pessoais de outras pessoas físicas ou jurídicas. A regulação, como o próprio nome diz, é “geral” e por isso alcança dos diversos âmbitos, além do digital. Abelha e Gomide explicam que aplicação dessa legislação alcança até mesmo o banco de dados de condomínios edilícios, já que eles realizam a coleta, armazenamento e exclusão de dados de moradores (ABELHA, GOMIDE, 2019).

O especialista em direito digital Vinicius Alves, explica que a lei apresenta a conceituação de vários termos. O primeiro a ser debatido é conceito legal de “dados”, que sofrerão o tratamento, como sendo àqueles que coletados por pessoas físicas ou jurídicas e entes públicos que a lei resguarda a proteção, exemplos desse tipo de dado são: nome, endereço, conduta de consumo, preferencias, etc (GLOBAL, 2019).

Dentro da legislação é possível encontrar também uma outra classificação de dados, os chamados de “dados pessoais sensíveis”, como àqueles que são objeto de uma maior tutela protetiva por parte do Estado, já que esse tipo dado contém informações sobre convicções religiosas, filosófica, política, opção sexual, dados genéticos, filiação a sindicatos, etnia, origem, informações sobre a saúde, etc (BRASIL, 2018c).

Uma situação que se pode destacar é que a prestação de informações não envolve apenas o fornecimento digital de informações, mas alcança outras situações como o preenchimento de algum formulário para empresa ou prestar informações ou digitais em leitura biométrica (dado sensível) para entrar em condomínios/empresas, por exemplo. Essa prática, em si, já configura a coleta e armazenamento de dados e, portanto, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) se aplica à pessoa física ou jurídica que faz essa coleta.

Uma das exigências da LGPD é em relação à prestação de informações pelo consumidor, atribuindo à pessoa que está demandando as informações que deixe expresso e de forma clara qual a finalidade da coleta dos dados, que na forma do art. 9º da Lei nº 13.709/2018, também deverão prestar as informações sobre: forma e duração do tratamento, com resguardo de segredos bancários e industriais;

identificação do controlador; informações de contato do controlador; informações acerca do uso compartilhado de dados pelo controlador e sua finalidade; a responsabilidade dos agentes que realizarão o tratamento para explicitar os direitos do titular dos dados, todos dispostos no art. 18 da LGPD (BRASIL, 2018c).

Sobre o último tópico, dos direitos do titular das informações, a Lei nº 13.709/2018 lista o rol com nove prerrogativas do titular, que vão desde acessar os dados que o controlador tem em seu poder, até a revogação da autorização do controlador possuir seus dados armazenados ou utilizados (BRASIL, 2018c). O descumprimento dessas medidas possui penalidade por descumprimento, consistente em uma multa de 2% do faturamento da empresa, limitado ao montante de R$ 50.000.000,00 (cinquenta milhões de reais), por infração, na forma do art. 52, inciso II da Lei nº 13.709/2018.

Essa legislação (LGPD), conforme o art. 4º, inciso III, exclui de sua abrangência as informações coletadas para fins econômicos, jornalísticos, artísticos e acadêmicos, e ainda, não entram nessa abrangência legislativa, os dados coletados em investigações sobre segurança pública ou defesa do Estado (segurança nacional) ou atividade investigativa para a repressão de infrações penais, ou seja, a abrangência da lei está voltada para fins particulares. Portanto, o indivíduo não pode ter acesso à quais dados/informações o poder público estiver atuando para a segurança coletiva e estatal, para que não haja a obstrução de justiça (BRASIL, 2018c).

A Lei nº 13.709/2018, estabelece quem é controlador e operador no tratamento de dados, o primeiro é o responsável pelas decisões acerca do tratamento dos dados, enquanto o segundo é aquele que realiza o tratamento de dados pessoais em nome do controlador. Ambos, controlador e operador, podem ser pessoas físicas ou jurídicas (público ou privado). Sobre o tratamento, o inciso X, do art. 5º da LGPD, destaca vinte termos para se referir à obtenção de dados (BRASIL, 2018c).

Já no final de 2018, o governo federal editou uma Medida Provisória, nº 869/2018, que trouxe uma correção e adições à Lei Geral de Proteção de Dados e modificou, ainda, a Lei 12.965/2014 (Marco Civil da Internet). A principal inovação da lei, que alvo de crítica quando a lei foi publicada, foi a inexistência de uma agência/órgão central para realizar a fiscalização.

No projeto de lei original da Lei nº 13.709/2018 havia previsto um órgão para fazer a fiscalização, porém a disposição foi vetada pelo presidente, à época, Michel Temer, visto a possibilidade de ser alvo de inconstitucionalidade, por ser de iniciativa do Presidente da República a criação de órgãos que demandem gastos do executivo. A medida provisória, então, criou a Autoridade Nacional de Proteção de Dados (ANPD), que inicialmente foi pensada para ser um órgão independente dos três poderes e com amplos poderes de fiscalização.

A medida provisória foi convertida na Lei nº 13.853/2019 estabelecendo os poderes e a natureza da Autoridade Nacional. Entre as suas atribuições está a de poder aplicar sanções, abrir procedimentos, elaborar e editar normas, sanar omissões, interpretar, implementar registro de relação, editar resoluções e requisitar informações de pessoas jurídicas ou físicas que coletam dados de cidadãos. O órgão foi integrado à administração pública federal, sendo parte da Presidência da República, fato que levou a ser criticada por alguns setores.

Autoridade Nacional de Proteção de Dados possui a seguinte estrutura: Conselho Diretor (órgão máximo da instituição, comporta por cinco membros com mandato de quatro anos, indicados pelo Presidente da República), Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, Corregedoria, ouvidoria, assessoramento jurídico, além de unidades administrativas especializadas. Destaca-se que os membros do Conselho Diretor, com o fim do mandado se sujeitam às regras do art. 6º da Lei nº12.813/2013, conhecido como Lei de Conflitos de Interesses no Poder Público, consistente em não divulgar informações do exercício do cargo e impedimentos específicos de atuação profissional por seis meses (MONTEIRO, 2019).

Ainda nessa legislação é possível identificar a existência de outro agente importante, o encarregado (regulado pelo art. 41 da Lei nº 13.709/2018), que é indicado pelo controlador e também pelo operador para que realize atividades de intermediação entre os agentes do tratamento de dados com o titular dos dados e também com a Autoridade Nacional de Proteção de Dados (ANPD), e suas demais atribuições consistem em fazer treinamento de funcionários da gestora dos dados, com treinamentos e procedimentos para proteção das informações, receber reclamações dos titulares e fazer executar medidas comunicadas pela ANPD.

Sobre a aplicação da legislação brasileira, na forma do art. 3º, segue o caminho da regulação europeia, ou seja, a aplicação territorial da lei foi bastante abrangente. A operação de “tratamento” que a lei se refere independe do meio ou do local (dentro do território nacional ou estrangeiro) que houve a obtenção dos dados respeitando três regras: 1) que a operação de coleta seja realizada no território brasileiro; 2) que o tratamento tenha como objetivo fornecer ou ofertar bens e/ou serviços ou tratamento de dados de indivíduos no Brasil; 3) quando os dados do titular tenham sido coletados no território nacional, no momento da coleta.

Em agosto de 2020 a legislação entrará em vigor, e até lá, as empresas, os entes públicos e as pessoas físicas deverão se adaptar às regras previstas na lei. A criação dessa legislação foi demanda em razão de que os dados de clientes/consumidores (em geral, pessoas físicas) estavam sendo alvo de comercio por grandes conglomerados digitais e empresas de comunicação em larga escala, o que levantou a necessidade de uma regulação que preze pela segurança da informação e da privacidade (prevista no art. 5º, inciso X da Constituição Federal e no art. 21 do Código Civil).

Ao fim deste capítulo é possível apreender que os meios de comunicação sofreram uma grande mudança, e as interações sociais se tornaram cada vez mais digitais, e para essa interação acontecer há necessidade de compartilhamento de dados pessoais para que o controlador e o operador consigam estabelecer um perfil ao indivíduo, e isso se aplica à muitas situações cotidianas.

A legislação sobre proteção de dados vem no sentido de relembrar que as informações e os dados pessoais fazem parte do arcabouço legal a ser preservado e respeitado, portanto, cabendo o resguardo legal para conferir segurança jurídica à indivíduos, empresas e ao próprio poder público. Dessa forma, a lei preza de que a utilização, para qualquer fim que se destina, seja cientificado e dado a oportunidade ao indivíduo de poder requerer a retirada dessas informações da fonte onde estão armazenadas.

No capítulo seguinte será abordado a questão do sigilo bancário, o direito à privacidade e aprofundamento conceitual da “sociedade em rede” teorizada por Manuel Castells em 1996 e a mesma “sociedade em rede” teorizada por Jan Van Dijk em 1999, para que seja possível entender e compreender melhor os movimentos

sociais e tecnológicos sobre a privacidade frente à evolução dos meios de comunicação e das mídias sociais e como os direitos fundamentais constitucionais se comportam com o tráfego substancial e rápido de informações.

