UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS
UNIDADE ACADÊMICA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO DA EMPRESA E DOS NEGÓCIOS
NÍVEL MESTRADO PROFISSIONAL

THIALES BORGES BONFIM

Segurança e Transparência no uso de Dados de Clientes de Bancos Digitais no Brasil

Porto Alegre
2020

THIALES BORGES BONFIM

Segurança e Transparência no uso de Dados de Clientes de Bancos Digitais no Brasil

Dissertação apresentada como requisito parcial para obtenção do título de Mestre em Direito, pelo Programa de Pós-Graduação em Direito da Universidade do Vale do Rio dos Sinos – UNISINOS.

Área de concentração: Direito da Empresa e dos Negócios.

Orientador: Prof. Dr. Silvio Bitencourt da Silva

Porto Alegre

2020

B713s Bonfim, Thiales Borges.
Segurança e transparência no uso de dados de clientes de bancos digitais no Brasil. / Thiales Borges Bonfim – 2020.
276 f. : il. ; 30 cm.

Dissertação (mestrado) – Universidade do Vale do Rio dos Sinos, Programa de Pós-Graduação em Direito, 2020.
"Orientador: Prof. Dr. Silvio Bitencourt da Silva"

1. Compliance. 2. Fintechs. 3. Lei Geral de Proteção de Dados. 4. Segurança da informação. I. Título.
CDU 34:004.056

Dados Internacionais de Catalogação na Publicação (CIP)
(Silvana Dornelles Studzinski – CRB 10/2524)

UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS
UNIDADE ACADÊMICA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO DA EMPRESA E DOS NEGÓCIOS NÍVEL MESTRADO PROFISSIONAL

O Trabalho de Conclusão de Curso intitulado: "**Segurança e Transparência no uso de Dados de Clientes de Bancos Digitais no Brasil",** elaborado pelo mestrando **Thiales Borges Bonfim,** foi julgado adequado e aprovado por todos os membros da Banca Examinadora para a obtenção do título de MESTRE EM DIREITO DA EMPRESA E DOS NEGÓCIOS - Profissional.

Porto Alegre, 31 de março de 2021.

Prof. Dr. **Wilson Engelmann**

Coordenador do Programa de Mestrado Profissional em Direito da Empresa e dos Negócios

Apresentada à Banca integrada pelos seguintes professores:

Presidente: Dr. Silvio Bitencourt da Silva (Participação por webconferência)

Membro: Dr. Éderson Garin Porto (Participação por webconferência)

Membro: Dr. Manoel Gustavo Neubarth Trindade (Participação por webconferência)

Membro: Dra. Clea Beatriz Macagnan (Participação por webconferência)

Dedico este trabalho, especialmente, ao meu pai, Flavio *(in memoriam)*, o qual desde que nasci sempre foi o melhor amigo que poderia ter; minha mãe Iara e esposa, Mônica, que, mesmo de longe, sempre torceram por minha vitória; e, finalmente, à filha, Monnique que é uma benção em minha vida. Não teria me tornado o homem que me tornei, tampouco conquistado o que já conquistei se não fosse com o apoio de todos vocês. Meu sincero agradecimento e eterna gratidão.

AGRADECIMENTOS

Agradeço a Deus, em primeiro lugar, pela benção da vida. À minha família, pela confiança, motivação e compreensão em face das ausências e trocas de momentos de lazer pelos momentos de estudos.

Ao Prof. Dr. Silvio Bitencourt da Silva, orientador deste trabalho, pelo apoio, disponibilidade e paciência em todas as etapas desta jornada.

Aos amigos e colegas, pela força e pela vibração em relação a mais este passo alcançado.

A todos que, com boa intenção, colaboraram para a realização e finalização deste trabalho.

Muito obrigado por tudo!

“Não é sobre chegar ao topo do mundo e saber que venceu. É sobre escalar e sentir que o caminho te fortaleceu”.
(Ana Vilela)

RESUMO

O trabalho “Segurança e Transparência no uso de Dados de Clientes de Bancos Digitais no Brasil” faz uma exposição inicial acerca dos principais aspectos relacionados à Lei Geral de Proteção de Dados (Lei nº 13.709/2018), sob o viés da segurança jurídica, com opções práticas em conformidade (*compliance*) ao tratamento de dados no Brasil. O presente estudo visa a analisar as exigências legais trazidas pela Lei as empresas de serviços financeiros, em especial os bancos digitais, de modo a garantir a segurança da informação de dados de seus usuários. A pesquisa contribui na identificação de procedimentos que visam proteger direitos fundamentais de liberdade e de privacidade na coleta e armazenamento de dados. Além disso, o trabalho também demonstra a evolução do mercado financeiro, com os surgimentos de novas empresas baseadas em tecnologia (*Fintechs)* e o crescimento dessas em nível nacional, bem como a importância dos dados, da transformação digital, da revolução 4.0, com suas novas tecnológicas disruptivas. A pesquisa foi elaborada através da combinação de dois métodos de pesquisa, a forma descritiva e a de investigação, caracterizada como uma pesquisa bibliográfica, por coletar dados nos mecanismos de pesquisa *on-line*, livros e periódicos científicos com abordagem sobre o tema. Nesse contexto, são expostos os desafios e perspectivas que irão provocar uma verdadeira revolução tecnológica para o setor de serviços financeiros oferecendo serviços digitais inovadores. Por fim, essa dissertação faz um comparativo entre a LGPD e a Lei do Sigilo Bancário (Lei Complementar nº 105/2001) analisando as questões que se apresentam relevantes entre esses dois dispositivos legais. Além disso, este trabalho tem como objetivo a confecção de um Contrato de termo de Uso e de Política de Privacidade ideal, para *fintechs* de serviços financeiros (bancos digitais). Foi possível tirar algumas conclusões importantes, com o início da utilização do *Open Banking* e a “nova” Lei do Cadastro Positivo, e o surgimento das normas de segurança impostas pelo BACEN referentes à preservação e ao tratamento de dados.

Palavras-chave: LGPD. *Compliance*. *Fintechs*. Segurança da Informação.

ABSTRACT

The work “Security and Transparency in the Use of Customer Data from Digital Banks in Brazil” makes an initial presentation about the main aspects related to the General Data Protection Law (Law nº 13.709 / 2018), under the bias of legal security, with practical options for compliance with data processing in Brazil. The present study aims to analyze the legal requirements brought by the Law to financial services companies, especially digital banks, in order to guarantee the security of the data information of its users. The research contributes to the identification of procedures that aim to protect fundamental rights of freedom and privacy in the collection and storage of data. In addition, the work also demonstrates the evolution of the financial market, with the emergence of new technology-based companies (Fintechs) and their growth at the national level, as well as the importance of data, digital transformation, the 4.0 revolution, with its disruptive new technologies. The research was elaborated through the combination of two research methods, the descriptive and the research, characterized as a bibliographic research, for collecting data in the online search engines, books and scientific journals with approach on the topic. In this context, the challenges and perspectives that will bring about a true technological revolution for the financial services sector are exposed, offering innovative digital services. Finally, this dissertation makes a comparison between the LGPD and the Banking Secrecy Law (Complementary Law nº 105/2001) analyzing the issues that are relevant between these two legal provisions. In addition, this work has the objective of drawing up an ideal Term of Use Agreement and Privacy Policy, for financial services fintechs (digital banks). It was possible to draw some important conclusions, with the beginning of the use of Open Banking and the “new” Positive Registration Law, and the emergence of security rules imposed by BACEN regarding the preservation and treatment of data.

Keywords: LGPD. *Compliance*. *Fintechs*. Information security.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE QUADROS

LISTA DE SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
API	Application Programming Interface
ATM	Automatic Teller Machine
BACEN	Banco Central do Brasil
BB	Banco do Brasil
BC	Banco Central
BNDES	Banco Nacional de Desenvolvimento Econômico e Social
CCB	Cédula de Crédito Bancário
CCO	*Chief Compliance Officer*
CCPA	*California Consumer Privacy Act*
CMN	Conselho Monetário Nacional
CNPC	Conselho Nacional de Previdência Complementar
CNSP	Conselho Nacional de Seguros Privados
CVM	Comissão de Valores Mobiliários
DPO	*Data Protection Officer*
DOC	Documento de Ordem de Crédito
FEBRABAN	Federação Brasileira de Bancos
FIPP	*Fair Information Privacy Principles*
FGC	Fundo Garantidor de Créditos
GDPR	General Data Protection Regulation
IMF	Fundo Monetário Internacional
ISO	Organização Internacional de Normatização
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados
MCTIC	Ministério da Ciência, Tecnologia, Inovações e Comunicações
PIX	Sistema de pagamento instantâneo
SCD	Sociedade de Crédito Direto
SEP	Sociedade de Empréstimo entre Pessoas
SFN	Sistema Financeiro Nacional
TED	Transferência Eletrônica Disponível
TIC	Tecnologias de Comunicação e Informação
UIF	Unidade de Inteligência Financeira

SUMÁRIO

1 INTRODUÇÃO

A dissertação apresentada ao Programa de Pós-Graduação – Stricto Sensu – Mestrado Profissional em Direito da Empresa e dos Negócios da Universidade do Vale dos Sinos, inserida na linha de pesquisa Direito da Empresa e Regulação apresentará a temática do conjunto de questões que colocam em debate a segurança e transparência no uso de dados de clientes de bancos digitais no Brasil. Desse modo, procura-se trazer novas perspectivas para o campo do Direito Empresarial e Digital.

O novo cenário global de novas tecnologias, fruto da revolução digital é uma das mais importantes discussões na atualidade e está diretamente ligada ao uso de um dos ativos mais valiosos da sociedade digital, que são as bases de dados relacionados às pessoas. Sendo assim as empresas de serviço financeiro, não terão outra alternativa senão se adaptarem à essa nova realidade e assim procurar garantir a segurança no tratamento de dados de seus clientes.

O presente trabalho, irá analisar a Lei Geral de Proteção de Dados – LGPD, Lei nº 13.709, de 14 de agosto de 2018, que oficialmente entrou em vigência, no país, em 18 de setembro de 2020. O referido diploma legal foi criado para dar maior proteção ao tratamento de dados pessoais, por qualquer meio, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Assim, sendo, para melhor abordagem do tema escolhido, foi apresentada, de maneira clara e objetiva, a interpretação sistemática da Lei de Proteção de Dados (LGPD), abordando conceitos básicos de toda a temática, desenvolvendo uma base, que auxiliará os discursos sobre a história, evolução, atualidades, construções doutrinárias, julgados e pôr fim demonstrar-se-á os procedimentos a serem adotados pelos bancos digitais na elaboração dos seus contratos de Termo de Uso e Política de Privacidade para estar em conformidade (*compliance*) com a Lei e proteger seus usuários efetivamente, garantindo à segurança da informação de seus dados pessoais.

Assim, esse trabalho irá se focar nas *fintechs* de serviços financeiros (bancos digitais), por se tratar de uma categoria que tem crescido muito nos últimos anos (50%), passando de 12 em 2019 para 17 em 2020.

Nesta esteira, no capítulo inicial do presente estudo é apresentado de forma introdutória, o tema, bem como a sua problemática, os objetivos gerais e específicos e a sua justificativa.

O capítulo subsequente, segundo capítulo, irá discorrer sobre os principais aspectos relacionados a Transformação Digital, Quarta Revolução Industrial, Dados e as Novas Tecnologias Digitais, evidenciando, assim, a importância do uso e comercialização adequada dos dados apoiado em mecanismos de controle interno eficazes (*compliance*), além das profundas transformações tecnológicas e disruptivas que o mundo vem sofrendo e que surgem no sentido de revolucionar os serviços financeiros, oferecendo serviços digitais inovadores modificando, significativamente, a forma como as instituições operam e como os consumidores acessam serviços e produtos diante dessa nova conjuntura, repleta de desafios e de necessidades por conta da pandemia do coronavírus, que certamente não foi um catalisador para adoção e inovação digital no setor, mas que está se mostrando um acelerador de mudanças. Ainda nesse mesmo capítulo, fez-se uma análise dos pontos mais relevantes, a respeito do Mercado Financeiro, *Startups* e *Fintechs*/Bancos Digitais, apresentando conceitos e definições, tendo como base o mapeamento do mercado e os marcos regulatórios do Banco Central do Brasil (BACEN) e a Comissão de Valores Mobiliários (CVM), além das normas suplementares, que recaem em todas as instituições.

No capitulo três deste trabalho, serão demonstradas as metodologias de desenvolvimento que foram utilizadas. A pesquisa foi elaborada através da combinação de dois métodos de pesquisa, a forma descritiva e a de investigação, caracterizada como uma pesquisa bibliográfica, por coletar dados nos mecanismos de pesquisa *on-line*, livros e periódicos científicos com abordagem sobre o tema.

No quarto capítulo, se explana, de forma detalhada, a segurança da informação e sua importância para empresas de serviços financeiros. Com destaque a proteção de dados e a privacidade de clientes através de controles de segurança e rotinas para mitigar riscos operacionais e reunir recursos para melhor defender interesses, caso haja algum incidente ou prejuízo envolvendo as atividades praticadas no meio digital. Envolve-se, assim, uma alteração comportamental, para estabelecer uma cultura de segurança e prevenção, com o treinamento de funcionários, transparência nos processos de coleta de dados e eficiência na abordagem com os consumidores. Ainda, nesse capítulo, fez-se uma análise dos

pontos mais relevantes, a respeito Segurança Digital, Cibersegurança e Privacidade sempre visando proteger identidade digital do usuário, no ambiente virtual, com o uso de ferramentas tecnológicas de proteção contra a atividade de cibercriminosos, especialmente no período de isolamento social por conta da pandemia do novo coronavírus onde se notou um aumento no número de fraudes no sistema bancário *online* e *mobile* brasileiro. Diante disso, foi possível perceber que o Banco Central do Brasil (BACEN) não mede esforços para garantir que o Sistema Financeiro Nacional (SFN) se mantenha sólido e estável e proteja os consumidores, regulamentando a questão da cibersegurança para as instituições financeiras, através da Resolução nº 4.658/2018 e da Resolução nº 4.752/2019. Por fim, se verificou que todo patrimônio está nos dados, por isso a necessidade de haver camadas de proteção de dados com ações que incluem investimentos em políticas, tecnologia, processos e em melhores práticas, além de campanhas de conscientização e educação em segurança e privacidade. Além disso, a Privacidade é um Direito e a Proteção de Dados é o meio de garantir segurança jurídica a esse Direito. Nesse sentido, verifica-se que a privacidade e a proteção de dados são elementos essenciais para Lei Geral de Proteção de Dados criada com o fim de proteger e tutelar direitos e garantir a inviolabilidade da intimidade, da honra e da imagem da pessoa natural e, com isso, o desenvolvimento econômico e tecnológico e a inovação através de princípios, direitos dos titulares de dados, bases legais de tratamento dos dados, bem como sanções e multas propostas. E, ainda, fora demonstrado quem é o DPO, a Autoridade Nacional de Proteção de Dados (ANPD), e também algumas dúvidas acerca do *Open Banking* (Sistema Financeiro Aberto) e a “nova” Lei do Cadastro Positivo frente a norma de proteção de dados, além do dialoga entre a Lei do Sigilo Bancário e a LGPD.

Superado esse ponto, temos o capítulo cinco onde será demonstrada uma análise dos principais pontos acerca da proteção de dados pessoais, sob a ótica da Lei do Sigilo Bancário, em relação a Lei Geral de Proteção de Dados, bem como uma minuta de Contrato de Termo de Uso e de Política de Privacidade ideal para *fintechs* de serviços financeiros (bancos digitais) em conformidade com a LGPD.