2 A SOCIEDADE EM REDE, O DIREITO DA PRIVACIDADE E O SIGILO BANCÁRIO

Para iniciar o debate deste segundo capítulo, serão destrinchadas as diferenças teóricas dos termos cunhados pelos autores Manuel Castells (Sociedade em Rede, 1996) e Jan Van Dijk (Sociedade em Rede, 1999). As publicações na língua inglesa dão ao leitor como referência a palavra "*network*", para se referir à informação/rede, contudo, os autores dão um significado diferente e agregam informações que se complementam, e ambas foram teorizadas em época do desenvolvimento dos meios de comunicação.

Manuel Castells foi o primeiro utilizar esse termo na obra chamada de "*The Rise of Network Society*" ("Sociedade em Rede", tradução oficial), integrante de uma trilogia chama de "*The Information Age*" (A Era da Informação, tradução oficial), em que define "informação", como uma rede de interação social entre os indivíduos, onde há dependência de fatores de coletivos que moldam a sociedade, como a religião, a organização política e a própria importância cultural (CASTELLS, 2010).

Jan Van Dijk por outro lado, entende que a informação será o fio condutor da estrutura organizacional da sociedade. Dessa forma um dos atributos possíveis das novas mídias seria o de alterar o padrão de informações em redes sociais, já que o poder de armazenamento de dados não estaria mais concentrado, mas sim difuso num fluxo indeterminado, e já que as mídias possuem como natureza o elevado grau de interação, os grupos, as organizações e os indivíduos poderiam pesquisar e trocar essas informações independentemente, sem depender de unidades centralizadas de informações (VAN DIJK, 2012).

Van Dijk faz uma série de análises do impacto do aumento do fluxo informacional nos campos da economia, da psicologia, da política, estruturas sociais e do direito, contudo, esta pesquisa se limitará às questões envolvendo os meios econômico e do direito. Em sua primeira análise o autor ressalta que as novas mídias criariam novas indústrias, ao mesmo tempo que fomentariam os negócios e alterariam a forma que o direito do consumidor lidará na relação entre os consumidores e

fornecedores com a ressignificação da economia da sociedade da informação (VAN DIJK, 2012).

Sobre o impacto ao direito, o autor destaca que a *internet* é o meio em que a prática de infrações legais é facilitada, visto que, ainda que haja jurisdições específicas para punir essas transgressões, há grande facilidade em se transferir o montante de dados para uma outra jurisdição que não preveja punição (procedimento legal em si e o devido julgamento) para as práticas infratoras (especialmente sobre direitos autorais, pela pirataria de informações, a honra subjetiva e informações bancárias e fiscais) (VAN DIJK, 2012).

Ainda sobre o impacto no direito, o autor destaca que a reformulação social influenciada pelo tráfego de informações mudaria o direito à privacidade. O principal fator de mudança seria com a “mineração de dados” (a rápida produção e processamento de dados e informações). A posição final defendida pelo autor está no sentido de que governos e legislações feitas para regular as mídias sociais não têm como ter efetividade em controlar o conteúdo da *internet*, a implementação de legislações sobre a internet dependeriam necessariamente da cooperação de corporações, políticas de governança da internet e controle no desenvolvimento de *softwares* (VAN DIJK, 2012).

Costa Júnior explica que a revolução tecnológica causa um efeito de corroer os limites da intimidade, em que a intimidade propriamente dita (onde não há interferência ou conhecimento externo de outras pessoas) é algo que está em extinção. Destaca ainda, que a as transformações tecnológicas avançam sem qualquer diretriz moral, o que causa uma série de violações progressivas (quanto mais se avança, mais se viola) dos direitos fundamentais sobre privacidade e intimidade, que se consubstanciam em assédio (COSTA JUNIOR, 1995).

Sabe-se que o sigilo/segredo de informações possui um longo arcabouço legal internacional (convenções sobre direitos humanos) e nacional (LGPD e o Marco Civil da Internet, ordinariamente) construindo um sistema de proteção global de informações de indivíduos, contudo, Bobbio chama a atenção para que, ainda que se faça toda regulação, o desafio que se enfrentará é como garantir esses direitos visto que a globalização digital não possui fronteiras físicas e materiais (BOBBIO, 2004).

Passa-se agora à análise do direito da privacidade e como este sistema está construído na legislação brasileira. No ponto, tratar-se-á das discussões doutrinárias com os direitos que nela (privacidade) estão, ou não, agregados, como o direito da intimidade e do sigilo de informações e, ainda, far-se-á um estudo mais aprofundado sobre a legislação e jurisprudência sobre o sigilo fiscal e bancário. Neste último ponto serão abordadas decisões do Supremo Tribunal Federal sobre a constitucionalidade do acesso, transmissão e utilização de dados financeiros de indivíduos.

O direito à privacidade é previsto na Constituição Federal de 1988 no art. 5º, inciso X onde se resguarda a inviolabilidade à vida privada, a honra, e a imagens das pessoas, e seu descumprimento (violação), por quem quer que seja, enseja o direito subjetivo de indenização por dano material ou moral (BRASIL, 1988), a legislação infraconstitucional também prevê esse direito no Capítulo II, Título I, do Código Civil Brasileiro de 2002 (BRASIL, 2002).

Há divisão doutrinária acerca do significado entre os termos privacidade e intimidade, alguns autores, como Barros (2009) tratam os termos como sinônimos entre si e necessários para a convivência humana em sociedade, enquanto que Diniz (2005) diz que ambos os termos não se confundem e possuem ideias diferentes, pois um se volta para um âmbito coletivo (privacidade) e outro ao meio individual (intimidade).

Gilmar Mendes defende que é necessária a diferenciação de ambos os termos para que se consiga perceber o âmbito de sua aplicabilidade, defendendo que a privacidade está inserida na aplicação de relações pessoais, empresariais, comerciais e profissionais, de forma que as informações tratadas nesses meios não sejam objeto de conhecimento público. Por outro lado, as relações de amizades próximas, e as familiares, estão inseridas num meio íntimo (por isso intimidade) (MENDES, 2008).

Tartuce (2014) leciona que os direitos de privacidade, intimidade e segredo/sigilo estão inseridos um no outro como num círculo concêntrico em que a privacidade engloba o conceito de intimidade, e na própria intimidade que se pode encontrar um círculo menor do segredo/sigilo. Esse entendimento de Tartuce segue a mesma linha de raciocínio de Gilmar Mendes.

Esta pesquisa se aterá ao conceito de privacidade, que será estudada a seguir com foco voltado para os estudos desse direito dentro do contexto do elevado grau

de tráfego de informações pelo meio digital. Posteriormente será estudado, dentro desse conceito, o segredo/sigilo como inserto no direito da privacidade e destrinchar-se-á o seu conceito.

Sales, Lima e Miranda apontam que o desenvolvimento tecnológico dos últimos anos contribuiu para que a troca de informações criasse três desvantagens: a) a obtenção de informações pessoais para fins fraudulentos; b) violação do direito à privacidade e; c) o comercio de informações pessoais de indivíduos (SALES, LIMA MIRANDA, 2014). Como resposta a esses riscos, foi sancionado o Marco Civil da Internet (Lei nº 12.965/2014), com regras para que haja o fornecimento de registro de conexa de usuários, para que haja a facilitação em localizar de um transgressor, na forma do art. 4º, inciso VI.

Não obstante esses dados legislativos, chama-se a atenção para o fato de que as legislações criadas foram decorrentes de comissões parlamentares de inquérito (CPI) sobre Espionagem, em 2013, (usada como base para o Marco Civil da Internet) e Crimes Cibernéticos, de 2015, (base para a Lei Geral de Proteção de Dados) ocorridas na Câmara dos Deputados. A CPI de 2013 em relatório final apontou que havia necessidade de uma legislação que criasse regulações amplas sobre o fornecimento de dados dos cidadãos às empresas e organizações internacionais (BRASIL, 2013).

Celso Ribeiro Bastos entende que privacidade é uma faculdade de um indivíduo limitar que estranhos à vida em família, ao círculo de amizades ou de atividades comerciais, tenham acesso às informações acerca de assuntos privados, impedindo dessa forma a sua divulgação (BASTOS, 1999). O magistério de Silva ainda ensina que na privacidade estão inseridos alguns direitos da privacidade, como a vida privada, a honra, imagem e a moral, pois elas fazem parte da própria existência humana e por isso são direitos fundamentais, portanto, invioláveis (SILVA, 2011).

A privacidade não é um direito previsto tão somente na legislação constitucional, pois é comtemplada em duas grandes legislações com procedimento diverso uma da outra, mas que tambémn visam a proteção desse direito. No Código Penal estão dispostas sanções para o descumprimento da inviolabilidade, consubstanciada nos crimes contra a honra que vão do art. 138 ao 140; a inviolabilidade de correspondência, comunicação radioelétrica, telegráfica e telefônica

no art. 151; a divulgação de segredo no art. 153; a violação dever se sigilo profissional no art. 154, Lei Carolina Dickman. Já no Código Civil Brasileiro de 2002, a regulação do art. 21 preceitua que a vida privada é inviolável, cabendo ao juiz, desde que o representado requeira, adotar providencias para impedir a divulgação de qualquer informação.

Para iniciar o debate acerca do conceito de sigilo, parte-se do pressuposto respaldado pela doutrina de que esse direito é um desdobramento do direito à privacidade. A palavra sigilo não é uma novidade contemplada na Constituição de 1988, o termo já era contemplado com tutela estatal desde a Constituição Imperial de 1824, e naquele tempo o sigilo estava descrito como “segredo inviolável de cartas”. Na constituição seguinte (1891) e nas subsequentes (1934 e 1937) o termo “sigilo” foi oficialmente adotado.