Diante de tudo isso, o trabalho, pretende demostrar que a lei não deixa dúvidas de que a proteção aos dados pessoais é necessária e o setor de serviço financeiro sabe disso e mesmo diante de tantas incertezas e de grandes obstáculos econômicos causados pela pandemia do Covid-19, mostra-se resiliente e inovador

frente à disrupção digital, buscando sempre a melhoria de processos voltado à criação de novos produtos e novos *insights* de modelos de negócio que valorize as pessoas para, assim, alcançar a transformação e se manter competitivo. Dessa maneira, esse trabalho pretende ajudar às empresas de serviço financeiro na adequação a nova legislação, servindo como ponto de partida a entrega de um contrato de Termo de Uso e de Política de Privacidade ideal que agregue eficiência, transparência e segurança no tratamento de dados pessoais

1.1 APRESENTAÇÃO DO TEMA

O presente trabalho trata da análise dos principais aspectos relacionados à Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD), sob o viés da elaboração de um plano de governança de dados adequado destacando o relevante papel dos Contrato de Termos de Uso[1] e de Políticas de Privacidade[2] em conformidade[3] com a Lei para segurança de dados dos usuários de bancos digitais de forma eficiente e significativa frente a atual situação vivenciada para essa modalidade de *fintech*, que vêm ganhando cada vez mais espaço no país, sobretudo em meio aos impactos causados pela COVID 19, oferecendo opções de acesso pelo aplicativo, na tela do celular, de maneira simples e rápida, com oferta de serviços com mais eficiência e melhores taxas, além disso, é possível ter controle das finanças sem burocracia, tarifas caras e o péssimo atendimento das instituições tradicionais do mercado financeiro.

Neste sentido, Bruno Diniz, expõe que os clientes bancários não só não têm interesse em ir até a agências bancárias, como também desejam soluções digitais que proporcionem uma melhor experiência e ofertas que sejam transparentes e façam, de fato, sentido para eles.[4]

Cabe ressaltar, ainda, que é necessária a análise de questões inerentes ao presente caso, sejam estas o entendimento, que *Fintechs*/Bancos Digitais são

---

[1]Documento utilizado na maioria das vezes por sites ou aplicativos, para explicar as condições de uso do serviço disponibilizado.

[2]Política de Privacidade também chamada de termos e condições de segurança por alguns sites. Refere-se às práticas e processos adotados por um site, app, ou outro tipo de provedor de aplicação para tornar transparente sua relação com o usuário. Basicamente, informa ao usuário todos os direitos, garantias, formas de uso, dados recolhidos, processamento e descarte dessas informações pessoais.

[3]Cumprimento de leis, regulamentos, normas técnicas e instrumentos jurídicos.

[4]DINIZ, Bruno. **O Fenômeno *Fintech*:** tudo sobre o movimento que está transformando o mercado financeiro no Brasil e no mundo. Rio de Janeiro: Alta Books, 2019, p.175.

empresas ou iniciativas que trazem novas abordagens e modelos de negócios em serviços financeiros e são escaláveis principalmente através de tecnologia. Já as iniciativas classificadas como de eficiência financeira são organizações que atuam por meio de *bureaus* de informações, soluções de prevenção à fraude, biometria, *blockchain*, *analytics*, além de outras tecnologias e serviços que apoiam e trazem maior agilidade e praticidade ao mercado financeiro.[5]

De acordo, com o Radar *FintechLab*, que faz parte da maior iniciativa de monitoramento do mercado de *Fintechs* nacional, na edição 2020, registrou mais de 270 novas *fintechs,* saltando de 604 em junho de 2019 para 771 em agosto deste ano, nas categorias Pagamentos, Empréstimos, Gestão Financeira, Investimentos, Seguros, *Cryptocurrency, Funding*, Negociação de Dividas, Câmbio de Remessas, Eficiência Financeira e Bancos Digitais. Atualmente, o setor de pagamentos manteve sua posição como principal motor do crescimento do ecossistema *fintech* brasileiro, com um aumento de 26% em quantidade de representantes. Em paralelo, praticamente no mesmo ritmo de evolução aparecem os bancos digitais que passaram de 12 em 2019 para 17 em 2020, crescendo 50%.[6]

1.2 DELIMITAÇÃO DO TEMA

Com a mudança na dinâmica econômica global e os recentes acontecimentos do uso indevido de dados pessoais[7], a LGPD constitui um avanço inegável a segurança da informação de dados. Os dados são um tesouro de suma importância e o armazenamento e utilização inadequado dos mesmos, podem causar danos irreparáveis.

Neste contexto, os bancos digitais, instituições financeiras reguladas pelo Banco Central, que funcionam de forma online (100% digital), tornaram-se uma alternativa viável em tempos de pandemia pela COVID-19, pela necessidade urgente de ter acesso de forma rápida e segura dos dados bancários, com mais eficiência de maneira simples pelo aplicativo, na tela do celular, sem burocracia.

---

[5]FINTECHLAB. **Radar FintechLab mapeia mais de 600 iniciativas.** Disponível em: < https://fintechlab.com.br/index.php/2019/06/12/8a-edicao-do-radar-fintechlab-registra-mais-de-600-iniciativas/>. Acesso em: 19 jun. 2020.

[6]FINTECHLAB. **Novo Radar FintechLab detecta 270 novas fintechs em um ano.** Disponível em: < https://fintechlab.com.br/index.php/2020/08/25/edicao-2020-do-radar-fintechlab-detecta-270-novas-fintechs-em-um-ano/>. Acesso em: 13 set. 2020.

[7]Qualquer informação que seja capaz de identificar ou facilitar a identificação de uma pessoa natural é considerado dado pessoal, nos termos do art. 5º, inciso I, da Lei 13.709/18.

Nessa ótica, tais bancos devem estar em *compliance* com a Lei Geral de Proteção de Dados.

Viktor Mayer, professor da Universidade de Oxford, aponta que as primeiras iniciativas deram errado por tentarem domesticar a tecnologia. Logo se constatou ser impossível prescrever de antemão uma lista fechada sobre seus usos lícitos e ilícitos. Migrou-se, então, para uma abordagem focada na definição dos direitos do titular da informação, cidadãos, consumidores e deveres das organizações que processavam tais dados.[8]

Mas, afinal, o que são esses dados? O dado na tecnologia da informação é a representação física de um evento no tempo e espaço que não agrega fundamento para quem o sente ou recebe, não podendo ser possível entender o que ele representa ou para que ele existe, pode-se ter como exemplo um número, se somente esse número for disponibilizado para alguém ou para o tempo e espaço, por alguém ou por um evento, não é possível saber o que ele significa ou o que ele representa, podendo representar qualquer coisa ou não representar nada, porém no momento que existir uma agregação com outro dado ele passa a ser ou não uma informação. Dados também podem ser um conjunto de informações que constituem uma informação.[9] Sequência de símbolos ou valores, produzidos como resultado de um processo natural ou artificial e representados em qualquer meio.

Para tanto, a LGPD define os dados como: (a) dado pessoal: informação relacionada a pessoa natural identificada ou identificável; (b) dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; (c) dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

De forma geral, a mineração de dados (*data mining*), para utilizar um termo da ciência da computação, sempre procura levar a um lugar: a extração de uma informação. Essa é, também, a racionalidade por trás da regulação (LGPD), por

---

[8]BIONI, Bruno Ricardo. INOVAR PELA LEI. **GVEXECUTIVO**, v. 18, n. 4, jul/ago 2019. FUNDAÇÃO GETULIO VARGAS. ISSN 1806-8979. Pag.30. Disponível em: < file:///C:/Users/Cliente/Downloads/gvexecutivo20194-190826203335.pdf>. Acesso em: 29 mar. 2020.

[9]Dados. In: Wikipédia: a enciclopédia livre. Disponível em: < https://pt.wikipedia.org/wiki/Dados> Acesso em: 29 mar. 2020.

meio da qual a organização precisa não só conhecer os dados que possui, como também deve convertê-los em informação útil. Todo o sistema gira em torno da lógica de se criar uma trilha auditável do dado, um modelo de governança para que o cidadão e os demais agentes envolvidos enxerguem a repercussão do uso dessas informações em suas atividades econômicas e relações sociais.

A Lei Geral de Proteção de dados assegura, ainda, direitos[10] e, simultaneamente, proporciona segurança jurídica para bancos digitais investirem na escolha de inovações tecnológicas. Hoje o Brasil está entre os países com legislação específica para proteção de dados pessoais estabelecendo regras detalhadas para coletas, uso, tratamento[11] e armazenamento afetando todos os setores da economia, inclusive a relação entre clientes e fornecedores de produtos e serviços, empregado e empregador, relações comerciais internacionais e nacionais, além de outras relações nas quais dados pessoais sejam coletados, tanto no ambiente digital quanto fora dele.

1.3 FORMULAÇÃO DO PROBLEMA

Com o intuito de garantir a privacidade e a segurança da informação, em 14 de agosto de 2018, foi sancionada a primeira Lei Geral de Proteção de Dados do Brasil, nº 13.709/2018, que teve a sua vigência em setembro de 2020. Tal Lei veio para reconhecer e regulamentar as relações jurídico-virtuais, pois muitas normas não estavam – e ainda não estão – adaptadas à transformação digital.[12] Trata-se especificamente sobre a regulamentação de dados pessoais, seu uso e destino e seu reflexo direto na forma pela qual as relações se desenvolvem.

---

[10] Acesso; Confirmação de tratamento; Portabilidade; Anonimização, bloqueio ou eliminação de certos dados; Exclusão de dados tratados com base no consentimento, com exceções; Correção; Oposição; Revogação do consentimento; Informações sobre uso compartilhado de dados; Revisão de decisões automatizadas.

[11] Art. 5º, X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

[12] Transformação Digital é o processo de reavaliar um modelo de negócio ou práticas exercidas em uma empresa levando em consideração a disponibilidade e acesso à tecnologia digital. Isto requer coordenação em toda a organização, já que implica na utilização de novas tecnologias para que de fato a mudança ocorra. Para a maioria dos negócios atuais, a principal motivação para esta mudança é a chance de obter vantagens competitivas ao aprimorar a experiência do cliente.

Considerando que a Lei é uma exigência legal, fundamentada nos direitos fundamentais de liberdade e de privacidade[13] e o livre desenvolvimento da personalidade da pessoa natural, de forma que todas as organizações terão que se adequar aos aspectos legais, processuais, tecnológicos, de governança e privacidade e dar mais direitos ao usuário que fornece seus dados, se pergunta: qual o modelo ideal de Contrato de Termos de Uso e de Políticas de Privacidade em conformidade com às disposições legais de proteção na coleta e armazenamento de dados nas relações estabelecidas entre os bancos digitais e seus usuários?

1.4 HIPÓTESES

O Brasil aprovou a sua Lei Geral de Proteção de Dados – LGPD, Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre o tratamento de dados pessoais (art.7º)[14], inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade (art.2º, inc. I) e o livre desenvolvimento da personalidade da pessoa natural.[15] Nesse sentido, a referida Lei que altera a lei 12.965, de 2014[16] nos seus arts. 7º, 16, 61, 62, 63, 64 e 65, surge como um novo marco legal brasileiro de grande impacto, tanto para as instituições privadas como para as públicas, por tratar da proteção de dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais, por qualquer meio, seja por pessoa natural, seja por pessoa jurídica. É uma

---

[13]O direito à Privacidade encontra-se disposto no Artigo 5º, X, da CRFB/88.

[14]Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: **I -** mediante o fornecimento de consentimento pelo titular; **II -** para o cumprimento de obrigação legal ou regulatória pelo controlador; **III -** pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; **IV -** para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; **V -** quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; **VI -** para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; **VII -** para a proteção da vida ou da incolumidade física do titular ou de terceiros; **VIII -** para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; **IX -** quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou **X -** para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

[15] Art. 1º da Lei 13.709/2018.

[16]Marco Civil da Internet - Lei que regula o uso da Internet no Brasil por meio da previsão de princípios, garantias, direitos e deveres para quem usa a rede, bem como da determinação de diretrizes para a atuação do Estado.

regulamentação que traz princípios (art.6º)[17], direitos e obrigações[18] relacionados ao uso de um dos ativos mais valiosos da sociedade digital, que são as bases de dados relacionados às pessoas.

Por conta disso, tem-se que a implementação da conformidade à LGPD trará um impacto grande nas instituições, podendo contribuir para o aumento do "custo Brasil"[19], especialmente nos setores de *Startups,* pequenas empresas e no setor público, com especial atenção aos que tratam de muitos dados pessoais sensíveis[20].

Tanto as empresas nacionais quanto estrangeiras deverão, ainda, resolver difíceis questões como a portabilidade, descarte seguro e o direito do titular à exclusão/alteração dos dados pessoais. Temas estes que envolvem custos elevados e que nos levam à constante preocupação da LGPD se tornar o objeto de inúmeras discussões nos tribunais brasileiros, com pedidos de indenizações por danos morais e materiais em razão do descumprimento da norma.[21]

A complexidade da implementação desse tipo de regulamentação se dá pela expansão da tecnologia no mundo, como resultado dos desdobramentos da globalização, que trouxe como uma de suas consequências o aumento da

---

[17]Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios**: I - finalidade:** realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; **II - adequação:** compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; **III - necessidade:** limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; **IV - livre acesso:** garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; **V - qualidade dos dados:** garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; **VI - transparência:** garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; **VII - segurança:** utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; **IX - não discriminação:** impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; **X - responsabilização e prestação de contas:** demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

[18] *Data Protection Officer* (DPO); Relatório de Impacto (DPIA); Padrões de Segurança da Informação; Registro das Atividades; Códigos de Conduta e Certificação; *Privacyby Design.*

[19]Termo que descreve o conjunto de dificuldades estruturais, burocráticas e econômicas que encarecem e comprometem novos investimentos pelas empresas e pioram o ambiente de negócios no país.

[20]Dado pessoal sensível é o dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

[21]MUKNICKA, Rosana. Você está em *compliance* com a LGPD? **Revista Estadão: 11 jun 2019.** Disponível em: < https://politica.estadao.com.br/blogs/fausto-macedo/voce-esta-em-compliance-com-a-lgpd/>. Acesso em: 29 mar. 2020.

importância da informação. Isso quer dizer que a informação passou a ser um ativo de alta relevância para governantes e empresários: quem tem acesso aos dados, tem acesso ao poder.

Dependendo do ramo do negócio, e da maturidade da governança dos dados pessoais, se torna necessário mecanismos de proteção para os dados daqueles que utilizam serviços, ou realizam qualquer tipo de transação *on-line* que envolva o fornecimento de informações pessoais, isso porque, a falta de transparência no tratamento de dados pessoais podem funcionar como vetor de violação à privacidade, posto que extrapolam os limites da vida privada das pessoas visando as mais diversas aplicações, geralmente de cunho financeiro.

A Governança de Dados[22] visa assegurar, por meio de processos, a qualidade, a transparência e a proteção aos dados, garantindo consistência e confiabilidade durante todo o ciclo de tratamento de dados elevando o nível de satisfação do cliente proporcionando a esse, de fato, uma melhor experiência.

Ao alinhar tecnologia, processos e pessoas para definir papéis, responsabilidades e procedimentos, a equipe de Governança de Dados atua como autoridade articuladora, estabelecendo diretrizes, liderando iniciativas de melhoria e orquestrando a gestão dos dados dentro da *fintech,* e uma forma de viabilizar isso é por meio da determinação dos envolvidos e de suas responsabilidades, cujas atribuições podem ser formalizadas em documentos denominados Contrato de termos de Uso e de Políticas de Privacidade expondo com clareza sobre o tratamento dos dados, a finalidade do seu uso, a justificativa jurídica para tanto, além de novos direitos dos usuários como portabilidade, exclusão, minimização de uso, limitação e outros.