Já na Constituição de 1967 a amplitude do sigilo foi estendida para abranger as comunicações telegráficas e telefônicas. Desse modo, a legislação desse direito está voltada para proteção, preservação de uma possível violação por particulares ou por parte do poder público, o cerne está consubstanciado na proteção de um segredo contra o conhecimento público ou à divulgação.

Ávila e Woloszyn ensinam que a Constituição Federal de 1988 traz em seu texto o conteúdo de tratados e convenções internacionais de direitos humanos (que incluem entre eles a privacidade e intimidade e, consequentemente, o sigilo) e materializa no art. 5º, incisos X (inviolabilidade da vida privada, intimidade honra) e XII (inviolabilidade de comunicação), e neste último a única hipótese de violar esse sigilo é por autorização judicial para investigações criminais (AVILA; WOLOSZYN, 2017).

Marmelstein leciona que a vinculação de sigilo à privacidade confere que os dados a que se dão proteção contém informações da vida privada de uma pessoa, e nesse caso haveria a distinção de espécies de sigilo: os que protegem as movimentações financeiras (sigilo bancário), os que protegem as declarações feitas ao importa de renda (sigilo fiscal), os que protegem as comunicações e registros de ligações telefônicas (sigilo telefônico), e qualquer outro dado de caráter pessoal que se deva ter entre um indivíduo e intuição/empresa/poder público. Via de regra, nem mesmo o poder público pode ter acesso à essas informações de caráter pessoal sem

que haja a permissão do próprio individuo para tal, já que ele é o titular da informação e tem o poder de decidir a exibição e uso da informação (MARMELSTEIN, 2003).

No que tange à legislação de sigilo de dados fiscais há uma grande discussão sobre a necessidade de autorização judicial para acessar as informações financeiras de um contribuinte pelo poder público quando houver investigação ou procedimento administrativo ou fiscal em curso. A Lei Complementar nº 105 de 2001, confere ao fisco e ao poder público executivo federal o poder de acessar os dados de contribuintes independentemente de autorização judicial, sob a justificativa de que como ele (poder público) é detentor das informações, há a prerrogativa de acessá-las desde que mantenha o sigilo entre as suas próprias instituições. Segue a íntegra do art. 6º:

> Art. 6º As autoridades e os agentes fiscais tributários da União, dos Estados, do Distrito Federal e dos Municípios somente poderão examinar documentos, livros e registros de instituições financeiras, inclusive os referentes a contas de depósitos e aplicações financeiras, quando houver processo administrativo instaurado ou procedimento fiscal em curso e tais exames sejam considerados indispensáveis pela autoridade; administrativa competente. (BRASIL, 2001)

Ou seja, para a melhor elucidação e prosseguimento da pesquisa, e ancorando-se no entendimento da Ação Direta de Inconstitucionalidade nº 2.859/DF, o poder público tem a prerrogativa de acessar esses dados (na forma da Lei Complementar nº 105/2001, pois o simples acesso aos dados não configura violação de sigilo, e somado à isso, ainda é possível um órgão público transferir esses dados para outro órgão público, e à ambos caberá o dever do sigilo (em fazer com que essas informações não circulem fora de seus âmbitos).

Antes de adentrar na fundamentação da ADI nº 2.859/DF, analisar-se-á decisões pretéritas do Supremo Tribunal Federal que orientavam de forma diversa a possibilidade de o poder público em poder acessar dados financeiros (bancários e fiscais) para fins de procedimentos administrativos e investigações criminais. As decisões analisadas serão: o Mandado de Segurança nº 21.729-4/DF, julgado em 1995; o Recurso Extraordinário nº 389.808/PR, julgado em 2010; o Mandado de Segurança nº 33.340/DF, julgado em 2015; análise mais detalhada da ADI nº 2.859/DF; o Recurso Extraordinário nº 1.055.941/SP, julgado em 2019 e, por fim, um exame da Medida Cautela na ADI nº 6.387/DF, concedida e referendada em 2020.

A primeira decisão é anterior à Lei Complementar nº 105/2001, em que a parte impetrante, Banco do Brasil, que à época fazia todo o controle de ativos e investimentos do tesouro do Governo Federal, pediu ao Supremo para que suspendesse um ofício do Procurador-Geral da República requisitando informações sobre contribuintes (informações bancárias e fiscais) para instrução administrativa e declarasse a inconstitucionalidade do § 2º do art. 8 da Lei Complementar nº 75/1993 (Lei Orgânica do Ministério Público da União).

O ministro Marco Aurélio Mello, em seu voto, defendeu a declaração de inconstitucionalidade incidental do artigo concedendo a ordem mandamental sob o argumento de que somente por ofício concedido por órgão de capacidade judicante (ou seja, a capacidade jurisdicional) que se é possível relativizar a garantia do sigilo que se extrai do comando do art. 5º, incisos X e XII da Constituição Federal (BRASIL, 1995).

Por outro lado, o ministro Francisco Rezek votou pelo indeferimento da ordem mandamental, sob o argumento de que a proteção do sigilo bancário e fiscal possuem proteção infraconstitucional por meio da Lei nº 4.595/64, e somado à isso a ausência do sigilo bancário expresso na Constituição Federal de 1988 não garantia status constitucional para o cabimento da medida diante da Corte (BRASIL, 1995).

O ministro ainda seguiu argumentando que o art. 38 do diploma legal de 1964, acima referido, ostentava, no artigo 38, relativizações do sigilo bancário e fiscal desde que houvesse interesse do poder público (a justiça, o parlamento e outros órgão do poder público (BRASIL, 1995, p. 118). Atualmente o referido artigo encontra-se revogado por disposições da Lei Complementar nº 105/2001, mas as possibilidades de extensão dessa disposição foram aperfeiçoadas, ainda que permitindo ao poder público de se apossar desses dados de sigilo bancário e fiscal sem necessidade de autorização judicial.

Na parte final da argumentação o ministro trabalha no conceito de “dados” insculpido no art. 5º, inciso XII, utilizando a obra de Celso Bastos e Ives Gandra, que defendem que a o sigilo abrange somente as comunicações: correspondência, a comunicação digital e a telefônica. Na seara bancária o que se protege da violação é o cadastro de informações, não os dados (movimentações, transações, transferências

etc). Os dados, então, se refeririam à uma espécie de “alta tecnologia na comunicação interbancária de informações contábeis” (BRASIL, 1995).

Por fim, o ministro denegou segurança (seguido pela maioria) destacando que não observava inconstitucionalidade no dispositivo do § 2º da Lei Complementar 75/1993, visto que a norma ali presente apenas estaria criando uma nova possibilidade de se alcançar os dados bancários (não protegidos pelo sigilo na forma da Constituição Federal de 1988) sem que, concomitantemente, não fira o art. 5º X e XII, da CF e amparado pela lei de 1964, que garante o pleno funcionamento do Ministério Público da União na forma do art. 129, VI da Carta Magna brasileira (BRASIL, 1995).

Já no bojo do julgamento do Recurso Extraordinário nº 389.808/PR, julgado em 2010, ano em que já vigorava a Lei Complementar nº 105/2001, decidiu-se pelo afastamento da aplicação dos termos do diploma complementar sob o argumento de que a Receita Federal necessita de prévia autorização judicial para acessar dados e informações bancárias e fiscais, sob a pena do judiciário banalizar a defesa constitucional do sigilo.

Nessa decisão, diferentemente da decisão anterior, não se permitiu que o Ministério Público, no exercício de suas funções institucionais, pudesse requisitar diretamente informações ou documento fiscal ou bancário diretamente do fisco (Receita) ou de qualquer outra instituição financeira sob pena de violação da intimidade da vida privada, que é uma garantia constitucional. Dessa forma, apenas com o poder judiciário como intermediário e autorizador do acesso, que seria possível acessar esses dados (BRASIL, 2010).

O relator do processo, ministro Marco Aurélio Mello, fez apenas uma observação quanto ao poder de acesso de dados sobre as Comissões Parlamentares de Inquérito, que confere a elas, na forma do art. 53, § 3º da Constituição Federal, o poder investigativo próprio de autoridades judiciárias (BRASIL, 2010, p. 225). Ainda no acórdão o ministro relembrou a decisão “estranha ao texto constitucional” dada pela maioria no julgado anteriormente analisado (MS nº 2.729-4/DF).

O Mandado de Segurança nº 33.340/DF, julgado em 2015, de relatoria do ministro Luiz Fux, decidiu de forma diversa do julgamento anterior. Dessa vez o caso tratava-se do Tribunal de Contas da União, que havia pedido o envio de dados das

operações bancárias e financeiras entre o Banco Nacional do Desenvolvimento Econômico e Social (BNDES) e o Grupo JBS/Friboi.

O relator inicia o voto com um tópico dedicado apenas a definir a missão institucional dada aos Tribunais de Contas, especialmente ao da União (no art. 71 da Constituição de 1988), como um órgão auxiliar independe do Estado Brasileiro com atribuição de ser apoio do Poder legislativo e para realizar o controle financeiro. Os membros possuem a prerrogativas conferidas aos magistrados, contudo, suas decisões possuem natureza administrativa e, portanto, passíveis de controle pelo judiciário (BRASIL, 2015).