Além do mais, é de fundamental importância a adoção de programas de *compliance* que tragam consigo mecanismos de gestão de dados, em consonância com que estabelece a LGPD, para segurança dos dados captados, adquiridos, processados, tratados, armazenados, descartados e disponibilizados aos clientes internos e externos evitando, portanto, a ocorrência de eventos danosos que

[22]A governança de dados, informação e conhecimento orienta-se pelos princípios da Constituição da República Federativa do Brasil, a Declaração Universal dos Direitos Humanos, o movimento global de Ciência Aberta, o marco legal de Ciência, Tecnologia e Inovação (Decreto nº 9.283, de 7 de fevereiro de 2018) e as diretrizes governamentais de Governança Digital, Divulgação de Informações Relevantes, Transparência, Segurança da Informação e Proteção de Dados Pessoais.

desrespeitem a privacidade, a transparência e a proteção dos dados pessoais, em conformidade com lei.

Assim, diante de tais considerações, o presente trabalho teve por base a uma interpretação sistemática da Lei nº 13.709/2018, abordando conceitos básicos de toda a temática, desenvolvendo uma base, que auxiliará os discursos sobre a história, evolução, atualidades, construções doutrinárias, julgados e pôr fim demonstrar-se-á os procedimentos a serem adotados pelos bancos digitais na elaboração dos seus contratos de Termo de Uso e Política de Privacidade para estar em conformidade (*compliance*) com a lei e proteger seus usuários efetivamente, garantindo à segurança da informação de seus dados pessoais.

1.5 OBJETIVOS

1.5.1 Objetivo Geral

Propor a elaboração de Contratos de Termos de Uso e de Políticas de Privacidade ideal, para bancos digitais, em conformidade com a Lei Geral de Proteção de Dados garantindo, assim, maior segurança da informação desses dados, de forma a prevenir e evitar riscos.

1.5.2 Objetivos Específicos

a) Analisar e identificar os pontos mais relevante da LGPD;
b) Averiguar as posições doutrinárias concordantes e não concordantes no que tange a Lei Geral de Proteção de Dados;
c) Fazer uma revisão das decisões do STF e do STJ para compreender como está ocorrendo à inserção da responsabilidade pela Segurança e Privacidade de Dados;
d) Explanar as formas de responsabilização por parte dos bancos digitais acerca da coleta de dados identificando os fundamentos para responsabilização;
e) Descrever as mudanças regulamentares e a evolução dos Bancos Digitais no Brasil;
f) Elucidar os impactos à Proteção de dados Pessoais em termos de segurança da informação frente à LGPD com a elaboração de um modelo ideal de Contrato de

Termos de Uso e de Políticas de Privacidade adequado às disposições da Lei na coleta e armazenamento de dados de clientes de bancos digitais.

1.6 JUSTIFICATIVA

A sociedade contemporânea vive a chamada transformação digital, na qual grande parte da vida das pessoas passa a ser gerenciada por sistemas informatizados. Na prática, tais sistemas armazenam diversas informações pessoais sobre os indivíduos, que englobam desde meros dados cadastrais como os seus nomes, endereços, *e-mail*, telefones, listas de contatos, etc. Fato é que essas informações, se exploradas, podem fomentar inúmeras aplicações, como manipulação virtual, espionagem, *marketing* direcionado, etc.[23]

Nesse momento de transformação, as preocupações ficam concentradas em alguns aspectos do reuso de dados[24], como os relacionados à privacidade e às práticas de *marketing* e comércio de dados. Porém, para ampliar a visão sobre o tema, é preciso refletir mais profundamente sobre a diversidade de dados e de seus possíveis reuso. Algumas situações, como a análise de dados pessoais para fins comerciais, devem ser regulamentadas, controladas e, em alguns casos, coibidas. Em contrapartida, outras aplicações, como a reutilização de dados para pesquisas nas instituições científicas, devem ser estimuladas e desenvolvidas para que possamos, de fato, nos beneficiar desse novo paradigma informacional.[25]

É difícil imaginar em que momento não estamos trocando dados e, sobretudo, quando nossas vidas não são orquestradas com base no que um banco de dados[26] diz a nosso respeito. Da concessão de crédito, passando pelo acesso a benefícios

---

[23]BARBOSA, Danilo Ricardo Ferreira; DA SILVA, Carlos Sérgio Gurgel. A COLETA E O USO INDEVIDO DE DADOS PESSOAIS: UM PANORAMA SOBRE A TUTELA DA PRIVACIDADE NO BRASIL E A LEI GERAL DE PROTEÇÃO DE DADOS. Disponível em: < http://www.cidp.pt/revistas/rjlb/2019/6/2019_06_0473_0514.pdf>. Acesso em: 5 mar. 2020.

[24]Reuso de dados consiste na utilização de dados para fins diferentes daqueles para os quais eles foram gerados. Implica desafios que vão desde a mudança de processos e de cultura interna até as expectativas e os impactos na sociedade.

[25]LUVIZAN, Simone S. DESAFIOS DE USAR DADOS PARA NOVOS FINS. **GVEXECUTIVO**, v. 18, n. 4, jul/ago 2019. FUNDAÇÃO GETULIO VARGAS. ISSN 1806-8979. Pag.16 Disponível em: < file:///C:/Users/Cliente/Downloads/gvexecutivo20194-190826203335.pdf>. Acesso em: 29 mar. 2020.

[26] Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

sociais até a *timeline* da rede social, todas essas atividades são automaticamente personalizadas com base nos registros que geramos.[27]

Fica claro e evidente, que é preciso garantir a conformidade com os regulamentos de privacidade e segurança, gerenciar e controlar ameaças cibernéticas com eficiência, assegurar a segurança e privacidade em toda a cadeia digital (serviços, aplicativos, dados, infraestruturas e terminais) e controlar os impactos de qualquer incidente de segurança ou violação de dados. Falhas provam que até mesmo gigantes como Google, Microsoft e Facebook não estão a salvo de falta de segurança que podem expor os dados confidenciais de seus usuários.[28]

A justificativa para a escolha do tema ocorreu da necessidade de garantir a privacidade e segurança dessas informações (dados pessoais), seu uso e destino, diante de bancos digitais juridicamente constituídos e regulados pelo Banco Central do Brasil (BACEN), que em tempos de pandemia pelo COVID-19 tornaram-se uma alternativa frente aos impactos sociais e econômicos que vivenciamos atualmente. O confinamento e as regras de distanciamento social estão colocando à prova nossa capacidade de continuar vivendo quase sem interações físicas, algo particularmente importante quando se trata do acesso a serviços sociais essenciais para grandes segmentos da população.[29]

Nesta perspectiva, os bancos digitais oferecem vantagens aos clientes, impactados economicamente pela pandemia, como empréstimo direto, financiamento de bens e serviços, menores juros, isenção de taxas, ausência de filas, serviço por meio de bate-papo *on-line* de forma rápida e segura – geralmente incorporados ao aplicativo do banco, na tela do celular – ou por contato telefônico. Por não ter uma agência, tudo é resolvido por esses canais, com ampla conveniência e transparência para o usuário de maneira fácil, ágil e sem burocracia.

Nesse sentido, a LGPD cria uma regulamentação para o uso, proteção e transferência de dados pessoais no Brasil, nos âmbitos privado e público, e

---

[27]BIONI, Bruno Ricardo. INOVAR PELA LEI. **GVEXECUTIVO**, v. 18, n. 4, jul/ago 2019. FUNDAÇÃO GETULIO VARGAS. ISSN 1806-8979. Pag.30. Disponível em: < file:///C:/Users/Cliente/Downloads/gvexecutivo20194-190826203335.pdf>. Acesso em: 29 mar. 2020.

[28]BARSOTTI, Danilo. Lei GDPR e LGPD: qual a relação na segurança da informação e os impactos nas organizações no mundo. **Revista Estadão: 24 maio 2019.** Disponível em: < https://politica.estadao.com.br/blogs/fausto-macedo/lei-gdpr-e-lgpd-qual-a-relacao-na-seguranca-da-informacao-e-os-impactos-nas-organizacoes-no-mundo/>. Acesso em: 29 mar. 2020.

[29] FARIAS, Pedro. **Serviços públicos à distância:** o que a pandemia nos ensinou. Disponível em: < https://blogs.iadb.org/brasil/pt-br/servicos-publicos-a-distancia-o-que-a-pandemia-nos-ensinou/ >. Acesso em: 19 jun. 2020.

estabelece de modo claro quem são as figuras envolvidas (art. 5º, V, VI, VII, VIII, IX)[30] e quais são suas atribuições, responsabilidades e penalidades[31] no âmbito civil.

Assim, inspirado na União Europeia com seu Regulamento Geral sobre a Proteção de Dados (GDPR),[32] o Brasil aprovou a sua Lei Geral de Proteção de Dados (LGPD) – Lei n° 13.709/2018 que, entrou em vigor no dia 18 de setembro de 2020, e que ainda é bastante impactante e suscita muitas discussões sobre sua eficácia.

Nesse contexto, é importante destacar: que a Lei protege dados (pessoais) para proteger as pessoas. Ao proteger de forma direta os dados pessoais, estabelecendo balizas normativas que definem as condutas que configuram usos justos e éticos desses dados, a legislação de proteção de tais dados pretende tutelar direitos que são fundamentais.[33]

Não obstante, se um dado é considerado como pessoal, por óbvio que está relacionado à pessoa. Logo, por ter esse caráter personalíssimo, qualquer excesso sobre esse tipo de dado pode pôr em risco a privacidade dos cidadãos.[34]

Riscos associados ao processamento de dados pessoais são, de certo modo, a poluição que decorre da sociedade da informação. Esses riscos se materializam, por exemplo, na possibilidade de decisões equivocadas.[35]

É justamente pelo fato de a coleta e a exploração dos dados pessoais se dar de forma obscura e, muitas vezes abusiva, que se impõe a tutela jurisdicional sobre

---

[30] Art. 5:
V- Titular pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
VI-Controlador pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
VII- Operador pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
VIII- Encarregado pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados;
IX- Agentes de tratamento o controlador e o operador.

[31] Penalidades / Multas (2% do faturamento, até 50 milhões de reais).

[32]GDPR – *General Data Protection Regulation*. Regulamento Geral sobre a Proteção de Dados (RGPD) (UE) 2016/679 é um regulamento do direito europeu sobre privacidade e proteção de dados pessoais, aplicável a todos os indivíduos na União Europeia e Espaço Económico Europeu que foi criado em 2018. Regulamenta também a exportação de dados pessoais para fora da UE e EEE. O RGPD tem como objetivo dar aos cidadãos e residentes formas de controlar os seus dados pessoais e unificar o quadro regulamentar europeu.

[33]CARVALHO, André Castro; ALVIM, Tiago Cripa et al. **Manual de *Compliance.*** Rio de janeiro: Forense, 2019. p. 501. ISBN 978-85-309-8315-4.

[34]BARBOSA, Danilo Ricardo Ferreira; DA SILVA, Carlos Sérgio Gurgel. A COLETA E O USO INDEVIDO DE DADOS PESSOAIS: UM PANORAMA SOBRE A TUTELA DA PRIVACIDADE NO BRASIL E A LEI GERAL DE PROTEÇÃO DE DADOS. Disponível em: < http://www.cidp.pt/revistas/rjlb/2019/6/2019_06_0473_0514.pdf>. Acesso em: 5 mar. 2020.

[35]CARVALHO, André Castro; ALVIM, Tiago Cripa et al. **Manual de *Compliance.*** Rio de janeiro: Forense, 2019. p. 500. ISBN 978-85-309-8315-4.

esses dados. Os indivíduos, que são os verdadeiros titulares de seus dados pessoais, terminam por estar sujeitos à violação de sua privacidade sem ao menos se dar conta disso.[36]

E é nesse sentido, que é importante a elaboração de um plano de governança de dados adequado destacando o relevante papel dos Contrato de Termos de Uso e de Políticas de Privacidade, como também um programa de *compliance* eficiente, para prevenir resultados danosos para os bancos digitais, evitando e prevenindo os riscos inerentes às suas atividades. A implementação do programa, de forma impositiva para esse tipo de *fintech* que apresentam riscos, sejam associados ao processamento de dados ou financeiros, traria, mesmo que a longo prazo, grandes resultados, no tocante à redução ou até mesmo exclusão de tais riscos.

Para, Carlos Gómez-Jara Díez, "um dos modelos especialmente idôneo de introdução de causas de exclusão da culpabilidade empresarial é o norte-americano, o qual se baseia nos denominados programas de conformidade corporativos – *Corporate Compliance Programs".*[37]

Então, como se ajustar ou criar *compliance* de Proteção de Dados neste ambiente da LGPD? Considerando-se os riscos do negócio e os preceitos basilares dos programas de integridade, como prevenção, processamento de informações sensíveis, e treinamento de colaboradores, pode-se enquadrar a Lei Geral da Proteção de Dados, perfeitamente como um tema de *compliance***.** Esse *compliance* se entende como o conjunto de estruturas, regras e procedimentos implementados com vistas a assegurar a conformidade do funcionamento da empresa a legislação, normas internas e padrões éticos desejáveis para o mundo dos negócios. Diante disso, para se manter em *compliance* efetivamente, os bancos digitais devem observar as etapas de conformidade da futura lei: (a) conscientização; (b) mapeamento; (c) identificação; (d) planejamento; (e) monitoramento; (f) gerenciamento; (g) análise e conformação jurídica; (h) padronização e implementação das tecnologias de segurança da informação adequadas; (i) *Data Protection Officer* (DPO); (j) *Privacy by Design* e *Privacy by Default.*

---

[36]BARBOSA, Danilo Ricardo Ferreira; DA SILVA, Carlos Sérgio Gurgel. A COLETA E O USO INDEVIDO DE DADOS PESSOAIS: UM PANORAMA SOBRE A TUTELA DA PRIVACIDADE NO BRASIL E A LEI GERAL DE PROTEÇÃO DE DADOS. Disponível em: < http://www.cidp.pt/revistas/rjlb/2019/6/2019_06_0473_0514.pdf>. Acesso em: 5 mar. 2020.

[37]GÓMEZ-JARA DÍEZ, Carlos. **A Responsabilidade Penal de Pessoa Jurídica:** teoria do crime para pessoas jurídicas. 1. Ed. São Paulo: Atlas, 2015, p.100.

Para tanto, é necessária a indicação de um profissional interno, que atue junto ao Comitê de *Compliance*,[38] e que possa se reportar ao *Chief Compliance Officer* (CCO)[39] e a alta administração sobre a realização de novos treinamentos, revisão das políticas do direito à informação, reavaliação contínua de dados pessoais e de transparência e da revisão dos contratos junto aos fornecedores, tendo em vista estes sofrerem mudanças continuas, inclusive em relação aos seus funcionários e com o restabelecimento de novas cláusulas contratuais, sob pena de eventual responsabilização solidária. [40]

Com tudo isso traçado, pede-se adequação. Afinal, a legislação deve ser mais do que simbólica. Para produzir benefícios e gerar valor, tanto para governos e empresas quanto para pessoas, ela necessita ser posta em prática. Assim, chegamos ao *compliance* digital, que é a união entre a conformidade à lei e a tecnologia da informação para a gestão de riscos, ou seja, é o conjunto de protocolos e práticas de segurança com que uma organização, pública ou privada, busca proteger dados e demais informações sigilosas de ataques ou de uso criminoso. Tal conjunto de ações define uma política de *compliance*.[41]

Ante tal cenário, resta claro que a LGPD é o mais novo grande paradigma de conformidade no Brasil. E assim, para estar em *compliance* quando da vigência da lei, os bancos digitais deverão acima de tudo enxergar a proteção de dados pessoais como importante direito dos indivíduos, para tanto, deverão agir com efetiva responsabilidade perante as obrigações a serem cumpridas no intuito de serem estritamente transparentes com os cidadãos e com mercado para conquistar sua confiança. Mais do que nunca fica a certeza de que prevenir é o melhor remédio e por conta disso é fundamental tratar da adequação à LGPD através das ferramentas de *compliance*, contemplando o monitoramento do programa, revisões

---

[38]O Comitê de Controles Internos e *Compliance*, doravante denominado “Comitê”, órgão não estatutário de caráter permanente, e com poderes deliberativos, rege-se por este Regimento e pela legislação aplicável e tem por objetivo assessorar o Conselho de Administração no desempenho de suas atribuições relacionadas à adoção de estratégias, políticas e medidas voltadas à difusão da cultura de controles internos, mitigação de riscos e conformidade com normas aplicáveis à Organização.

[39]O CCO tem a função específica de receber mensagens e falar com pessoas que desviaram do que deveriam fazer, se ocupando de falar mais com quem cometeu algum desvio, logo é um solucionador de problemas.

[40]COSTA, Juliana. A importância da adequação da LGPD aos programas de *compliance*. **Revista Consultor Jurídico: 21dez. 2018** Disponível em: < https://www.conjur.com.br/2018-dez-21/juliana-costa-importancia-adequacao-lgpd-compliance>. Acesso em: 29 mar. 2020.

[41]SARTORI, Adriana. ***Compliance* digital e LGPD:** tudo para seu escritório praticar. 2019. Disponível em: < https://blog.sajadv.com.br/compliance-digital-e-lgpd/>. Acesso em: 29 mar. 2020.

periódicas de análise de riscos e revisão e adequação de treinamento, até porque *compliance* nada mais é do que o estabelecimento de um padrão básico de negócios, perpetrado por ações práticas voltadas a assegurar relações éticas e transparentes entre empresas, mercado e poder público. [42]

[42]FILHO, Renato Valbert de Casto; LUZ, Thiago Terin Luz. **Cuide do seu negócio. Esteja em *compliance* com a LGPD.** Disponível em: < https://www.migalhas.com.br/depeso/307191/cuide-do-seu-negocio-esteja-em-compliance-com-a-lgpd>. Acesso em: 29 mar. 2020.

2 REFERENCIAL TEÓRICO

Com o intuito de fundamentar o presente estudo, este capítulo é designado para apresentar os principais conceitos ou definições que versam sobre os temas de: Transformação Digital, Quarta Revolução Industrial, Dados e as Novas Tecnologias Digitais. Ainda, na sequência, abordaremos alguns pontos relevantes, a respeito do Mercado Financeiro, *Startups* e *Fintechs*/Bancos Digitais.

2.1 TRANSFORMAÇÃO DIGITAL

Conforme explorado anteriormente, não há a menor dúvida de que o tema da transformação digital está cada dia mais inserido no discurso dos bancos digitais. A adoção de tecnologias, que consequentemente traz a transformação digital, beneficia não somente os negócios, mas a sociedade – em um crescimento exponencial.

Falar de transformação digital realmente simboliza discutir a transformação do negócio. Os produtos e serviços experimentarão uma verdadeira revolução, e surgirão serviços de valor agregado que aproveitarão as novas tecnologias para gerar um impacto direto sobre a apresentação de resultados e sobre a experiência com o cliente. Para tanto, é preciso otimizar canais e processos; procurar novos modelos e fluxos de receita com base em exigências dos clientes; e, naturalmente, mudar a cultura interna da instituição para incluir o “digital” no coração de tudo o que é feito.[43] Dessa forma, é possível perceber que a transformação digital é fazer coisas que nunca foram feitas. Mesmo nas transações financeiras mais tradicionais, os bancos digitais, os pagamentos invisíveis e outras simplificações da experiência de consumo obrigaram todos a digitalizar os processos de ponta a ponta. As instituições e mesmo a autoridade reguladora, nesse contexto, aceleraram sua transformação para a nova realidade.[44]

---

[43] LLORENTE, José Antônio. A Transformação digital. **Revista UNO**, 2016, n. 24, p. 09. Disponível em: < https://www.revista-uno.com.br/wp-content/uploads/2013/09/160520_UNO24_BR.pdf>. Acesso em: 29 ago. 2020.

[44] CANTARINO BRASILEIRO. Anuário Brasileiro de Bancos (ABB) 2019. **Relatório Bancário**, 14 ed. São Paulo, 2019. Disponível em: < https://cantarinobrasileiro.com.br/publicacoes/anuariodebancos19/download/>. Acesso em: 26 ago. 2020.

Nesse sentido, o conceito de transformação digital deve ser assim entendido, como um processo pelo qual as instituições utilizam da tecnologia para garantir não apenas seus resultados, como também melhorar o seu desempenho.[45] Tal transformação afeta estratégia, talentos, modelos de negócios e até mesmo a forma como a instituição está organizada. Essa é uma maneira de conquistar a satisfação de clientes e atrair novos – atendendo à demanda existente no contexto atual, suprindo as suas necessidades.[46] Por certo, não é novidade alguma, que uma das principais maneiras de alcançar novos clientes é por meio de tecnologias digitais.

Sendo assim, ir ao guichê do banco para fazer depósitos já é algo impensado às novas gerações (sobretudo as gerações “Millennium” e a “Digital Natives “). É por esse motivo que os serviços digitais são tão chamativos para a nova geração de consumidores que valorizam sua liberdade e seu tempo. Ser atendido de forma simples e rápida é o que a maioria deles preza hoje.

É importante ressaltar, ainda, que temos um grande desafio à frente, principalmente no que tange o montante e a qualidade do investimento em tecnologia, pesquisa e desenvolvimento. Igualmente importante é definir um plano estratégico para que a transformação digital esteja alinhada aos objetivos governamentais de tal forma que o progresso seja mensurável na melhoria da qualidade de vida dos cidadãos. Isso implica: prover transparência dessa estratégia e envolver possíveis agentes que possam contribuir para aceleração desse movimento.[47]

Nota-se, portanto, que é preciso que haja uma mudança estrutural, uma mudança de cultura, uma mudança do famoso *mindset*.[48] Além disso, as instituições, hoje, por certo precisam de novos referenciais para formular suas próprias estratégias, a fim de adaptar-se e crescer na era digital.[49] Aquelas que contam com

---

[45] EROLES, Pedro. ***Fintechs*, Bancos Digitais e Meios de Pagamento:** aspectos regulatórios das novas tecnologias financeiras. São Paulo: Quartier Latin, 2019, p.141.

[46] HSM UNIVERSITY. **A transformação digital nos bancos e o surgimento das *fintechs*.** São Paulo, 2019. Disponível em: < https://hsmuniversity.com.br/blog/transformacao-digital-bancos/>. Acesso em: 26 ago. 2020.

[47] STRAFACCI, Gilberto. **Um resumo do cenário da Transformação Digital no Brasil.** Disponível em: <https://www.setecnet.com.br/artigo-um-resumo-do-cenario-da-transformacao-digital-no-brasil/>. Acesso em: 26 ago. 2020.

[48] MORAIS, Felipe. **Transformação digital.** São Paulo: Saraiva educação, 2020, p.51.

[49] ROGERS, David L. **Transformação digital:** repensando o seu negócio para a era digital. Tradução: Afonso Celso da Cunha Serra. 1º ed. São Paulo: Autêntica Business, 2019. p.25.

uma estratégia abrangente têm tido um desempenho positivo, enquanto outras enfrentam dificuldades.

Neste ponto, David L. Rogers, afirma que a transformação digital passa por cinco domínios fundamentais de estratégia: clientes, competição, dados, inovação e valor.

> 1- Clientes: interagem dinamicamente por meios e modos que transformam suas relações entre si e com as empresas. O uso de ferramentas digitais vem mudando a maneira como descobrem, avaliam, compram e usam os produtos, e como compartilham, interagem e mantêm-se conectados com as marcas.
> 2- Competição: nossos maiores desafiadores podem ser concorrentes assimétricos, isto é, empresas estranhas ao setor, em nada parecidas com a nossa, mas que oferecem aos nossos clientes valores concorrentes. As tecnologias digitais estão turbinando o poder de modelo de negócios de plataforma, permitindo que uma empresa crie e capte enorme valor ao facilitar as interações envolvendo outras empresas ou clientes. Há cada vez mais disputa por influência entre empresas.
> 3- Dados: a maioria dos dados que hoje inunda as empresas não é gerado por qualquer planejamento sistemático, como pesquisa de mercado. Em vez disso, é produto de quantidade sem precedentes de conversas, interações ou processos, dentro ou fora das empresas. Dados são componentes fundamentais sobre como as empresas funcionam, diferenciam-se nos mercados e geram novo valor.
> 4- Inovação: baseia-se no aprendizado continuo por experimentação rápida. Trata-se de experimentos cuidadosos e em protótipos de viabilidade mínima, que maximizam o aprendizado ao mesmo tempo que minimizam os custos.
> 5- Valor: a única prevenção segura em um contexto de negócios e mutação é escolher o caminho da evolução constante, considerando todas as tecnologias como maneira de estender e melhorar a nossa proposta de valor aos clientes.[50]

Observa-se assim, que esses cinco domínios descrevem o panorama da transformação digital para instituições de hoje serem bem-sucedidas. E em face de tudo isso, percebe-se que as tecnologias digitais mudaram a maneira como nos conectamos com os clientes e lhes fornecemos valor transformando a maneira como encaramos a competição. Cada vez mais, nossos recursos competitivos não mais se situam em nossa organização, mas sim numa rede de parceiros que reunimos em relações de negócios mais difusas. Também estão transformando a maneira como as instituições inovam, possibilitando a verificação e a experimentação contínua. Talvez as tecnologias digitais tenham mudado ainda mais o nosso mundo, pela maneira como passamos a considerar os dados, que até pouco tempo eram caros de obter e difíceis de armazenar. Hoje, os dados são gerados em quantidades sem precedentes por pessoas comuns, não só por empresas e organizações, a toda hora

[50] MORAIS, Felipe. **Transformação digital.** São Paulo: Saraiva educação, 2020, p.98-99.

e em todos os lugares, onde o armazenamento na nuvem é cada vez mais barato, acessível e amigável e cujo o maior desafio é converter a enorme quantidade de dados em informações valiosas.[51]

Contudo, é importante destacar ainda, que sem dados, a transformação digital não passa de um monte de ideias. A inovação está no DNA do guarda-chuva do conceito de transformação digital. A concorrência deve ser analisada todos os dias. Não é apenas a sua marca que se transforma, todas o fazem. E, por fim, quanto ao valor: mostre-o ao cliente. As pessoas pagam mais por aquilo em que enxergam valor.[52]

A vista disso, o (quadro 1) comparativo expondo as principais mudanças nos pressupostos estratégicos, da era analógica para era digital:

Quadro 1 – As principais mudanças nos pressupostos estratégicos, da era analógica para a digital

	Da Era Analógica	Para Era Digital
Clientes	- Cliente como mercado de massa; - Comunicações são transmitidas aos clientes; - A empresa é o principal influenciador; - Marketing para induzir à compra; - Fluxos de valor em mão única; - Economias de escala (empresa).	- Clientes como rede dinâmica; - Comunicações fluem em mão dupla; - Os clientes são o principal influenciador; - Marketing para inspirar a compra, a lealdade e a defesa da marca; - Fluxos de valor recíprocos; - Economias de valor (clientes).
Competição	- Competição em setores delimitados; - Distinções nítidas entre parceiros e rivais; - Competição é jogo de soma zero; - Os principais ativos são mantidos na empresa; - Produtos com características e benefícios únicos; - Poucos concorrentes dominantes por categoria.	- Competição entre setores fluidos; - Distinções nebulosas entre parceiros e rivais; - Concorrentes cooperam em áreas-chave; - Os principais ativos situam-se em redes externas; - Plataformas com parceiros que trocam valor; - O vencedor leva tudo, devido aos efeitos de rede.
Dados	- Dados são dispendiosos para serem gerados nas empresas; - O desafio dos dados é armazená-los e gerenciá-los; - As empresas usam apenas dados estruturados; - Os dados são gerenciados em departamentos operacionais; - Os dados são ferramentas para gerenciar processos.	- Dados são gerados continuamente em todos os lugares; - O desafio dos dados é convertê-los em informações valiosas; - Os dados não estruturados são cada vez mais úteis e valiosos; - O valor dos dados é conectá-los entre os departamentos; - Os dados são ativos intangível importante para criar valor.

[51] ROGERS, David L. **Transformação digital:** repensando o seu negócio para a era digital. Tradução: Afonso Celso da Cunha Serra. 1º ed. São Paulo: Autêntica Business, 2019. p.18-20.
[52] MORAIS, Felipe. **Transformação digital.** São Paulo: Saraiva educação, 2020, p.99.

Inovação	- As decisões são tomadas com base na intuição e na autoridade; - O teste de ideias é caro, lento e difícil; - Os experimentos são raros e conduzidos por especialistas; - O desfio da inovação é encontrar a solução certa; - O fracasso é evitado a todo custo; - O foco se concentra no produto “acabado”; - Otimize o modelo de negócios por tanto tempo quanto possível; - Julgue a mudança pela intensidade do impacto sobre o negócio vigente; - O sucesso no mercado dá lugar à complacência.	- As decisões são tomadas com base em testes e validações; - O teste de ideias é barato, rápido e fácil; - Os experimentos são contínuos e conduzidos por todos; - O desafio da inovação é resolver o problema certo; - Os fracassos são fontes precursoras e baratas de aprendizado; - O foco se concentra em produtos de viabilidade mínima e em iterações pós-lançamento; - Evolua antes de ser necessário, para manter-se à frente da disrupção; - Julgue a mudança pela maneira como cria oportunidade para o próximo negócio; - “Só os paranoicos sobrevivem”.
Valor	- Proposta de valor definida pelo setor; - Execute a sua atual proposta de valor.	- Proposta de valor definida pela evolução das necessidades dos clientes; - Descubra a próxima oportunidade de criar valor para o cliente.

Fonte: David L. Rogers[53]

Cabe destacar, ainda, resumidamente, o (quadro 2) guia da transformação digital, com temas estratégicos e conceitos-chaves, conforme se verá a seguir:

Quadro 2 – Guia da transformação digital

Domínios	Temas Estratégicos	Conceitos-Chave
Clientes	Explore as redes de clientes	- Reinvenção do funil de marketing; - Jornada de compra; - Principais comportamentos das redes de clientes.
Competição	Construa plataformas, não apenas produtos	-Modelos de negócio de plataforma; - Efeitos de rede (in)diretos; - (Des)intermediação; - Trens de valor Competitivos.
Dados	Converta dados em ativos	- Padrões de valor dos dados; - Drivers para o *Big Data*; - Tomada de decisão baseada em dados.
Inovação	Inove por experimentação rápida	- Experimentação divergente; - Experimentação convergente; - MVP (produto mínimo viável); - Caminho para escalar.
Valor	Adapte a sua proposta de valor	- Conceitos de valor de mercado; - Caminhos de saída de um mercado em declínio; - Passos para evolução da proposta de valor.

Fonte: David L. Rogers[54]

[53] ROGERS, David L. **Transformação digital:** repensando o seu negócio para a era digital. Tradução: Afonso Celso da Cunha Serra. 1º ed. São Paulo: Autêntica Business, 2019. p.24.