Sobre o sigilo, destaca-se a existência de uma seção própria para apresentar o direito ao sigilo bancário, uma outra espécie de sigilo, o empresarial, avocado pela impetrante, e não obstante as explicações dadas ao conceito de sigilo, o ministro o identificou na Carta Magna do Brasil (art. 5º, inciso X e XII da CF), e tratou de listar as exceções constitucionais do sigilo insculpidos nos incisos XXXIII (segurança social e do Estado) e inciso LX (respeito à intimidade ou interesse social), ambos do art. 5º da CF (BRASIL, 2015).

Em respeito à jurisprudência da Corte, o magistrado trata de fazer o *distinguishing* do caso em apreciação, à época, de duas decisões parâmetros, os Mandado de Segurança nº 22.801/DF e o Mandado de Segurança nº 22.934/DF, que estabeleceram que o Tribunal de Contas da União não poderia manejar a Lei Complementar nº 105/2001 para quebrar o sigilo bancário e empresarial. Nesses dois casos, o BACEN e o Banco do Brasil possuem em sua custódia, informações acerca de movimentações financeira e por isso a decisão era acertada, pois as informações possuíam o caráter privado (BRASIL, 2015).

No caso demandado à Suprema Corte o Tribunal de Contas da União estava atuando na fiscalização de entidades federais, o BNDES e o BNDES Participações S.A. (BNDESPAR), com o apoio da Comissão de Fiscalização e Controle da Câmara dos Deputados. Portanto, o caso tratava-se de requerer ao próprio banco de fomento informações sobre a contratação de terceiros com financiamento público. A natureza do banco, apesar de privada, se sujeita aos controles da utilização de erário público (BRASIL, 2015).

Portanto, a decisão da Corte se consubstancia na tese de que, quando se tratar de valores, capitais e verbas públicas empregadas para um terceiro particular (ou ainda público), não há de se falar de sigilo bancário, pois este reside na proteção de movimentações financeiras entre particulares. Sempre que o poder público estiver envolvido na relação econômica, o poder público (seja pelo Tribunal de Contas, ou qualquer outro órgão de controle), há dever de prestar essas informações sem que haja violação de outros princípios constitucionais como a “proporcionalidade, necessidade, adequação e proporcionalidade em sentido estrito” (BRASIL, 2015, p. 22).

Agora sob a ótica da ADI nº 2.859/DF de relatoria do ministro Dias Toffoli, julgada em 24 de fevereiro de 2016, o entendimento adotado permitiu que a Fazenda Nacional acesse diretamente, sem a necessidade de autorização judicial, os dados de contribuintes, sob o argumento de que o direito ao sigilo disposto no artigo 5º, inciso X da Constituição Federal se materializa na não-circulação desses dados nos meios de comunicação pública e não com o simples acesso (BRASIL, 2016).

De acordo com o art. 5º e 6º da Lei Complementar 105/2001 determinam que aos agentes públicos (órgãos administrativos) detentores dos dados acessados continuam a dever o sigilo da informação obtida. Dessa forma, a transferência entre eles ainda mantém essa mesma obrigação (uma obrigação duplamente aplicada). O ministro justifica numa linha argumentativa sobre a legitimidade do Fisco (e seus órgãos, em especial à Receita Federal) em obter esses dados sem autorização judicial, pois ela já possui acesso à um conjunto maior de informações sobre o patrimônio de contribuintes (por meio da Secretaria da Receita Federal) (BRASIL, 2016).

O ministro, então, indaga o porquê de não se deixar acessar um conjunto menores de informações (movimentação financeira) se ela própria (Receita Federal) já possui acesso ao conjunto maior de informações (bens e rendas). Assim o princípio da eficiência (finalístico dos artigos 5º e 6º da LC nº 105/2001) ganha primazia, segundo o magistrado, pois se torna instrumento de combate à sonegação fiscal e essencial para o Estado desempenhar o seu papel fiscalizatório (BRASIL, 2016).

Nos votos seguintes, os ministros Luiz Roberto Barroso e Teori Zavascki, entendem que as informações financeiras não se encontram protegidas por dispositivo

constitucional e por isso prescinde de autorização judicial, Barroso ainda acrescenta que a intimidade é passível de restrição pelo legislador que objetiva compatibilizar o contribuinte com o dever de pagar tributos, respeitar a isonomia tributária e a capacidade contributiva (BRASIL, 2016). Zavaski, por sua vez, defendeu que uma vez que os contribuintes já prestam informações bancárias (e outras ainda mais íntimas) para o Fisco quando se presta declaração do imposto de renda, haveria reserva de intimidade em manter essas informações do contribuinte em segredo (o sigilo em si), portanto, o Fisco não possui prerrogativa de quebrar o sigilo, mas apenas de acessá-los (BRASIL, 2016).

Por fim, o saudoso ministro Zavaski ainda chama a atenção de que em relação às pessoas jurídicas, não se pode falar jamais de sigilo, pois lhe é estranho falar de "intimidade da pessoa jurídica", e atenta à situação de que elas [PJ's] tem obrigações de prestar informações financeiras em prestar contas ao Fisco e ao Comissão de Valores Mobiliário (CVM) ou aos seus acionistas (se for o caso) para dar publicidade de seus atos financeiros e da situação patrimonial (BRASIL, 2016).

O ministro Marco Aurélio manteve seu posicionamento, desde outros julgados, de que há necessidade de intermediação e autorização judicial para que seja possível o acesso do fisco aos dados bancários e financeiros. Ávila e Woloszyn concordam com a corrente vencida da Corte por entendê-la como mais adequada no resguardo dos direitos privacidade e sigilo, consideram que a modificação jurisprudencial se opera pelo caminho interpretativo constitucional questionável, já que há menção expressa de autorização judicial na quebra do sigilo (ÁVILA; WOLOSZYN, 2017).

No ano de 2019, o Supremo Tribunal Federal julgou o Recurso Extraordinário nº 1.055.941/SP, que alterou o entendimento da Corte sobre o acesso e compartilhamento de dados fiscais e bancários entre a Receita Federal e o Ministério Público para fins de investigação ou instrução penal, estabelecendo uma regra geral para o compartilhamento e acesso entre as instituições citadas. Nesse julgamento ficou vencido o Ministro Marco Aurélio, que seguiu seu entendimento conforme os julgamentos passados sobre o mesmo tema.

O julgamento, em resumo, estabeleceu que o sigilo bancário em nada é afetado quando se transmite os dados entre instituições públicas, seja de natureza fiscal ou de persecução penal, já que, assim como defendido em outras ações, o dever de sigilo

entre as instituições se mantém. A regra geral que se debateu, firmou-se no sentido de que a transmissão de dados deve seguir um padrão procedimental rígido, com a utilização de sistema próprio que garanta segurança dos dados.

Conforme o voto do ministro Celso de Melo, esse entendimento facilita o trabalho da ex-Unidade de Inteligência Financeira, o atual Conselho de Controle de Atividades Financeiras (COAF), contudo, ressaltou que, o COAF ou a Receita Federal não podem mandar ao órgão de persecução (seja o Ministério Público ou as polícias judiciárias) os dados protegidos por força constitucional de sigilo bancário, como extratos bancários, livros contábeis, declaração do imposto de renda etc) (BRASIL, 2019), mas sim noticiar (semelhante à uma *notitia criminis*) a probabilidade de um ilícito financeiro (seja pela ordem tributária ou contra a Previdência Social).

O ministro Alexandre de Morais propôs a tese que se firmou pela maioria de como se deve proceder para que as instituições públicas (A Receita Federal do Brasil, o Conselho de Controle de Atividades Financeiras e o Ministério Público) façam e transmitam os dados entre si: que seja feita por meio de comunicação formal, com garantia do sigilo; certificação do destinatário, e estabelecer instrumentos efetivos (internos de cada órgão) para que haja apuração e correção de “eventuais desvios” (BRASIL, 2019).

No ano de 2020, a ministra Rosa Weber concedeu uma Medida Cautelar pedida pelo Conselho Federal da Ordem dos Advogados do Brasil (CFOAB), na Ação Direta de Inconstitucionalidade nº 6.387/DF, para suspender a eficácia da Medida Provisória nº 954/2020, que dispôs sobre o compartilhamento de dados das operadoras de telefonia ao Instituto Brasileiro de Geografia e Estatísticas (IBGE), para a realização do senso oficial, visto que a coleta de dados restou suspensa devido à pandemia mundial de SARS-COV 2 (chamado popularmente de COVID 19).

A medida provisória impugnada tinha uma previsão específica relacionada ao sigilo no artigo 3º, preceituando que o compartilhamento teria caráter sigiloso e, portanto, não poderia ser disponibilizado ou compartilhado com qualquer empresa pública ou privada, com entes da administração pública (direta e indireta) ou com qualquer ente federativo, além disso, haveria a expedição de uma relatório de impacto à proteção de dados pessoais, na forma estabelecida pela Lei nº 13.709/2018 (LGPD) (BRASIL, 2020a).

A análise inicial foi em relação ao argumento levantado pelo requerente de violação dos termos do art. 62, caput, da Constituição Federal de 1988, referente à ausência de relevância e urgência característicos do instrumento normativo impugnado. A ministra Rosa Weber deixa claro que a Medida Provisória não possui explicações acerca da importância do compartilhamento e nem a forma que será utilizada para a elaboração de políticas públicas sanitária de combate à pandemia, a esses argumentos a ministra aponta que o IBGE já havia se pronunciado sobre o adiamento do senso nacional para o ano de 2021 (BRASIL, 2020b).

Sobre o argumento relativo à não haver uma finalidade no uso da pesquisa com a coleta de dados, a relatora explicou que essa ausência viola os termos do que foi decidido no RE nº 1055941, sobre o compartilhamento de dados entre o COAF e o Ministério Público, já elucidado em parágrafos anteriores. O requerente apresentou à ministra de que o IBGE, intimado da decisão do Supremo, decidiu emitir a Instrução normativa nº 2/2020, regulamentando a transmissão de dados, a qual o requerente considerou ser “precário” em regulamentação.

A Advocacia Geral da União (AGU) ao responder a ação, declarou que a medida provisória em comento estava de acordo com os requisitos legais de relevância e urgência, com a Lei nº 13.709/2018, que pela redação do instrumento o IBGE manteria a confidencialidade e sigilo, nos mesmos moldes já decididos pela Corte, com a posterior eliminação desses dados coletados pela instituto. Sobre a finalidade da pesquisa, explicou que entre os motivos que motivaram a edição da medida foi para o levantamento da Pesquisa Nacional de Amostra por Domicílio - PNAD e também para referência estatística para a base de cálculo do Fundo de Participação dos Estados (BRASIL, 2020b).

Em sede de decisão, a ministra ressaltou que o instrumento normativo exorbitou os limites constitucionais ao dispor sobre a transmissão de dados dos Serviço Telefônico Fixo Comutado (STFC) e Serviço Móvel Pessoal (SMP) e das operadoras inseridas nos sistemas. A medida provisória não oferecia adequação e nem necessidade (compatibilidade do tratamento descrito na ementa da lei com o alcance da finalidade em combate ao COVID 19). Outro argumento levantado pela relatora é a ausência de previsão de mecanismos técnicos e/ou administrativos para proteção dos dados em caso de vazamento acidental ou utilização indevida (BRASIL, 2020b).

Por fim, a relatora reconheceu que, por meio da análise de respostas dada pela Agência Nacional de Telecomunicações (ANATEL), o IBGE não possui uma estrutura que garanta a segura transmissão de dados e nem a estrutura para manter os dados armazenados em segurança. Apontou que há risco no apontamento de responsabilização, visto que a Lei Geral de Proteção de Dados ainda não está em vigor, o que afeta a imputação e os critérios que definem a responsabilidade de entes que gerem danos, quando em tratamento de dados pessoais (BRASIL, 2020b).

Neste capítulo podemos perceber que a dinâmica dos últimos anos com a *internet* tem alterado substancialmente a forma que os indivíduos lidam com os direitos alheios, especialmente sobre os dados pessoais em rede, e isso levou ao governo a decidir sobre a extensão do alcance protetivo de direitos da privacidade e os seus decorrentes, com foco no sigilo.

Infelizmente podemos perceber na jurisprudência que nos últimos anos, o Supremo Tribunal Federal tem alterado inúmeras vezes ou criando mais possibilidade de interpretação do seu entendimento sobre o alcance do sigilo de dados, uma gama de seletividades e exclusões da necessidade de intermediação do poder judiciário quando do acesso aos dados, o que pode causar instabilidade na aplicação da Lei Geral de Proteção de Dados (com a colheita, armazenamento, utilização e não com a administração desses dados, já que estaria fora do escopo legal).

No capítulo seguinte será analisado os desafios da proteção de dados bancários na sociedade da informação, com foco localizado em disposições para a adaptação de empresas, instituições e o poder público para o armazenamento de dados de indivíduos por meio da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) ao mesmo tempo em que o setor financeiro, por meio do Banco Central do Brasil, precisam se adaptar às exigências da Resolução nº 4.658/2018, que trata da armazenamento, coleta e utilização de dados e informações bancárias.

3 DESAFIOS DA PROTEÇÃO DE DADOS BANCÁRIOS

Neste terceiro e último capítulo trataremos sobre as legislações que obrigam as instituições financeiras a adotar procedimentos internos para o tratamento de trados (pela Lei Geral de Proteção de Dados), política de cibersegurança para instituições financeiras pela Resolução do Conselho Monetário Nacional – CMN nº

4.658/2018, e a política de cibersegurança para instituições financeiras de pagamento (pela Circular BACEN3.909/2018). Essa última parte disporá sobre os dois instrumentos normativos do Banco Central Brasileiro.

A Resolução nº 4.658/2018 editada e publicada pelo Banco Central do Brasil (BACEN), aprovada pelo CMN estabeleceu que todas as instituições que tem funcionamento aprovado pelo BACEN devem adotar um parâmetro de segurança interna para a proteção de dados de seus clientes, e para isso estabeleceu que é necessário a contratação de um serviço de nuvem de processamento e armazenamento de dados (TEÓFILO *et al.*, 2019).

As instituições devem implantar e constituir uma Política de Segurança Cibernética que tenham por princípios basilares a confidencialidade, a disponibilidade de dados e sistemas de informações utilizados e integridade, na forma do art. 2º da Resolução nº 4.658/2018, e, ainda, devem elaborar um "Plano de Ação e Respostas à Incidentes", para quando houver uma invasão de sistema com o objetivo de roubar dados financeiros de clientes (TEÓFILO *et al.*, 2019). Cada parte desse tema será destrinchada a seguir.

Para a implantação da Política de Segurança Cibernética, é necessário que o Conselho de Administração ou a Diretoria da instituição (na ausência do primeiro) aprove o plano, que deve conter (necessariamente) sete pontos para a defesa.

O primeiro é o objetivo de segurança cibernética, que contempla a capacidade institucional para se prevenir, reduzir e prevenir vulnerabilidades dos sistemas internos. O segundo ponto é a adoção de procedimentos e formas de controle para reduzir as vulnerabilidades institucionais à incidentes e para concretização dos demais objetivos de segurança cibernética, que deverão compreender, no mínimo: a criptografia, autenticação, prevenção e detecção de agentes externos (intrusos), prevenção contra o vazamento de informações, proteção contra softwares maliciosos (malware), instituição de dispositivos de rastreabilidade, controles de acesso e segmentação (divisão de acesso) de dados/informações, e adoção de novas tecnologias empregas para a proteção do sistema de informação interna (TEÓFILO *et al.*, 2019).

O terceiro ponto é instituir controles específicos para rastreabilidade das informações, para garantir a segurança de "dados sensíveis" (que são aqueles dados que foram definidos na Lei Geral de Proteção de Dados, ainda que esse instrumento seja anterior à lei, já que a própria lei e os "dados sensíveis" são de discussão há mais

tempo). O quarto ponto trata da realização do registro, análise da causa, impacto e controle sobre incidentes relevantes para as atividades da empresa (vale ressaltar que esses eventos devem atingir os dados dos clientes, ainda que não sejam de natureza digital) (TEÓFILO *et al.*, 2019).

O quinto ponto trata de estabelecer: diretrizes para a elaboração de cenários incidentes, nos testes de continuidade de negócios; de definir os procedimentos e os controles de prevenção aos incidentes no tratamento de dados sensíveis ou aqueles considerados importantes na atividade operacional da instituição, contemplando níveis de complexidade, abrangência e precisão compatível com a instituição; classificação sobre a relevância de dados e informações; e definição de parâmetros a serem utilizados na análise da relevância do incidente (BRASIL, 2018b).

O sexto ponto refere-se à implementação da "cultura de segurança cibernética" na instituição, que devem incluir a capacidade e avaliação periódica de pessoal, prestação de informações a clientes e usuário sobre a forma de utilizar os produtos (financeiros) contratados e demonstrar o comprometimento institucional com a melhoria de procedimentos de segurança cibernética. O último ponto, refere-se a iniciativas de compartilhamento de informações com outras instituições financeiras autorizadas pelo BACEN sobre os incidentes [relevantes] sofridos (TEÓFILO *et al.*, 2019).

A resolução do Banco Central também definiu parâmetros para a Política de Segurança Cibernética: o primeiro trata da compatibilização dessa política com o porte, perfil, risco e tipo de modelo de negócios que são desenvolvidos pela instituição. Destaca-se que este primeiro ponto é de suma importância, pois contempla a lógica de o instrumento normativo ligou-se à lógica de que quanto maior a instituição for, maior será a quantidade de dados (empresariais e de clientes) que ela possuirá.

O segundo parâmetro relaciona-se com a natureza das operações e complexibilidade de negócios da instituição, essa disposição existe para, também, garantir que as operações financeiras se tornem mais seguras, visto que por elas é possível se extrair grande quantidade de informações que podem prejudicar a instituição, clientes e terceiros com a subtração ou uso dos dados coletados. O terceiro parâmetro trata da sensibilidade de dados/informações em posse da instituição (o que acarreta a responsabilidade desta) (BRASIL, 2018b).