Antes de seguir adiante, vale ressaltar, que o negócio digital é um tema dominante que aborda como a falta de clareza entre os mundos físico e virtual está transformando os projetos de negócios, setores, mercados e organizações. A evolução contínua dos negócios digitais explora novos modelos digitais com o objetivo de alinhar os mundos físico e digital de forma mais direta para colaboradores, parceiros e clientes.[55]

Por essa razão, transformar digitalmente uma empresa ou instituição financeira implica afrontar vários desafios, entre eles o fato de que a disrupção[56] causada pelo digital está se acelerando e, em alguns casos, levando a dinâmicas de mercado em que poucos são os líderes que terminam concentrando a maior fatia do mercado.[57] De certo, estamos diante de uma disrupção sem precedentes e vivendo um momento de grande mudança do mercado financeiro, gerado pelas tecnologias cada vez mais baratas, por uma cultura cada vez mais aberta e por uma regulação mais flexível.[58]

A título de curiosidade, é importante destacar a pesquisa feita pela *McKinsey & Company* sobre a maturidade digital no Brasil. A divulgação do Índice de Maturidade Digital permitiu comparar o desempenho individual da maturidade digital de empresas pares e de líderes digitais no país e no mundo, além de sensibilizar as empresas sobre a importância da digitalização. Nesse sentido, os resultados da pesquisa revelaram cinco *insights* sobre o processo de transformação digital das empresas no Brasil, nos termos que, resumidamente, seguem:

> 1. Os líderes digitais apresentam melhor desempenho financeiro: As empresas líderes em maturidade digital no Brasil alcançam uma taxa de crescimento do EBITA até 3 vezes maior que as demais empresas, –

---

[54] ROGERS, David L. **Transformação digital:** repensando o seu negócio para a era digital. Tradução: Afonso Celso da Cunha Serra. 1º ed. São Paulo: Autêntica Business, 2019. p.26.

[55] GARTNER IT SYMPOSIUM/XPO. **Transformação digital nos negócios.** Disponível em: < https://www.gartner.com/pt-br/conferences/la/symposium-brazil/featured-topics/digital-transformation>. Acesso em: 26 ago. 2020.

[56] A disrupção não é meramente a destituição do líder de mercado. Significa mudar as regras do jogo, o que permite que um novo jogador vença o detentor do recorde, ou seja, é o mercado livre em ação. Sendo lentamente liberado, por meio da tecnologia, dos grilhões de legados existente.

[57] Heitor Martins, H.; Bartolumeu Dias, Y.B.; Castilho, P.; Leite, P. Transformações digitais no Brasil: *insights* sobre o nível de maturidade digital das empresas no país. ***McKinsey&Company*.** Disponível em: <https://www.mckinsey.com/br/our-insights/transformacoes-digitais-no-brasil#>. Acesso em: 26 ago. 2020.

[58] CANTARINO BRASILEIRO. Anuário Brasileiro de Bancos (ABB) 2019. **Relatório Bancário**, 14 ed. São Paulo, 2019. Disponível em: < https://cantarinobrasileiro.com.br/publicacoes/anuariodebancos19/download/>. Acesso em: 26 ago. 2020.

> globalmente, os líderes digitais cresceram 5 vezes mais que as demais empresas.
> 2. A pontuação de maturidade dos líderes digitais no país está próxima à dos líderes globais, mas há grande disparidade de maturidade entre as empresas pesquisadas: os líderes digitais no Brasil apresentam maturidade digital alinhada à dos líderes globais, atingindo uma nota geral média de 66 pontos na ferramenta A&DQ, próxima aos 67 pontos da média dos líderes globais.
> 3. As empresas líderes reconhecem a natureza complementar das práticas e se destacam nas três mais desafiadoras segundo o estudo, enquanto as de menor maturidade desenvolvem práticas pontuais, de forma isolada: os líderes digitais são capazes de capturar a natureza complementar das práticas e suas respectivas dimensões, sem tratamento isolado de cada uma delas; essa qualidade, entretanto, desaparece no grupo de empresas ascendentes. Eles também asseguram o sucesso e a ampla implementação de iniciativas digitais definindo e acompanhando ativamente os KPIS de transformação digital.
> 4. Grande parte das empresas pesquisadas enfrenta desafios em quatro práticas da transformação digital: (a) *Roadmap* específico; (b) Dados e *analytics;* (c) Talento; (d) Mentalidade baseada em dados.
> **5.** A maturidade e a velocidade de transformação das empresas estão correlacionadas ao setor da economia a que pertencem: embora haja empresas líderes em todos os setores, a pesquisa demonstrou que aqueles que apresentam maior maturidade média parecem ser mais homogêneos, com maior concentração de líderes e menos empresas em estágios iniciais de maturidade. Duas hipóteses explicariam esta homogeneização nos níveis de maturidade digital, (i) criação de um diferencial competitivo relevante para as empresas mais avançadas, levando as outras a se movimentarem no sentido de avançar em sua transformação digital, ou (ii) esses setores estão mais próximos do ponto de inflexão, criando um diferencial competitivo relevante para as empresas mais avançadas em digital. **Além disso, no Brasil, três setores claramente despontam em maturidade digital (pontuação acima da média geral) são eles: Serviços financeiros, Varejo, e Telecomunicações e Tecnologia – precisamente, estes são os setores mais afetados pelas mudanças de comportamento e necessidades do cliente, bem como pela dinâmica competitiva. Especificamente, o setor de Serviços financeiros é o que apresenta maior grau de maturidade em modelos e ferramentas e apresenta maior regularidade em todas as dimensões. Neste setor, os bancos são as empresas com o nível de maturidade mais elevado do estudo. Na amostra, 82% das empresas de serviços financeiros têm nota na prática de modelos e ferramentas acima da média nacional, comparado com apenas 35% das empresas dos demais setores. O setor também tem disseminado temas de experiência do cliente, digitalização de processos e jornadas, e implementação do modo ágil de trabalhar. Logo, o serviço financeiro é o setor que apresenta a maior maturidade digital no Brasil e é o segundo mais bem posicionado no mundo. Sua maturidade é superior à média nacional em todas as dimensões e seus líderes se destacam em relação aos demais líderes nas dimensões Capacidades, Organização e Cultura.** [59] (Grifo nosso)

Outro ponto, interessante, é que os bancos digitais, variam em termos de maturidade digital de acordo com o nível de automação e digitalização dos

[59] Heitor Martins, H.; Bartolumeu Dias, Y.B.; Castilho, P.; Leite, P. Transformações digitais no Brasil: *insights* sobre o nível de maturidade digital das empresas no país. ***McKinsey&Company.*** Disponível em: <https://www.mckinsey.com/br/our-insights/transformacoes-digitais-no-brasil#>. Acesso em: 26 ago. 2020.

processos. O nível máximo de maturidade digital significaria ter procedimentos de gestão de risco automatizados, segmentação dinâmica de clientes, ofertas focadas de produtos e serviços, ferramentas complexas de CRM[60] e integração total entre os canais.[61]

Cabe destacar, que a introdução de novas tecnologias modifica a forma como as instituições operam e como os consumidores acessam serviços e produtos. Por isso, usamos o termo inovação para indicar qualquer mudança de tecnologia existente usada por uma instituição e reconhecemos que tal mudança pode assumir duas formas: (a) inovação sustentável refere-se a quaisquer melhorias no desempenho do produto, sendo de natureza incremental ou mais radical, que permita que uma instituição aumente a qualidade da sua oferta, para afastar a concorrência, ou para incrementar as margens comerciais, operando a custos mais baixos ou com preços mais latos acessíveis. Finanças estruturadas ou fundos de investimento seriam alguns exemplos e a (b) inovação disruptiva, ao contrário, poderia resultar em um desempenho pior do produto, pelo menos em curto prazo. Tais produtos revolucionários são geralmente mais baratos, mais simples ou mais convenientes de usar e atraem novos clientes ou criam novas necessidade na clientela existente.[62]

É curioso notar que quando se pensa em inovação, é muito comum relacionar as ideias com *startups*, empresas jovens que se destacam por terem um modelo de negócio diferente ou por investirem em soluções tecnológicas. Mas não são somente as novas organizações que têm essa aptidão inovadora. O setor de serviços financeiros é o mais tecnológico e digitalizado do país. Os bancos investem, anualmente, cerca de R$ 20 bilhões em tecnologia da informação. Sendo assim, inovar é preciso, desde que haja cautela e sustentabilidade, atendendo princípios de segurança e privacidade de dados cada vez mais cobrados e exigidos pela sociedade.[63]

---

[60]CRM é a sigla usada para *Customer Relationship Management* e se refere ao conjunto de práticas, estratégias de negócio e tecnologias focadas no relacionamento com o cliente. O conceito de CRM significa ser centrado no cliente. É estratégia, é um processo, é ferramenta e tecnologia. O CRM armazena informações de clientes atuais e potenciais.

[61]SIMPLY. **Banco digital:** o desafio para o setor financeiro. Disponível em: < https://blog.simply.com.br/banco-digital-desafio-setor-financeiro/>. Acesso em: 26 jun. 2020.

[62]CHISHTI, Susanne; BARBERIS, Janos. **A Revolução Fintech:** o manual das *startups* financeiras. Tradução: Samantha Batista. Rio de janeiro: Alta Books, 2017, p.152-153.

[63]Revista CIAB - FEBRABAN. 2020. **Inovação e segurança devem ser inseparáveis no segmento financeiro.** Disponível em: <https://noomis.febraban.org.br/especialista/patricia-peck-

De igual modo, é inegável que esta onda de inovação e transformação digital promete uma revolução tecnológica que irá democratizar os serviços financeiros, com os seguintes benefícios imediatos: (1) os consumidores terão mais opções, serviços mais direcionados às suas necessidades e preços mais atrativos; (2) as pequenas e médias empresas terão acesso a novas facilidades de créditos e a melhores condições de mercado; (3) o próprio sistema financeiro tornar-se-á mais resiliente, com maior diversidade, redundância e profundidade; (4) e, principalmente, os serviços financeiros serão mais inclusivos, com pessoas melhor conectadas, mais informadas e cada vez mais capacitados.[64]

Assim, é importante destacar o relatório Brazil Digital Report, produzido pela *McKinsey & Company* em parceria com a Brazil at Silicon Valley, publicado em abril de 2019. Esse documento traz de forma organizada algumas informações nos campos da economia brasileira, incluindo o atual cenário digital, empresarial e de inovação. Alguns dos principais destaques do relatório:

> a) No que tange a digitalização, os brasileiros estão prontos e ávidos pela disrupção digital. Mais de 2/3 dos brasileiros têm *smartphones* e gastam em média 9 horas conectados à *Internet* todos os dias (contra 6 horas nos EUA), um dos mais altos do mundo. No entanto, as velocidades da *Internet* a 13 Mbps ainda são muito inferiores às economias desenvolvidas e atrás da média global de 31 Mbps.
> b) O Brasil tem alguns dos consumidores digitais mais ávidos do mundo. Por número de usuários, o Brasil ocupa o segundo lugar no *ranking* mundial para o *WhatsApp*, o segundo para o Instagram, o terceiro para o *Facebook*, o terceiro para o *LinkedIn*, o segundo para o *Pinterest* e o segundo para o *Waze*. No entanto, o *e-commerce* ainda está atrasado em relação às nações mais desenvolvidas, com 6% do total de vendas no varejo (comparado a 20% para a China e 12% para os EUA).
> c) O ecossistema global de *startups* do Brasil está crescendo em um ritmo acelerado, com mais de 10.000 *startups* – 46% das quais com menos de dois anos de idade – e 30.000 empregos. A partir de 2018, existem oito *startups* com status de unicórnio de US $ 1 bilhão (comparado a 13 na Índia e 92 na China). No entanto, o Brasil ainda ocupa a 109ª posição em facilidade de fazer negócios globalmente – por exemplo, leva em média 79 dias para abrir uma empresa (contra metade de um dia no Reino Unido).
> d) **O sistema financeiro brasileiro tem sido um território privilegiado para a inovação.** Mais da metade da população são usuários ativos de serviços bancários *on-line*, e 58% de todas as transações bancárias estão *on-line*. Existem mais de 400 *startups* de tecnologia financeira, e mais de 7 milhões de clientes abriram contas em bancos apenas digitais, a tendência é que os usuários de banco sejam digitais. No entanto, comparado aos países desenvolvidos, o Brasil ainda tem baixa penetração de quase todos os produtos financeiros.

---

pinheiro/inovacao-e-seguranca-devem-ser-inseparaveis-no-segmento-financeiro>. Acesso em: 26 jun. 2020.

[64] CORDEIRO, António Menezes; DE OLIVEIRA, Ana Perestrelo; DUARTE, Diogo Pereira. ***Fintech*:** desafios da tecnologia financeira. 2º ed. Almedina, 2019, p.13.

> e) Algumas áreas que merecem olhares mais cuidadosos e profundos: (i) Saúde: ainda que o país tenha melhorado em alguns indicadores relacionados à saúde, ele ainda está muito atrasado na adoção de tecnologias digitais, com apenas 23% das unidades de saúde usando prontuários eletrônicos e 45% ainda totalmente em papel. Cerca de 300 *startups* brasileiras já enfrentaram o desafio e estão impulsionando a agenda de inovação digital no setor de saúde; (ii) Educação: o desafio de melhorar o desempenho da educação do país é evidente. Mesmo com melhoria em alguns índices como nível médio de escolaridade e taxa de analfabetismo. Mais de 250 *startups* em educação digital estão tentando alcançar escala dentro e fora das salas de aula – as empresas de educação a distância estão liderando o caminho, com 25% de todas as aplicações para o ensino superior; (iii) Governo: a inovação tem transformado os serviços públicos e ainda existem outros campos que as *GovTechs* podem atuar para criar e melhorar os serviços públicos para a população.[65] (Grifo nosso)

Também, cabe observar o relatório DIGITAL 2020: BRASIL (publicado em fevereiro de 2020), feito pela *DataReportal,* que apresentou todos os dados, estatísticas e tendências para entender o uso digital no Brasil em 2020, incluindo os números mais recentes relatados para o número de usuários de internet, usuários de mídia social e conexões móveis.

> **Internautas no brasil**
> - Havia 150,4 milhões de usuários de Internet no Brasil em janeiro de 2020.
> - O número de usuários de internet no Brasil aumentou de 8,5 milhões (+ 6,0%) entre 2019 e 2020.
> - A penetração da Internet no Brasil era de 71% em janeiro de 2020.

> **Usuários de mídia social no Brasil**
> - Havia 140,0 milhões de usuários de mídia social no Brasil em janeiro de 2020.
> - O número de usuários de mídias sociais no Brasil aumentou de 11 milhões (+ 8,2%) entre abril de 2019, janeiro 2020.
> - A penetração das mídias sociais no Brasil era de 66% em janeiro de 2020.

> **Conexões móveis no Brasil**
> - Havia 205,8 milhões de conexões móveis no Brasil em janeiro de 2020.
> - O número de ligações móveis no Brasil diminuiu por 3,4 milhões (-1,6%) entre janeiro de 2019, e janeiro 2020.
> - O número de conexões móveis no Brasil em janeiro de 2020 era equivalente a 97% da população total.[66]

Assim sendo, é importante destacar o estudo, realizado pelo Observatório Febraban (IV) Brasil *online*, de setembro 2020, em parceria com o Instituto de

---

[65]*MCKINSEY&COMPANY*. **Relatório Brazil Digital Report.** 1º edição, 2019. Disponível em: <https://www.mckinsey.com.br/~/media/McKinsey/Locations/South%20America/Brazil/Our%20Insights/Brazil%20Digital%20Report/Brazil-Digital-Report-1st-Edition_Portuguese-vAjustado.pdf>. Acesso em: 29 ago. 2020.

[66]DATAREPORTAL. **Relatório Digital 2020: Brasil.** Disponível em: <https://datareportal.com/reports/digital-2020-brazil>. Acesso em: 29 ago. 2020.

Pagamentos Especiais de São Paulo (Ipespe), que identificou a percepção de aumento do acesso à internet entre a população brasileira: 96% dos entrevistados, em todos os segmentos, consideram que nos últimos cinco anos houve uma evolução positiva do acesso, onde 73% apontam melhoria na qualidade dos serviços de internet no Brasil. Essa percepção de avanço é menos expressiva entre aqueles com 60 anos ou mais (62%) e maior entre os que têm renda acima de 5SM (76%). Todavia, se a maior parcela reconhece uma tendência positiva nas bases do processo de inclusão digital (acesso e qualidade dos serviços), as opiniões dividem-se quanto à avaliação do estado atual de democratização da internet no país: para 48% dos entrevistados “o acesso à internet se ampliou no Brasil e ajudou a democratizar o acesso a informações, conhecimento, lazer e serviços”. Essa avaliação favorável é maior no Nordeste (54%), mas metade (50%) considera que “a internet no Brasil ainda é restrita a uma parcela da população, deixando de fora a maioria das pessoas mais pobres, dos idosos e outros”, visão ligeiramente mais expressiva no Sudeste (55%).

Outro ponto, interessante, ao qual não se pode deixar passar em branco está relacionado a experiência vivida durante o período de quarentena ou *lockdown*, com uso intenso do trabalho remoto, que pode vir a encorajar um “novo normal”, com maior incentivo ao trabalho à distância, com jornadas mais flexíveis e disseminação de novas ferramentas de suporte e engajamento com clientes. Havendo, assim, uma transformação em nossa forma de interagir com as pessoas que amamos, de trabalhar, viajar, receber atendimento médico, gastar nosso tempo livre e conduzir muitas das transações rotineiras da vida. Tais mudanças aceleraram a migração para tecnologias digitais a uma velocidade e em uma escala impressionantes, em todos os setores. Diante dessa nova conjuntura, repleta de desafios e da necessidade de profundas transformações que já vinham se impondo mesmo antes da pandemia, no Brasil, os bancos digitais inovaram ao oferecer contas 100% digitais, sem mensalidade e tarifas e com outros benefícios, como por exemplo, serviços mais rápidos, transparentes, integrados e personalizados.

Cabe mencionar, também, a pesquisa, publicada em julho de 2020, desenvolvida pela KPMG, uma das maiores empresas de prestação de serviços de consultoria e auditoria do mundo. A KPMG verificou no estudo, uma análise das transformações no segmento Bancário, onde um em cada 10 respondentes da pesquisa consideram trocar de instituição financeira – impulsionados pela Covid-19

– sendo que 40% estimam migrar para bancos digitais.[67] Isso porque, quando o assunto é banco digital, as novidades tecnológicas proliferam, bem como o volume de clientes atraídos pelo novo formato.[68]

De fato, a transformação digital chegou e está em nosso presente mais ativa do que nunca. Ela está transformando a maneira com que agimos, nos relacionamos e vemos o mundo. Por meio dela, também estamos mudando como seres humanos. E em tempos de crise, isso é muito bom.[69]Sendo assim, o que se observa é a importância e relevância do meio digital desempenhando papel fundamental nos comportamentos digitais, especialmente quando milhões de pessoas recorrem a dispositivos conectados para ajuda-los a lidar com a vida e o trabalho bloqueados durante e pós COVID-19.

Segundo a edição 2020 do relatório The Networked Readiness Index (NRI), publicado anualmente pelo Fórum Econômico Mundial, na sua segunda edição, de outubro de 2020, baseada na Série Diálogo de Transformação Digital do Portulans Institute, que entrevistou especialistas de alto nível de todo o mundo sobre vários aspectos sobre a aceleração da Transformação Digital em uma economia global pós-COVID, se constatou o seguinte:

> - Suécia, Dinamarca e Cingapura são as sociedades mais preparadas para o futuro. Com três países entre os quatro primeiros globais, a Europa é a região líder mundial.
> - Os Estados Unidos continuam sendo o líder global indiscutível quando se trata de tecnologias do futuro; na verdade, está classificado entre os 10 primeiros em cada um dos cinco indicadores do subpilar (ocupando o primeiro lugar em dois deles).
> - A China agora é um competidor global em áreas-chave, como IA, e-commerce, 5G.
> - A África continua atrás de outras regiões, especialmente quando se trata de acesso, acessibilidade e uso de TICs. Uma vez que o “efeito cascata” da COVID comece a atingir o comércio internacional e os fluxos de investimento, tais divergências entre “economias prontas para a rede” e “retardatários” podem ser amplificadas.

---

[67]KPMG. **Consumers and the new reality.** Disponível em: < https://home.kpmg/br/pt/home/insights/2020/07/consumers-and-the-new-reality.html>. Acesso em: 29 ago. 2020.

[68] CANTARINO BRASILEIRO. Anuário Brasileiro de Bancos (ABB) 2017. **Relatório Bancário**. São Paulo, 2017. Disponível em: < https://cantarinobrasileiro.com.br/publicacoes/anuariodebancos17/download/>. Acesso em: 29 ago. 2020.

[69] Revista CIAB - FEBRABAN. 2020. **O que era uma opção virou necessidade**: a transformação digital em tempos de pandemia! Disponível em: < https://noomis.febraban.org.br/especialista/alessandra-montini/o-que-era-uma-opcao-virou-necessidade-a-transformacao-digital-em-tempos-de-pandemia>. Acesso em: 29 ago. 2020.

> - Em todos os tipos de economia, os investimentos em tecnologia por si só não podem garantir níveis mais altos de prontidão da rede. A capacidade das economias nacionais de sustentar os esforços para permitir a requalificação e qualificação de sua força de trabalho e talentos locais é a chave para seu futuro. Os pacotes de recuperação terão um papel fundamental a desempenhar.
> - As estratégias de COVID e bloqueio aceleraram a transformação digital. Isso cria oportunidades e desafios, como possíveis aumentos nas desigualdades. Mecanismos de governança apropriados são necessários para mitigar a questão sem prejudicar a primeira.
>
> **Atenção:** Embora tenha havido algumas mudanças de classificação dentro do grupo, os países no NRI 2020 top 10 permanecem os mesmos da edição do ano passado . Todas as 10 principais economias são economias de alta renda; oito países são europeus, enquanto Cingapura é a única economia com maior posição situada na Ásia e no Pacífico, e os Estados Unidos são o único localizado nas Américas. Uma característica distintiva dos 10 melhores desempenhos é que eles se saem bem na maioria das dimensões do NRI. Na verdade, eles estão todos entre os 15 países com melhor classificação em cada um dos quatro pilares (Tecnologia, Pessoas, Governança e Impacto) e têm um desempenho igualmente bom em pelo menos dois terços dos 12 subpilares. 17 dos 25 principais países estão na Europa (principalmente na Europa do Norte e Ocidental), quatro economias estão no Leste e Sudeste Asiático, duas estão na Oceania (Austrália e Nova Zelândia) e duas estão na América do Norte (Canadá e Estados Unidos Estados).[70]

Ademais, segundo a quarta edição do Observatório Febraban 2020, os brasileiros com acesso à internet já vivenciam uma expressiva digitalização de atividades e mais de um terço desse universo espera aumentar suas atividades *online* (35%) no período pós-pandemia. Apenas 9% esperam diminuí-las, e 55% acreditam que não haverá mudanças em seus hábitos digitais. Nesse item, variações entre os segmentos de público foram pouco expressivas. No mundo pós-pandêmico, 66% dos brasileiros conectados esperam acessar a internet preferencialmente das suas casas. Entre aqueles com 60 anos ou mais, este percentual é de 81%. Um quinto (24%) aposta no acesso principalmente a partir do trabalho. Além disso, a frequência das seguintes atividades após a pandemia: 30% acompanhar notícias e informações (e 54% vão manter a frequência); 29% acessar as redes sociais (e 55% vão manter); 29% estudar, fazer cursos e ter aulas a distância (e 29% vão manter); 29% conversar e se relacionar com amigos e familiares por meio de vídeo (e 45% vão manter) e 28% trabalhar, fazer reuniões e outras atividades profissionais pela *net* (e 28% vão manter); 27% usar serviços bancários digitais (45% vão manter); 27% realizar serviços públicos pela internet

[70]PORTULANS INSTITUTE. **Relatório The Networked Readiness Index (NRI).** 2ºed. 2020. Disponível em: < https://networkreadinessindex.org/wp-content/uploads/2020/10/NRI-2020-Final-Report-October2020.pdf>. Acesso em: 29 ago. 2020.

(40% vão manter); 26% fazer compras *online* (38% vão manter); e 26% acessar filmes e séries por serviços de *streaming* (40% vão manter).

É importante frisar, ainda, que para 2021, está previsto priorizar a implementação de um conjunto de ações estratégicas de transformação digital, incluindo aquelas voltadas: (i) à ampliação das redes de telecomunicações e de acesso à Internet; (ii) a novos avanços em segurança cibernética; (iii) à educação e à capacitação profissional em tecnologias digitais; (iv) à aceleração das *startups* digitais; e (v) à disseminação dos instrumentos de governo digital em todos os níveis da Federação.

Com base nessas informações, pode-se concluir que a transformação digital representa o desafio de entender o quão disruptiva é a tecnologia digital e o quanto já está a afetar a experiência do cliente... e mudar a forma como as instituições precisam de passar a fazer o seu negócio.[71] Por certo, essa transformação é uma realidade, que está cada vez mais presente nos bancos digitais, com suas tecnologias inovadoras, transformando a relação com o cliente final, hoje mais conectado e informado, habituado à tecnologia, que espera e exige melhores serviços e mais conveniência. Não se trata de apenas ofertar facilidades a partir dos serviços digitais, mas de proporcionar novas experiências, capazes de transformar o dia a dia dos clientes. Logo, a transformação digital como consequência da transformação do cliente se torna um avanço essencial para a sustentabilidade das instituições financeiras devido ao ambiente de negócios em constante evolução e às mudanças na mentalidade de seus consumidores.

Após compreender-se um pouco sobre transformação digital é importante uma análise dos aspectos relevantes da quarta revolução industrial, como se verá a seguir.

2.2 QUARTA REVOLUÇÃO INDUSTRIAL

Antes de mais nada, é importante ressaltar que para melhor compreensão do assunto, será apresentada, de maneira clara e objetiva, algumas noções básicas sobre a quarta revolução industrial tendo como foco principal conceitos ou definições, bem como seus impactos.

---

[71]ALCARVA, Paulo. **Banca 4.0. Revolução Digital:** *fintechs, blockchain*, criptomoedas, *robo-advisers* e *crowdfunding*. Coimbra: Conjuntura Actual Editora, 2018, p.45.

O mundo à nossa volta está mudando – em nossos negócios e em nossa vida pessoal, estamos "*mobile*", conectados e regularmente interagindo com pessoas de todo o mundo. Temos uma gama de dispositivos eletrônicos em nossos bolsos, mesas e casas, o que significa que não pensamos duas vezes em pegar o que estiver mais perto para enviar fundos de um país para outro, comprar itens *online* de pessoas que não conhecemos e administrar nossas finanças pessoais. Precisa ser rápido, precisa ser agora e precisa ser conveniente.[72]

Nesse cenário, deparamos com a possibilidade de um mundo virtual com o desenvolvimento de novas tecnologias cada vez mais rápidas e sofisticadas que nos direcionam para uma próxima etapa do desenvolvimento humano, a era das conexões e inter-relacionamentos, onde máquinas já dialogam com outras máquinas e com os humanos, absorvendo uma imensidão de informações e deliberando sobre diversos assuntos de nossa vida cotidiana.[73]

Palavras e expressões como *Fintechs, Big Data, Blockchain*, Inteligência Artificial, Internet das Coisas, Cibersegurança são alguns exemplos dos conceitos que dão corpo à profunda transformação que as economias estão a conhecer: a quarta revolução industrial, a da economia digital, revolução que consiste na fusão de métodos correntes de produção com os mais recentes desenvolvimentos na tecnologia da informação e comunicação, e que se tem desenvolvido a um ritmo frenético, impulsionado pela tendência de digitalização da economia e da sociedade. Está garantida, desde já, a sustentação tecnológica desta revolução, graças a sistemas inteligentes e interligados que permitem que pessoas, máquinas, equipamentos, sistemas logísticos e produtos comuniquem e cooperem diretamente entre si.[74]

De acordo com Klaus Schwab, a primeira revolução industrial ocorreu aproximadamente entre 1760 e 1840 trazendo à tona a máquina a vapor e as ferrovias, dando início à produção mecânica. A segunda ocorreu no final do século XIX com o advento da eletricidade e da linha de montagem. A terceira começou na década de 1960 com a revolução digital ou do computador e de várias outras

---

[72]CHISHTI, Susanne; BARBERIS, Janos. **A Revolução *Fintech*:** o manual das *startups* financeiras. Tradução: Samantha Batista. Rio de janeiro: Alta Books, 2017, p.109.

[73] SOARES, Matias Gonsales. **A Quarta Revolução Industrial e seus possíveis efeitos no direito, economia e política.** Disponível em: < https://migalhas.uol.com.br/arquivos/2018/4/art20180427-05.pdf>. Acesso em: 30 ago. 2020.

[74] ALCARVA, Paulo. **Banca 4.0. Revolução Digital:** *fintechs, blockchain*, criptomoedas, *robo-advisers* e *crowdfunding*. Coimbra: Conjuntura Actual Editora, 2018, p.15.

tecnologias digitais, como por exemplo, semicondutores, *mainframes*, computadores pessoais e internet. A quarta revolução industrial ocorreu de acordo com o autor na virada do século. É a era da convergência das tecnologias digitais, físicas (as coisas) e biológicas (as pessoas), uma revolução tecnológica que já começa a mudar a forma de vida, trabalho e de relacionamento, com o crescimento exponencial da capacidade de computação. Existem forças e fatores que torna essa revolução fundamentalmente diferente das anteriores: (a) Velocidade: é incomparável e nunca na história houve mudanças tão rápidas e significativas; (b) Amplitude: as mudanças se estendem por todos os setores do mercado e da sociedade, desde das áreas de exatas, humanas, biológicas e também intercalando todas em diversos momentos; (c) Profundidade: as mudanças abalam os sistemas bases de todos os setores reformulando-os dos pés à cabeça, mudando até mesmo a própria maneira de fazer o mercado e o comércio; (d) Megatendências tecnológicas: força impulsionadora dessa revolução. As inovações tecnológicas cominam em megatendências que resultam em produtos, serviços e métodos que intercalam todos os domínios da sociedade excluindo assim as barreiras que limitam o poder de abrangência do mercado explorando a capacidade de disseminação das informações e dados na digitalização e na tecnologia de informação. Essas megatendências podem ser: (i) Físicas: veículos autônomos, impressão 3D, robótica avançada e novos materiais; (ii) Digital: internet das coisas, plataformas digitais e a criação de novas moedas; (iii) Biológica: genética (biologia sintética, engenharia genética e xenotransplantes); (iv) Ética: ponto mais influente que norteia as decisões humanas usada para julgar as inovações viáveis ou inviáveis.[75]

O mesmo autor, ainda, aponta impactos positivos e negativos causados por essa revolução:[76]

Impactos Positivos: para enxergar todos os benefícios o gestor precisa ter liderança, uma visão estratégica dos negócios (inteligência de mercado) investindo na modernização dos processos (dimensões nacionais e globais) com isso haverá uma grande redução nos custos de produção com máquinas inteligentes, deste modo o gestor ao identificar demandas e tendências do mercado poderá agir com

[75] SCHWAB, Klaus. **A quarta revolução industrial.** Tradução: Daniel Moreira Miranda. São Paulo: Edipro,2016, p.18-35.
[76] SCHWAB, Klaus. **A quarta revolução industrial.** Tradução: Daniel Moreira Miranda. São Paulo: Edipro,2016, p.38-48.

muita velocidade para colocar um novo produto na rua, por exemplo, assim a realidade trás impactos positivos também para o público consumidor que terá maior acesso a produtos personalizados de qualidade e a um custo menor.