Teófilo afirma que as instituições podem adotar uma Política de Segurança Cibernética única, por meio de conglomerados prudenciais (união contábil e

econômicas de instituições sobre o mercado financeiro) e sistemas de cooperação de crédito. Dessa forma haveria padronização já que todas as instituições que integram o conglomerado prudencial por si já criariam um sistema cooperativo de crédito amplo, e devido a força normativa da Resolução nº 4.195/2013, a apresentação da documentação e revisão das contas do conglomerado devem acontecer no mínimo uma vez por ano, e assim poderia se controlar também as estatísticas cibernéticas de todas as instituições.

Teófilo afirma que é necessário também fazer a divulgação (de forma clara, acessível, detalhada e direta) da Política de Segurança Cibernética para as empresas que prestam serviços para as instituições financeiras e para os serviços de terceiros. Essa divulgação também deve alcançar, sobretudo, o público, o autor chama atenção para uma regra de que se deve apresentar um resumo com os principais pontos sobre essa política (art. 10 da Resolução nº 4.658/2018).

Outro ponto da resolução trata de instituir um Plano de Ação e de Respostas a Incidentes, que regulara quais medidas devem ser adotadas quando houver a ocorrência de incidentes, como o vazamento de informações ou o armazenamento incorreto de dados, como também outros usos indevidos de dados e informações. Assim como a Política de Segurança Cibernética, esse plano também deve ser aprovado pelo Conselho de Administração ou pela diretoria da instituição (na ausência da primeira).

O plano deve abranger: a) quais ações serão desenvolvidas pela instituição para adequar sua estrutura organizacional e operacional à regras, princípios e diretrizes da Política de Segurança Cibernética; b) controles, procedimentos , rotinas e tecnologias empregadas para prevenção e resposta à incidentes, conforme a Política de Segurança Cibernética; c) atribuição de uma área/setor responsável pelo registro dos efeitos (danos) causados pelos incidentes relevantes. Somados a isso, todas as instituições devem apresentar um diretor com dúplice responsabilidade, pela Política de Segurança Cibernética e pelo Plano de Ações e de Respostas à incidentes.

O art. 8º da Resolução CMN nº 4.658/2018, dispõe que as instituições financeiras (excluídas as instituições de pagamento), deverão apresentar um relatório anual sobre a implementação do Plano de Ação e de Respostas a Incidentes, definindo como data-base o dia 31 de dezembro, contendo (no mínimo) informações sobre efetividade da implementação do plano; resumo sobre resultados da implementação dos controles, rotinas, procedimentos e tecnologias usadas (ou a

serem usadas) para prevenção e resolução de incidentes; a listagem dos incidentes (do meio cibernético) relevantes ocorridos no período; os resultados dos testes de continuidade de negócios, considerado o tempo de indisponibilidade de sistemas por razão do incidente (art. 8º, §1º).

O parágrafo segundo do art. 8º do mesmo instrumento, ainda estabelece que o relatório anual deverá ser submetido ao Comitê de Riscos da instituição, e no caso da sua inexistência para o Conselho de Administração ou para a Diretoria institucional (na ausência do conselho) até o dia 31 de março do seguinte à data-base. Assim como a Política de segurança cibernética, o plano deve ser revisado uma vez por ano (BRASIL, 2018b).

A resolução dispõe uma série de requisitos a serem observados pelas instituições para a contração de serviços de armazenagem em nuvem, que devem preservar a confidencialidade, integridade, disponibilidade (opção para a retirada de informações sensíveis), segurança e sigilo (de operações), além do cumprimento da legislação (não apenas a LGPD, mas também o Marco Civil da Internet, o Código Civil, Penal e demais legislações que possuem disposições sobre o uso de dados). Essa contratação deve ser realizada junto ao Banco Central no prazo de 60 dias antes da efetivação do serviço (assim como as alterações contratuais, que devem ser encaminhados no mesmo prazo da contratação) na forma do art. 15 e 16 (BRASIL, 2018a).

O art. 21 da resolução ainda dispõe que as instituições ao fazerem a contratação de serviços de armazenagem de dados e de computação (respeitado os requisitos disposto no instrumento), deverão atender três obrigações para que se efetivem a política cibernética, o plano de respostas e o armazenamento em nuvem, quais sejam, a) definir processos, trilhas e teste de auditória; b) definir métricas e indicadores adequados e; c) identificar e corrigir eventuais deficiências (de segurança).

Por fim, as disposições finais do instrumento destacam que alguns documentos deverão estar disponíveis para o Banco Central no prazo de cinco anos, são alguns deles: documentação da Política de Segurança Cibernética, a ata de reunião do conselho de administração (ou da diretoria, se for o caso), documentação do Plano de Ação e Respostas a Incidentes, documentos de contratação de serviços relevantes de processamentos de dados em nuvem, etc (BRASIL, 2018a).

O Banco Central ainda poderá, conforme a necessidade (discricionária, portanto), estabelecer outros requisitos e/ou procedimentos para o compartilhamento de informações; estabelecer a exigência de certificação (certificado digital) ou outros requisitos técnicos a serem exigidos das empresas contratadas pelas instituições; estabelecer, aumentar ou diminuir prazos máximos para reinicio ou normalização da atividade empresarial ou serviços relevantes interrompidos; adotar outros requisitos técnicos e/ou operacionais para o cumprimento da resolução. O Banco Central, ainda, pode vetar ou restringir, a qualquer tempo, a contratação de serviços de processamento e armazenamento de dados e definir prazo de adequação para todos os serviços mencionados (BRASIL, 2018a).

Em agosto de 2018 o Banco Central publicou a Circular nº 3.909, prevendo regras específicas para a contratação de serviços de processamento e armazenamento de dados em nuvem para as instituições de pagamento com funcionamento permitido pelo BACEN. As disposições sobre a Política de Segurança Cibernética, Plano de Ação e de Respostas à Incidentes e o regime de contratação de contrato de serviços de processamento e armazenamento de dados em nuvem foram replicados da Resolução CMN nº 4.658/2018.

As instituições de pagamento são definidas pelo Banco Central como pessoas jurídicas que viabilizam serviços de compra e venda de movimentação de recursos no âmbito de pagamento, sem a possibilidade de conceder empréstimos e financiamento a seus clientes (BRASIL, 2020).

A primeira diferença da Política de Segurança Cibernética para essas instituições consiste no fato de que não há restrições para o compartilhamento de informações sobre incidentes relevantes, pois as instituições financeiras só podem compartilhar essas informações com outras instituições financeiras, e as de pagamento podem transmitir entre elas, para as financeiras e outras instituições autorizadas pelo Banco Central.

A segunda maior diferença se refere ao prazo de comunicação das informações a serem prestadas para o Banco do Brasil, quando da contratação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem, podendo ocorrer no prazo inferiores à 60 dias (a depender a situação excepcional, desde que devidamente fundamentada e demonstrada), para garantir o funcionamento regular da instituição, na forma do art. 15,§ 4º da Circular nº 3.909/2018.

A terceira diferença encontra-se nos prazos para o envio do cronograma de adequação ás normas regulatórias, já que dispõe o prazo de 90 (noventa) dias, contado a partir da entrada em vigor da Circular, para que haja a aprovação da Política de Segurança Cibernética e do Plano de Ação e Respostas a Incidentes, enquanto que as instituições financeiras autorizadas pelo Banco Central possuíam até o dia 06 de maio de 2019, na forma do art. 25 da Circular.

A última diferença analisada concentra-se nas competências atribuídas ao Banco Central. A resolução previu que o BACEN poderia vetar ou impor restrições para contratação de serviços de processamento ou armazenagem em nuvem, quando considerasse inobservância ou descumprimento da resolução CMN nº4.658/2018) e determinar prazos para adequação dos serviços. Já na circular a competência do BACEN é expandida prevendo mais uma possibilidade, que é a definição do prazo de adequação para os contratos correspondentes, na forma do art. 26 da Circular.

A Lei Geral de Proteção de Dados já foi devidamente destrinchada nos capítulos anteriores, onde se destacou as disposições sobre a classificação de dados, princípios, e sua aplicabilidade, que inclusive há uma exceção, que é a aplicação ao mercado financeiro. Faz-se aqui um adendo à essa disposição, a legislação não aplica ao mercado financeiro apenas no que diz respeito à algumas disposições sobre alguns direitos que, se exercidos no mercado financeiro, não seria viável a atividade financeira (por exemplo, a retirada de dados cadastrais de clientes ativos e inativos da instituição).

As instituições financeiras, de pagamento e demais autorizadas a funcionar pelo Banco Central, devem seguir a LGPD quando se tratar da coleta e tratamento de dados, tanto que a Resolução nº 4.658/2018 e Circular nº 3.909/2018 também utilizam do termo “dados sensíveis”, que é utilizado, conceituado e tutelado pela Lei Geral de Proteção de Dados.

Pode-se observar que as duas legislações criam várias obrigações para o tratamento e coleta de dados, além de definir regras e princípios a serem seguidos. Para o setor empresarial, pode-se perceber que as figuras do controlador, operador e encarregado (pela LGPD) seriam compatíveis com o cargo do diretor de segurança cibernética para lidar com a Autoridade Nacional de Proteção de Dados e com o Banco central num eventual ataque, invasão e coleta de dados de cliente de operadoras financeiras.