Impactos Negativos: distribuição de poder na mão de pessoas que tem mais conhecimento de tecnologia; *ciberataques* (espionagem industrial) e utilização de inteligência artificial para fins escusos como golpes, guerras e *fake news*. Com relação ao trabalho a indústria potencializa a automação (as máquinas assumem a função humana), já não se pode mais contar com o fator natureza humana, resultando assim numa diminuição na oferta de emprego (desemprego). Necessidade de as pessoas aperfeiçoarem suas competências para lidar com todas as novas tecnologias e garantir sua empregabilidade. Outros pontos a serem considerados são os riscos do aumento da desigualdade social, mudanças políticas e na forma de pensar de cada um, insegurança quanto as inovações bélicas e os impactos causados com a super saturação de inovações tecnológicas, a conectividade e a interatividade entre pessoas, Estados e de pessoas com o Estado (o grande acesso de informações e ferramentas de *aplaude* de dados) geram problemas quase que irreparáveis.

Observa-se assim, que sempre que o mundo está diante de uma mudança tecnológica, é grande o medo do desemprego em massa. Com as “tecnologias 4.0” ficará cada vez mais difícil para trabalhadores menos qualificados encontrarem um emprego. Muitos postos de trabalho poderão desaparecer inclusive no setor de média qualificação. A combinação dos processos de decisão autônomos, a inteligência artificial, com a integração entre dispositivos e mercadorias proporcionada pela “internet das coisas” e mais o acesso a grandes volumes de dados para apoio à decisão, eliminaria a necessidade de participação do homem em uma variedade de atividades, em praticamente todos os setores da economia, levando a um desemprego crônico.[77]

Diante disto, é possível perceber que desde o tear até a impressora 3D, as tecnologias vêm impactando não só os modos de produção, mas também um

[77] RODRIGUES, Vivian Machado. Tecnologias 4.0 nos bancos e os impactos no emprego bancário. **Revista ciências do trabalho**: ISSN 2319-0574, nº 9, dez. 2017. Disponível em: < https://rct.dieese.org.br/index.php/rct/article/view/153/pdf>. Acesso em: 30 ago. 2020.

realinhamento das relações dos seres humanos com o mundo. Nessa profunda mutação, a tecnologia digital tem um papel crucial.[78]

De imediato, o que se tem denominado de “Revolução 4.0” resulta de um novo salto tecnológico que tem em sua base a microeletrônica associada à informação apropriada por grandes corporações, grupos e indivíduos privados. Um salto que permite acelerar o tempo e condensar o espaço, e que gera no mundo, não o fim do trabalho, mas a crise estrutural do emprego.[79] Contudo, essa revolução representa uma oportunidade para as instituições redefinirem seus clientes, a experiência que têm com seus serviços e produtos e atingirem novos patamares de produtividade, pois cada vez mais os usuários do século 21, consumidores “vorazes” de tecnologia, valorizam uma marca quando sentem uma conexão emocional mais inteligente e mais profunda.[80]

A partir de então, chegamos ao Século XXI com a chamada “Tecnologia Disruptiva”, onde damos um salto de qualidade e produtividade. Disrupção é uma expressão utilizada para representar as inovações disponibilizadas pelo mercado em forma de produtos amigáveis e a preços módicos, criando um novo nicho de atividade, desequilibrando as antigas empresas que encabeçaram o setor.[81]

Estes são sintomas claros, que indicam que estamos imersos em uma autêntica revolução digital, onde as tecnologias digitais criaram uma espécie de segunda economia (para não lhe chamar impudicamente paralela), virtual e autônoma, não assente em trabalhadores humanos auxiliados por meios tecnológicos, mas em algoritmos e máquinas da economia virtual.[82] Desse modo, a tecnologia digital revolucionou a maneira de consumir, de nos comunicar, a forma

---

[78] SANTOS, João Vitor. Entrevista com Yann Moulier Boutang. **IHU On-Line Revista Instituto Humanitas Unisinos**, São Leopoldo, ano 18, n. 525, p.49-55, 30 jul. 2018. Disponível em: < http://www.ihuonline.unisinos.br/artigo/7350-capitalismo-no-seculo-xxi-e-a-forca-cerebral-no-cerne-da-cadeia-do-valor>. Acesso em: 30 ago. 2020.

[79] SANTOS, João Vitor. A Revolução 4.0 e a reedição das lógicas das revoluções burguesas. Entrevista com Gaudêncio Frigotto. **IHU On-Line Revista Instituto Humanitas Unisinos**, São Leopoldo, ano 19, n. 544, p.41, 04 nov. 2019. Disponível em: < http://www.ihuonline.unisinos.br/media/pdf/IHUOnlineEdicao544.pdf>. Acesso em: 30 ago. 2020.

[80] LLORENTE, José Antônio. A Transformação digital. **Revista UNO:** 2016, n. 24, p. 39-50. Disponível em: <https://www.revista-uno.com.br/wp-content/uploads/2013/09/160520_UNO24_BR.pdf>. Acesso em: 30 ago. 2020.

[81] SOARES, Matias Gonsales. **A Quarta Revolução Industrial e seus possíveis efeitos no direito, economia e política.** Disponível em: < https://migalhas.uol.com.br/arquivos/2018/4/art20180427-05.pdf>. Acesso em: 30 ago. 2020.

[82] ALCARVA, Paulo. **Banca 4.0. Revolução Digital:** *fintechs, blockchain*, criptomoedas, *robo-advisers* e *crowdfunding*. Coimbra: Conjuntura Actual Editora, 2018, p.30.

como pensamos e trabalhamos, e transformou radicalmente a forma como fazemos negócios.[83]

Vale destacar que a tecnologia digital teve várias fases que se estenderam por um período que ultrapassou aquele das transformações técnicas da Revolução Industrial, conforme destaca Yann Moulier Boutang:

> Entre 1936 (Turing), a decodificação do código Enigma (1940-43), as bases do computador (1945), a fabricação dos grandes computadores, os computadores pessoais baseados na revolução cibernética, a calculadora e o processamento da informação numérica (1940-1950), os grandes computadores, a internet, o celular, a internet das coisas. A revolução da supracondutividade, da fibra ótica, a miniaturização dos transistores, as nanotecnologias ampliaram as capacidades de memória e cálculo (a Lei de Moore, que está começando apenas agora a desacelerar), bem como a transmissão. A fase da *web* 1.0 se contentava com a exibição de conteúdo por *download*. Com a *web* 2.0, a interação se torna efetiva (pode-se comentar, marcar conteúdos, ter um *blog*, reagir, anotar, escolher diversos aplicativos, conectar-se a redes profissionais e sociais). A *web* 3.0 é aquela do armazenamento da informação, do *Big Data*, gerados pelo rastreamento da interatividade na internet das coisas, e da personalização do consumo, da produção. Essa fase é coroada hoje pelo empreendimento 4.0 e pela generalização da inteligência artificial em todos os níveis. O digital entra não apenas nos serviços de gestão de informática e logística, mas também na concepção, na "*robótica*" (uso de robôs combinados com humanos), na fabricação por robôs ou por impressoras 3D, substituindo, sobretudo, tarefas de serviços considerados complexos por inteligência artificial, isto é, por algoritmos aprendizes, geralmente por *machine learning* com base em redes neuronais. Essa indústria de fabricação e serviços por *software* 4.0 tem um poder de substituição do emprego muito qualificado comparável somente com a onda de mecanização da Revolução Industrial (1750-1850). A força de trabalho está cada vez menos no centro da produção. São a força cerebral e a força de invenção que estão no cerne da cadeia do valor. Em todas as atividades, a atividade humana se situa na origem da concepção, durante a fabricação, na supervisão, no controle das máquinas, e, na outra ponta, nos processos de design do consumo. A principal força produtiva passa a ser a ciência e suas aplicações.[84]

De acordo com o Technology Vision Consumer Survey, 52% dos consumidores dizem que a tecnologia desempenha um papel proeminente ou está enraizada em quase todos os aspectos de suas vidas diárias. Na verdade, 19% relatam que a tecnologia está tão interligada com suas vidas que a veem como uma

---

[83] LLORENTE, José Antônio. A Transformação digital. **Revista UNO:** 2016, n. 24, p. 55. Disponível em: < https://www.revista-uno.com.br/wp-content/uploads/2013/09/160520_UNO24_BR.pdf>. Acesso em: 29 ago. 2020.

[84] SANTOS, João Vitor. Capitalismo no século XXI e a força cerebral no cerne da cadeia do valor. Entrevista com Yann Moulier Boutang. **IHU On-Line Revista Instituto Humanitas Unisinos**, São Leopoldo, ano 18, n. 525, p.49-55, 30 jul. 2018. Disponível em: < http://www.ihuonline.unisinos.br/artigo/7350-capitalismo-no-seculo-xxi-e-a-forca-cerebral-no-cerne-da-cadeia-do-valor>. Acesso em: 30 ago. 2020.

extensão de si mesmos. Globalmente, as pessoas passam em média 6,4 horas *online* diariamente. Eles são pós-digitais.[85]

Por isso, é fundamental entender que, a tecnologia digital desafia o setor de serviços financeiros de duas maneiras. Em primeiro lugar, ela está transformando os negócios tradicionais. Um exemplo disso é o número de transações financeiras que migraram dos meios tradicionais para aplicativos móveis e via internet, proporcionando mais opções aos clientes. A outra maneira é como o processamento financeiro está sendo acelerado e os custos de transações sendo reduzidos. Desse modo, a tecnologia digital está reinventando os negócios financeiros e novos modelos estão sendo introduzidos no mercado.[86]

Dessa forma, é possível perceber o quanto essa revolução tecnológica digital foi importante para o setor financeiro que sempre esteve na vanguarda da inovação tecnológica, responsável pela transformação do setor. Atualmente, qualquer definição estratégica sobre negócio bancário só pode ser concretizada se for enquadrada num ambiente de mobilidade, interatividade e adaptabilidade continua. A evolução tecnológica dos últimos tempos alterou significativamente a forma como os clientes se relacionam com seus bancos, essa transformação se deve essencialmente, ao forte desenvolvimento da oferta de soluções bancarias através de dispositivos móveis, em particular o tele móvel (*smartphones*) com uma abordagem ágil e rápida na prestação do serviço, onde plataformas *online*, com uma leve estrutura de custos, conseguem oferecer ao cliente um serviço mais rápido e mais barato.[87]

Além do mais, é importante destacar a pesquisa feita pelo Anuário Brasileiro de Bancos abb 2020, elaborado pelo Cantarino Brasileiro, especializada em inovação, pesquisas, ações e conteúdo editorial para o mercado financeiro, em sua edição de nº 15, relatou que as operações com movimentação financeira no *smartphone* tiveram 41% de incremento e todas as transações pesquisadas avançaram no período: contratação de investimento (alta de 114%); tomada de crédito (+47%); transferências, DOCs e TEDs (+43%); pagamento de contas (+39%)

---

[85] ACCENTURE. **Technology Vision Consumer Survey 2020**. Disponível em: < https://www.accenture.com/us-en/insights/technology/technology-trends-2020>. Acesso em: 30 ago. 2020.

[86] RUBINI, Agustin. **A Fintech em um Flash**. Tradução: Fernanda Belokurows. Babelcube Inc., 2017. Livro eletrônico, não paginado.

[87] ALCARVA, Paulo. **Banca 4.0. Revolução Digital:** *fintechs, blockchain*, criptomoedas, *robo-advisers* e *crowdfunding*. Coimbra: Conjuntura Actual Editora, 2018, p.35.

e contratação de seguros (+133%). Além disso, houve migração de operações sem movimentação financeira dos ATMs (-4%) e do *internet banking* (1%) para o *smartphone*. Logo, tudo vai migrar para o celular, com diminuição da necessidade de dinheiro físico, que gera transporte e abastecimento caros. As transações vão ser cada vez mais digitais, seguras e transparentes.

Note-se ainda que o isolamento social teve impacto evidente nos serviços bancários digitais. Impulsionado inclusive pelo aumento de contas digitais decorrente do pagamento do Auxílio Emergencial, instituições financeiras reforçaram suas soluções tecnológicas, lançaram ferramentas e aprimoraram aplicativos. Por sua vez, consumidores passaram a evitar operações presenciais, recorrendo aos serviços *online*. O Observatório Febraban, em sua quarta edição de 2020, confirma essas tendências nas operações financeiras e no consumo no ambiente digital, onde 48% dos respondentes acreditam que depois da pandemia irão utilizar mais o atendimento bancário digital. Como esperado, este percentual é menor entre os de 60 anos ou mais (22%); os que têm nível fundamental (37%); aqueles com renda até 2SM (39%); e na região Nordeste (43%). No total, apenas 13% declaram que vão utilizar mais o serviço presencial e 37% creem que vão utilizar as duas modalidades após a pandemia. Ainda, para 43% dos respondentes, o aplicativo do celular será o principal meio de acesso para fazer operações bancárias, seguido de longe pelo *internet banking* (22%), caixas eletrônicos (12%) e agências físicas (11%). Também nesse caso, os mais velhos, com menor instrução e com menor renda mostram-se menos afeitos à opção digital.

E o que exatamente essa tecnologia móvel pode fazer? Tudo o que seria feito tradicionalmente dentro do sistema bancário, incluindo financiamento de cadeia de suprimento, empréstimos, microfinanças de curto prazo e empréstimos comerciais, mais padrões, economias, credito rotativo, etc. Todos esses instrumentos financeiros podem ser acessados com o toque de um dedo ou o clique de um botão. E estão ocorrendo fora da infraestrutura bancaria sobre uma tecnologia móvel pura, segura e elegante.[88]

De fato, é inegável que, para que isso se torne possível, é preciso uma infraestrutura de rede e aplicações de tecnologias de comunicação e informação bem desenvolvida, adaptada às condições regionais, nacionais e locais, de fácil

[88] CHISHTI, Susanne; BARBERIS, Janos. **A Revolução Fintech:** o manual das startups financeiras. Tradução: Samantha Batista. Rio de janeiro: Alta Books, 2017. p.68.

alcance e a preço acessível, e consequentemente, a ampliação da utilização da banda larga e de outras tecnologias inovadoras.[89]

É importante ressaltar que, estabelecer esse novo nível de resiliência em operações pode ser dispendioso, tanto em termos de tempo como de recursos. No entanto, a boa notícia é que os líderes em inovação já demonstraram como a "Indústria 4.0" (ou a Quarta Revolução Industrial, com seu conjunto de ferramentas e abordagens analíticas e digitais) pode reduzir substancialmente o custo da flexibilidade. Em suma, operações de baixo custo e alta flexibilidade não são apenas possíveis – elas já estão ocorrendo. A maior parte das empresas do setor financeiro já estava no processo de digitalizar suas operações antes da chegada da pandemia. Se elas acelerarem esses esforços agora, é provável que possam perceber benefícios em produtividade, flexibilidade, qualidade e conectividade com o cliente final.[90]

Nota-se, portanto, que está em curso a chamada quarta revolução industrial, resultando na Indústria 4.0, expressões usadas para descrever as profundas mudanças ocasionadas pela crescente adoção de tecnologias digitais pela sociedade. Tal fenômeno pode ter impactos comparáveis ou superiores àqueles experimentados em ciclos tecnológicos anteriores. A Indústria 4.0 agrega ao processo de automação, que marcou a terceira revolução industrial, elementos da conectividade, da coleta e do processamento de dados em tempo real e em larga escala. As redes de telefonia móvel de quinta geração (5G), a Internet das Coisas e a inteligência artificial são tecnologias que compõem essa nova realidade, com inúmeros impactos para a sociedade nas mais diversas áreas, como emprego, trabalho, saúde, segurança pública e proteção de dados.[91]

---

[89] Documentos da Cúpula Mundial sobre a Sociedade da Informação [livro eletrônico]: Genebra 2003 e Túnis 2005 / International Telecommunication Union; [traduzido por Marcelo Amorim Guimarães]. São Paulo: Comitê Gestor da Internet no Brasil, 2014, p.24. Disponível em: < https://www.cgi.br/media/docs/publicacoes/1/CadernosCGIbr_DocumentosCMSI.pdf>. Acesso em: 30 ago. 2020.