Contudo, apenas quando houver o vigor oficial da Lei Geral de Proteção de Dados, que se pode afirmar se as estruturas são compatíveis entre si, podendo haver a conjugação dessas estruturas em um setor para a gestão e proteção de dados, ou ambas deverão funcionar separadas visto que respondem à órgãos diferentes. Mas pode-se perceber que a tendência é que quanto mais evoluem as comunicações digitais, mais a estrutura deverá ser aperfeiçoada.

Na hipótese de ambas as estruturas serem incompatíveis entre si, e também por falta de previsão em qualquer dos instrumentos, o dispêndio de gastos setoriais se tornam elevados, visto que haverá dois setores que estarão voltados para a proteção de dados, somado à isso tem o prazo dado pela legislação e pelas normas do Banco Central, que colocam uma série de novos requisitos que demandam pesquisa de mercado e adequação institucional em prazo de 1 ano (2019, para a Resolução CMN nº 4.658/2018; e 2020, para a Lei Geral de Proteção de Dados).

Não se busca, nessa pesquisa, dizer que a proteção de dados não é necessária, pois ela é, visto que a internet é um campo muito vasto para a propagação de dados, notícias e informações de todos os tipos, e por ser um meio de difusão informativa, nesse meio estão envolvidos indivíduos que buscam aplicar golpes para prática de crimes, especialmente os contra a ordem tributária e financeira.

Nesse capítulo estudamos que a Resolução nº CMN 4.658/2018 e a Circular BACEN nº 3.909/2018 são regras que disciplinam a serviço para a proteção de dados, e esses dados possuem conceituação, proteção e procedimentos previstos na Lei Geral de Proteção de Dados. Todos os instrumentos visam proteger os dados e as informações, e a partir desses dados fazer um arcabouço maior que dá mais condições de garantia ao sigilo de informações bancárias, fiscais e sensíveis, seja pelo poder público, seja pelas instituições privadas.

CONSIDERAÇÕES FINAIS

Ao final desta pesquisa, pode-se observar que cada capítulo tratou e interligou os temas do desenvolvimento dos meios de comunicação, especialmente as mídias sociais, que Manuel Castells e Jan Van Dick teorizaram, ainda na época dos primeiros softwares de processamento em massa, que esse fenômeno causaria uma grande discussão acerca dos limites da privacidade, levando-se em conta que a digitalização poderia encurtar a cadeia de transmissão da informação pela velocidade.

De fato, isso ocorreu, e com esse fenômeno de transmissão de dados, inseriram-se sujeitos e/ou organizações que se dedicam a obter informações pessoais, bancárias e fiscais para dar uma utilização indevida. O direito à privacidade das informações da vida privada foi e está sendo severamente atacado, o que demandou dos Estados o desenvolvimento de uma legislação para regular o uso da rede mundial de computadores (*internet*). Tal como a União Europeia com a *General Data Protection Regulation* (GDPR), o Brasil editou e publicou a Lei nº 12.965/2014, chamada de Marco Civil da Internet (para regular o uso da rede de computadores) e a Lei nº 13.709/2018, chamada de Lei Geral de Proteção de Dados (disciplinando o tratamento de dados pessoais), com vigência programada para iniciar em agosto de 2020.

Essas duas legislações brasileiras possuem diversos princípios que envolvem direitos fundamentais, entre eles o da privacidade, intimidade, sigilo de informações e dignidade da pessoa humana. A Lei Geral de Proteção de Dados disciplina a coleta de dados em um âmbito muito maior que o meio digital, regulando qualquer coleta de dados que seja feita por pessoa física ou jurídica, por meio digital ou por meio físico, garantindo o direito de terem suas informações excluídas de bancos de dados, e com a garantia de que esses dados não serão usados para meios comerciais ou qualquer venda para usos diversos realizados pela coleta.

A partir do estudo sobre a teorização da sociedade em rede abordado no segundo capítulo, pôde-se concluir que os autores Manuel Castells e Jan Van Dick divergiam sobre o papel que a informação possui na sociedade. Enquanto Manuel Castells teoriza que a informação é elemento que sofre modificação em sua interpretação a depender do meio social que é inserido, Jan Van Dick, entende que a informação é elemento formador da sociedade, e não um elemento que é inserido. Ambos os autores são concordantes na afirmação de que a informação possui um valor não mensurável, mas que confere poder àquele que o possui.

Em seguida, tem-se percebido que o Supremo Tribunal Federal tem formado entendimentos divergentes sobre a possibilidade de compartilhamento de dados bancários e outras informações ficais para entes federativos para fins de persecução penal e investigação de possíveis fraudes. Desde o primeiro julgamento da Corte Constitucional tem-se observado que a prática das decisões é a de definir se o órgão

público que solicita a informação e o órgão que mantem a informação podem compartilha-las entre si, desde que resguardados o sigilo.

É notório que as decisões sobre o sigilo tem trazido consequências negativas, visto que o Supremo Tribunal Federal tem dado a possibilidade de definir qual órgão pode e qual não pode compartilhar informações, o que pode acarretar uma série de decisões judiciais definindo o nível de atuação, e chamando à competência do STF para definir onde os demais órgãos podem ou não atuar e entender o valor (infra)constitucional do sigilo. Conclui-se, portanto, não ser juridicamente aceitável e nem cabível por meio judicial esse tipo de movimento, sob pena de sobrecarga judicial, insegurança jurídica e desvirtuação da missão constitucional da Suprema Corte.

No terceiro capítulo, onde foram abordadas as regulamentações gerais do Banco Central do Brasil e do Conselho Monetário Nacional (CMN), nesse aspecto, tem-se observado novas regras a serem adotadas pelas instituições bancárias para oferecer maior proteção e respostas as tentativas de ataques para obtenção de dados de clientes do sistema financeiro nacional. As exigências das portarias, portanto, tem sido o de desenvolvimento de ferramentas de controle de acesso, de controle de armazenamento, de políticas internas para respostas a crises, e de políticas de comunicação entre instituições bancárias e o Banco Central.

Além disso, foi possível concluir que as regulações, somadas à Lei Geral de Proteção de Dados, criam uma infraestrutura robusta para a proteção de dados, mas o decurso de tempo dado para as adaptações geram um custo operacional enorme (as portarias definiram o período de 1 (um) ano e a LGPD, 2 anos), isso porque as exigências feitas nos instrumentos normativos demandam uma série de pesquisas de mercado, negociações com investidores, criação e sistematização, e organização de estruturas internas que precisam de aprovação de diretorias ou assembleia de investidores, juntamente com as organizações fiscais e de custeio dessas estruturas. Observa-se, portanto, que o prazo certamente é um empecilho, que gera dificuldades para a adaptação das empresas.

Uma solução viável para essa situação seria a de um prazo maior para adaptação das instituições do sistema financeiro, ou a criação de uma transição gradual (definindo um calendário de implantação por setor), com prazo estendido para as instituições, visto que a pandemia do SARS-COV 2 (chamado popularmente de

COVID 19) praticamente paralisou a economia mundial, sendo imprescindível a prorrogação do prazo de adaptação por parte do governo brasileiro.

Por fim, a pesquisa dedicou-se a mostrar o panorama do desenvolvimento informacional sob a ótica do direito, e pôde-se concluir que a rede mundial de computadores (*internet*), por ser um sistema sem fronteiras, torna-se muito difícil de controlar, visto que nem todos os países possuem regulações sobre a *internet*, o que pode torná-los redutos de organizações criminosas virtuais, incentivando crimes digitais em massa. A partir dos estudos extrai-se que ainda estamos longe de um consenso quanto ao tratamento judicial sobre o fenômeno da difusão das *fake news* (notícias falsas), e sobre a forma que os entes públicos devem entender “dados”, “sigilo”, “privacidade” e “intimidade”, mas que pelo menos os órgãos competentes tem se esforçado na regulação do fenômeno de modo a proteger os direitos e garantias das pessoas físicas e jurídicas.

REFERÊNCIAS

ÁVILA, Ana Paula Oliveira; WOLOSZYN, André Luís. A tutela jurídica da privacidade e do sigilo na era digital: doutrina, legislação e jurisprudência. **Revista de Investigações Constitucionais**, Curitiba, v. 4, n. 3. p. 167-200, set./dez. 2017. DOI: 10.5380/rinc.v4i3.51295. Disponível em: https://www.scielo.br/scielo.php?script=sci_abstract&pid=S2359-56392017000300167&lng=en&nrm=iso&tlng=pt . Acesso em 05 jun 2020.

BOBBIO, Norberto. **A era dos direitos**. Rio de Janeiro: Elsevier, 2004.

BRASIL. Banco Central do Brasil. ***O que é instituição de pagamento?*** *Disponível em:* https://www.bcb.gov.br/estabilidadefinanceira/instituicaopagamento. Acesso em: 19 jan. 2020.

BRASILa. Banco Central (BACEN). **Circular nº 3.909, de 16 de agosto de 2018**. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições de pagamento autorizadas a funcionar pelo Banco Central do Brasil. Disponível em: https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachme. Acesso em: 19 jan. 2020.

BRASILb. Banco Central do Brasil (BACEN). **Resolução nº 4.658, de 26 de abril de 2018**. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. Disponível em:

https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50581/Res_4658_v1_O.pdf. Acesso em 19 jan. 2020.

BRASIL. Câmara dos Deputados. **Relatório final da CPI dos crimes cibernéticos**. 2016. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/comiss oes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos. Acesso em: 23 nov. 2019.

BRASILc. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 16 nov. 2019.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 16 nov. 2019.

BRASILa. **Medida Provisória nº 954, de 17 de abril de 2020**. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm. Acesso em: 13 maio 2020.

BRASIL. Senado Federal. **Relatório Final da CPI da Espionagem**. 2013. Disponível em: https://www12.senado.leg.br/noticias/arquivos/2014/04/04/integra-do-relatorio-de-fer raco. Acesso em: 26 jul. 2016.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 2859/DF**. Ementa: Ação direta de inconstitucionalidade. Julgamento conjunto das ADI nº 2.390, 2.386, 2.397 e 2.859. Normas federais relativas ao sigilo das operações de instituições financeiras. Decreto nº 4.545/2002. Exaurimento da eficácia. Perda parcial do objeto da ação direta nº 2.859. Expressão “do inquérito ou”, constante no § 4º do art. 1º, da Lei Complementar nº 105/2001. Acesso ao sigilo bancário nos autos do inquérito policial. Possibilidade. Precedentes. Art. 5º e 6º da Lei Complementar nº 105/2001 e seus decretos regulamentadores. Ausência de quebra de sigilo e de ofensa a direito fundamental. Confluência entre os deveres do contribuinte (o dever fundamental de pagar tributos) e os deveres do Fisco (o dever de bem tributar e fiscalizar). Compromissos internacionais assumidos pelo Brasil em matéria de compartilhamento de informações bancárias. Art. 1º da Lei Complementar nº 104/2001. Ausência de quebra de sigilo. Art. 3º, § 3º, da LC 105/2001. Informações necessárias à defesa judicial da atuação do Fisco. Constitucionalidade dos preceitos impugnados. ADI nº 2.859. Ação que se conhece em parte e, na parte conhecida, é julgada improcedente. ADI nº 2.390, 2.386, 2.397. Ações conhecidas e julgadas improcedentes. Relator: Min. Dias Toffoli. Tribunal

Pleno. Julgada em 24/02/2016. Publicada em 21 de outubro de 2016. Disponível: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=11899965. Acesso em: 05 jun 2020.

BRASIL. Supremo Tribunal Federal. **Mandado de Segurança nº 21.729-4/DF**. Ementa: - Mandado de Segurança. Sigilo bancário. Instituição financeira executora de política creditícia e financeira do Governo Federal. Legitimidade do Ministério Público para requisitar informações e documentos destinados a instruir procedimentos administrativos de sua competência. 2. Solicitação de informações, pelo Ministério Público Federal ao Banco do Brasil S/A, sobre concessão de empréstimos, subsidiados pelo Tesouro Nacional, com base em plano de governo, a empresas do setor sucroalcooleiro. 3. Alegação do Banco impetrante de não poder informar os beneficiários dos aludidos empréstimos, por estarem protegidos pelo sigilo bancário, previsto no art. 38 da Lei nº 4.595/1964, e, ainda, ao entendimento de que dirigente do Banco do Brasil S/A não é autoridade, para efeito do art. 8º, da LC nº 75/1993. 4. O poder de investigação do Estado é dirigido a coibir atividades afrontosas à ordem jurídica e a garantia do sigilo bancário não se estende às atividades ilícitas. A ordem jurídica confere explicitamente poderes amplos de investigação ao Ministério Público - art. 129, incisos VI, VIII, da Constituição Federal, e art. 8º, incisos II e IV, e § 2º, da Lei Complementar nº 75/1993. 5. Não cabe ao Banco do Brasil negar, ao Ministério Público, informações sobre nomes de beneficiários de empréstimos concedidos pela instituição, com recursos subsidiados pelo erário federal, sob invocação do sigilo bancário, em se tratando de requisição de informações e documentos para instruir procedimento administrativo instaurado em defesa do patrimônio público. Princípio da publicidade, ut art. 37 da Constituição. 6. No caso concreto, os empréstimos concedidos eram verdadeiros financiamentos públicos, porquanto o Banco do Brasil os realizou na condição de executor da política creditícia e financeira do Governo Federal, que deliberou sobre sua concessão e ainda se comprometeu a proceder à equalização da taxa de juros, sob a forma de subvenção econômica ao setor produtivo, de acordo com a Lei nº 8.427/1992. 7. Mandado de segurança indeferido. Relator: Min. Marco Aurélio. Pleno. Julgado em 05/10/1995. Publicado em 19 de outubro de 2001. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=11899965. Acesso em: 05 jun. 2020.

BRASIL. Supremo Tribunal Federal. **Mandado de Segurança nº 33.340/DF**. Ementa: Direito administrativo. Controle legislativo financeiro. Controle externo. Requisição pelo tribunal de contas da união de informações alusivas a operações financeiras realizadas pelas impetrantes. Recusa injustificada. Dados não acobertados pelo sigilo bancário e empresarial. Relator: Min. Luiz Fux. Primeira Turma. Julgado em 26/05/2015. Publicado em 03 de agosto de 2015. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=8978494. Acesso em: 05 jun. 2020.

BRASIL b. Supremo Tribunal Federal. **Medida Cautelar na Ação direta de Inconstitucionalidade nº 6.387/DF**. Requerente: Conselho Federal da Ordem dos Advogados do Brasil – CFOAB. Intimado: Presidente da República. Relator: Ministra Rosa Weber. Julgado em: 24/04/2020. Liminar referendada em: 07/05/2020. Disponível: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf. Acesso em: 05 jun. 2020.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário 389.808/PR**. Ementa: SIGILO DE DADOS – AFASTAMENTO. Conforme disposto no inciso XII do artigo 5º da Constituição Federal, a regra é a privacidade quanto à correspondência, às comunicações telegráficas, aos dados e às comunicações, ficando a exceção a quebra do sigilo – submetida ao crivo de órgão equidistante – o Judiciário e, mesmo assim, para efeito de investigação criminal ou instrução processual penal. sigilo de dados bancários – receita federal. Conflita com a Carta da República norma legal atribuindo à Receita Federal – parte na relação jurídico-tributária o afastamento do sigilo de dados relativos ao contribuinte. Relator: Min. Marco Aurélio. Pleno. Julgado em: 15 de dezembro de 2010. Publicado em: 10 de maio de 2011. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docI D=622715. Acesso em: 05 jun. 2020.

CASTELLS, Manuel. **The rise of the network society:** information age. Oxford: Blackwell, v. 1. 2. 2010.

COSTA JÚNIOR, Paulo José. **O direito de estar só: tutela penal da intimidade**. 2. ed. São Paulo: Revista dos Tribunais, 1995.

GLOBAL, mf press. Como a nova Lei de Proteção de Dados Pessoais impacta na sua empresa? **Portal Exame**, 2019. Disponível em: https://exame.abril.com.br/negocios/mfpress/como-a-nova-lei-de-protecao-de-dados-pessoais-impacta-na-sua-empresa%EF%BB%BF/. Acesso em: 18 nov. 2019.

MARMELSTEIN, George. **Curso de direitos fundamentais, direitos de personalidade, intimidade, privacidade, honra e imagem**. 5. ed. São Paulo: Atlas, 2003.

MONTEIRO, Yasmin Sousa. **A efetividade dos mecanismos de proteção de dados pessoais na Lei 13.709/2018.** 2019. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Faculdade de Ciências Jurídicas e Sociais, Centro Universitário de Brasília, Brasília, 2019. Disponível em: https://repositorio.uniceub.br/jspui/handle/prefix/13383. Acesso em: 05 jun 2020.

PLUGAR. **Conheça a origem da Lei Geral de Proteção de Dados (LGPD)**. 2019. Disponível em: https://www.plugar.com.br/conheca-a-origem-da-lei-geral-de-protecao-de-dados-lgpd/. Acesso em: 18 nov. 2019.

RONCOLATO, Murilo. O que diz a nova lei de proteção de dados da Europa e o efeito no Brasil. **Nexo Jornal**, 2018. Disponível em: https://www.nexojornal.com.br/expresso/2018/05/25/O-que-diz-a-nova-lei-deprote%C3 %A7% C3%A3o-de-dados-da-Europa.-E-o-efeito-no-Brasil. Acesso em: 16 nov. 2019.

SILVEIRA, Larissa da; CALDONAZZO, Tayana R. M. O direito fundamental à privacidade na era digital. *in*: SIMPÓSIO INTERNACIONAL DE ANÁLISE CRÍTICA DO DIREITO (IV SIACRID), Jacarezinho/PR, p. 83-96, 2014, **Anais [**...]. Disponível em: http://eventos.uenp.edu.br/siacrid/trabalhos-antigos/sistema-constitucional-de-garanti a-de-direitos-iii.pdf#page=84. Acesso em: 23 nov. 2019.

VAN DIJK, Jan. **The network society**. 3. ed. Londres: Sage Publications, 2012.

VIDOR, Daniel Martins. LGPD: origem e implicações. **Mercury LBC**, 2019. Disponível em: http://mercurylbc.com/lgpd-origem-e-implicacoes/. Acesso em: 18 nov. 2019.

WATSON, Chloe. The key moments from Mark Zuckerberg's testimony to Congress. **The Guardian**, 2018. Disponível em: https://www.theguardian.com /technology/2018/apr/11/mark-zuckerbergs-testimony-to-congress-the-key-moments. Acesso em: 16 nov. 2019.