[90] SNEADER, Kevin; STERNFELS, Bob From surviving to thriving: reimagining the post-covid-19 return. **McKinsey & Company.** Disponível em: < https://www.mckinsey.com/featured-insights/future-of-work/from-surviving-to-thriving-reimagining-the-post-covid-19-return/pt-br>. Acesso em: 19 out. 2020.

[91] BRASIL. Presidente (2019 -: Jair Messias Bolsonaro). **Mensagem ao Congresso Nacional, 2020:** 2ª Sessão Legislativa Ordinária da 56ª Legislatura. – Brasília: Presidência da República, 2020. – (Documentos da Presidência da República). Disponível em: < https://static.poder360.com.br/2020/02/Mensagem-ao-Congresso-2020.pdf>. Acesso em: 29 ago. 2020.

Com base nessas informações, pode-se concluir que a quarta revolução industrial (revolução tecnológica), também chamada de “Industria 4.0” ou “Revolução 4.0”, expandiu as possibilidades de uma transformação digital efetiva, tornando-a um diferencial competitivo ao negócio. Tal revolução combina e conecta tecnologias digitais, físicas e biológicas para impulsionar empresas mais flexíveis, responsáveis e interconectadas, capazes de tomar decisões mais acertadas de maneira mais eficiente: mais inteligente, rápida e precisa. Sejam, por isso, bem vindos ao admirável mundo dos bancos digitais (*fintechs* de serviços financeiros), que estão a transformar o modelo de negócio de todo o setor financeiro, impactando de maneira profunda as nossas vidas, com seus avanços tecnológicos, transformando o mundo, com modelo de negócios flexíveis, democráticos e realmente próximos das necessidades de seus clientes, apresentando serviços acessíveis (por *smartphones*), descomplicados, menos burocráticos e baratos, por meio de plataformas eletrônicas (100% *online*), priorizando a agilidade e a simplicidade das operações, ótima ferramenta para facilitar a vida financeira das pessoas em tempos de crise por corona vírus.

Entendido algumas noções básicas sobre a quarta revolução industrial, é o momento de compreender melhor o que são os dados, qual sua importância e relevância, conforme se discorrerá a seguir.

2.3 DADOS

Conforme já informado anteriormente, os dados fazem parte dos domínios fundamentais de estratégia. Cabe agora entender um pouco mais sobre eles de maneira simples, pois não se pretende abordar, tecnicamente, os elementos que compõem um banco de dados, o que demandaria um conhecimento especializado no assunto.

De início, cabe destacar, a diferença entre dados e informação para esclarecer algumas questões terminológicas.

Os dados são tratados para gerar informações, que, por sua vez, produzem conhecimento e, eventualmente, valor econômico. Consequentemente, as informações são extraídas a partir dos dados (inclusive de sua relação a uma pessoa) e não o inverso. Por isso, pode-se afirmar que os dados são a matéria-prima da informação. Por exemplo, um nome, um endereço de *e-mail* e um número

de telefone, são dados pessoais porque dizem respeito a uma pessoa natural. O conhecimento de que todos esses dados pertencem a uma mesma pessoa é uma informação. Ainda, o conhecimento de que o nome e o endereço de *e-mail* são de uma mesma pessoa, mas o número de telefone não, também é uma informação (diferente da informação anterior). Dessa forma, os dados podem ser compreendidos como elementos que, isoladamente, não possuem necessariamente um sentido compreensível, enquanto a informação consiste na ordenação dos dados para produzir e transmitir conhecimento.[92]

Assim, o "dado" apresenta conotação mais primitiva e fragmentada, semelhante a uma informação em estado potencial, antes de ser transmitida ou associado a uma espécie de "pré-informação", que antecederia a sua interpretação e elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição. Sem aludir ao seu significado ou conteúdo em si, na informação já se pressupõe uma fase inicial de depuração de seu conteúdo – daí que a informação é um termo que carrega também um sentido instrumental, no sentido da redução de um estado de incerteza. A doutrina, por vezes, trata estes dois termos – dado e informação – indistintamente, ou então, procede a uma diferenciação algo empírica que merece ao menos ser ressaltada. Por certo, o conteúdo de ambos se sobrepõe em várias circunstâncias, o que acarreta uma inadequação na utilização de um termo por outro. Ambos servem a representar um fato, um determinado aspecto de uma realidade. Não obstante, cada um carrega um peso particular.[93]

Ainda, é claro, os dados "treinam" o programa para reconhecer padrões, fornecendo muitos exemplos, e o poder computacional permite que o programa analise esses exemplos em alta velocidade.[94] Por definição, um computador não processa informações, mas sim, dados.

---

[92] CARDOSO, Oscar Valente. A Lei Geral de Proteção de Dados protege dados ou informações? **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 25, n. 6280, 10 set. 2020. Disponível em: < https://jus.com.br/artigos/85291/a-lei-geral-de-protecao-de-dados-protege-dados-ou-informacoes>. Acesso em: 15 out. 2020.

[93] BRASIL. Escola Nacional de Defesa do Consumidor. A proteção de dados pessoais nas relações de consumo: para além da informação creditícia. vol.2, elaboração Danilo Doneda. – Brasília: SDE/DPDC, 2010. Disponível em: < https://legado.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf>. Acesso em: 29 ago. 2020.

[94] LEE, Kai-Fu. **Inteligência artificial: como os robôs estão mudando o mundo, a forma como amamos, nos relacionamos, trabalhamos e vivemos.** Tradução: Marcelo Barbão. 1º ed. Rio de janeiro: Globo Livros, 2019. p.18.

Por isso, a informação avoca um papel central e adjetivante da sociedade: sociedade da informação.[95] A informação é o (novo) estruturante que (re)organiza a sociedade, tal como o fizeram a terra, as máquinas a vapor e a eletricidade, bem como os serviços, respectivamente, nas sociedade agrícola, industrial e pós-industrial.[96]

Segundo Patrícia Peck Pinheiro, “informação é um ativo composto por um conjunto de dados ou elementos que, como qualquer outro ativo importante para os negócios, tem valor para a organização e, consequentemente, necessita ser adequadamente protegido”.[97]

Geralmente, chegar à tomada de decisão apenas nos dados brutos, sem uma análise, sem uma interpretação inteligente de sua potencialidade como informação e conhecimento é potencializar as falhas,[98] já que o dado “bruto” não possui valor, mas ao ser “refinado” passa a ser altamente rentável.[99]

Também cabe destacar a conceituação de informação dada pela Lei de Acesso à Informação (LAI), em seu artigo 4º, inciso I: “Informação são dados, processados, ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato”.[100]

Embora, haja diferentes definições podemos concluir que dado é uma estrutura elementar da cadeia informacional, que será transformada em informação no patamar seguinte e que informação é a semântica e contextualização dos dados para a geração de fatos.[101]

---

[95] Sociedade de informação é caracterizada pela capacidade de armazenar, processar e transmitir informações em quantidades outrora inimagináveis, onde a informação se tornou base de diversos negócios, de modo que passa a ter valor monetário e mercado e simultaneamente torna-se objeto de atos e negócios jurídicos.

[96] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. Rio de janeiro: Forense, 2020, p.05.

[97] PINHEIRO, Patrícia Peck. **Direito Digital**. 5 ed. São Paulo: Editora Saraiva, 2013.Livro eletrônico, não paginado.

[98] Cadernos Adenauer 2019. **Proteção de dados pessoais:** privacidade versus avanço tecnológico. ano 20. n. 3. Rio de Janeiro: Fundação Konrad Adenauer, 2019. Disponível em: < https://www.kas.de/documents/265553/265602/Caderno+Adenauer+3+Schutz+von+pers%C3%B6nlichen+Daten.pdf/476709fc-b7dc-8430-12f1-ba21564cde06?version=1.0&t=1571685012573>. Acesso em: 09 set. 2020.

[99] TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei geral de proteção de dados pessoais:** comentado artigo por artigo. 2.ed. ver., atual e ampl. Salvador: Editora JusPodivm, 2020, p.29.

[100] CÂMARA DOS DEPUTADOS. Legislação sobre acesso à informação, proteção de dados pessoais e internet. [recurso eletrônico] Claudio nazareno, Guilherme Pereira Pinheiro (organizadores). n.22, 1.ed. Brasília: Câmara dos Deputados, Edição Câmara, 2020, p.27.

[101] BARBIERI, Carlos. **Governança de dados:** práticas, conceitos e novos caminhos. Rio de Janeiro: Alta Books, 2019, p.15-16.

Entendido, a diferença entre dados e informação, é momento de compreender melhor os dados, sua importância e relevância, conforme se discorrerá a seguir.

Antes de seguir, porém, faz-se necessário apresentar a taxonomia de dados, bem como as suas origens:

> 1. Dados Fornecidos: se originam de ações diretas tomadas por seus titulares, nas quais ele ou ela encontra-se plenamente ciente das ações que levaram à coleta dos dados. Consideram-se dados fornecidos os registros, aplicativos de pesquisas (*e.g*. demográficas, eleitorais) e quaisquer outros nos quais o indivíduo forneça dados em plena consciência de suas ações.
> 2. Dados Observados: são simplesmente aqueles observados e arquivados. O surgimento da Internet como um meio de consumo interativo tornou possível observar e processar dados de uma forma mais robusta. Na Internet, pode-se observar de onde o indivíduo veio, o que ele busca, o quão frequentemente ele realiza buscar por conteúdo, e até mesmo a duração das pausas em tais buscas. O reconhecimento facial e a Internet das Coisas possibilitam que a observação digital seja possível no mundo real.
> 3. Dados Derivados: são dados que são simplesmente derivados, de forma bastante mecânica, de outros dados e tornam-se um novo conjunto de dados relacionados ao indivíduo. Por exemplo, técnicas de *marketing* dirigido produzem dados derivados.
> 4. Dados Inferidos: são produtos de um processo analítico baseado em probabilidade (análise preditiva). São exemplos de dados inferidos, a capacidade de crédito e a identidade, assim como muitas das inferências que surgem da análise de *Big Data*.
>
> **Atenção:** entre as origens de 1 a 4, há uma gradação quanto ao nível de consciência e controle do titular dos dados a respeito da natureza dos dados coletados ou produzidos, bem como das finalidades de utilização. Essa gradação varia, do maior nível de consciência no grau 1 (dados fornecidos) ao menor, no grau 4 (dados inferidos). A ideia é que, quanto o maior o grau de consciência, mais significativo o consentimento e o controle do titular dos dados pessoais sobre a privacidade. Assim, quanto mais perto do grau 4, menor a importância do consentimento, e maior a necessidade de responsabilização do titular dos dados (responsabilidade demonstrável).[102]

Pois bem, com a necessidade crescente da busca de soluções otimizadas e facilidades operacionais, as instituições incorporam-se de dados e tecnologias gerados em prol da transformação digital, posicionando-se, mesmo que de forma embrionária, na quarta revolução industrial – convergência das tecnologias dos mundos digitais, físicos e biológicos, onde os dados são elementos fundamentais de sua consolidação – o que representa um desafio vital para a sociedade, sendo que, mais do que os aspectos tecnológicos que a singulariza, é um processo que depende de uma eficiente compreensão pelas pessoas. Trata de uma onda de transformação surfada no barateamento, miniaturização e aumento da capacidade de produção de dados, onde pessoas, dados e tecnologias se complementam em

---

[102] CARVALHO, André Castro; ALVIM, Tiago Cripa et al. **Manual de *Compliance.*** Rio de janeiro: Forense, 2019, p. 511-512. ISBN 978-85-309-8315-4.

suas ações e finalidades, sendo os dados transformados em inteligência competitiva aplicada em diferentes segmentos.

Nessa linha de pensamento, podemos dizer que várias tecnologias produzem, acessam e coletam dados com facilidade o que seria inimaginável poucas décadas atrás. Para se ter uma ideia, estima-se que por dia os seres humanos produzem 2,5 quintilhões de bytes de dados (o que significa 2,5 seguidos de dezoito zeros). Neste contexto, a ideia de que "dados são o novo petróleo" ("*Data is the new oil*"), permite discutirmos transformações na produção e disseminação desses dados e como poderíamos tentar desenhar mecanismos para distribuí-los e preservá-los quando for o caso, de modo mais democrático.[103]

Por isso, é fundamental entender que, nesta nova realidade, o papel dos dados para negócios, hoje, está mudando drasticamente. Muitas instituições que, durante anos, usaram dados como parte específica de suas operações estão agora descobrindo uma revolução dos dados: os dados estão sendo fornecidos por novas fontes, estão sendo aplicados a novos problemas e estão se tornando importante vetor de inovações. E para que esses dados se transformem em autênticas fontes de valor, é preciso que as instituições mudem a maneira como pensam em dados, ou seja, tratando-os como ativo estratégico intangível.[104] De igual modo, as inovações tecnológicas abrem um grande potencial de produção e acesso a dados.

Em linhas gerais, os dados estão sendo minados para novos *insisghts* e otimizações de maneira que eram impossíveis até poucos anos. Para cada conjunto de dados adicional que se torna disponível, há dezenas de maneiras em que esse conjunto pode ser usado para gerar um sinal de negociação.[105]

Há também que se falar, segundo Gartner, mais de 40% das tarefas de ciência de dados serão automatizadas, resultando em maior produtividade e uso mais amplo por cientistas de dados cidadãos. Ou seja, entre cientistas de dados de cidadãos e análises aumentadas, as percepções de dados estarão mais

---

[103] CÓRDOVA, Yasodara; PROL, Flávio Marques. **Repensando a distribuição democrática de dados.** Disponível em: < https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/artigos/repensando-a-distribuicao-democratica-de-dados-10032017>. Acesso em: 09 set. 2020.

[104] ROGERS, David L. **Transformação digital:** repensando o seu negócio para a era digital. Tradução: Afonso Celso da Cunha Serra. 1º ed. São Paulo: Autêntica Business, 2019. p.121-125.

[105] CHISHTI, Susanne; BARBERIS, Janos. **A Revolução *Fintech*:** o manual das *startups* financeiras. Tradução: Samantha Batista. Rio de janeiro: Alta Books, 2017, p.161.

amplamente disponíveis em todas as instituições, incluindo analistas, tomadores de decisão e trabalhadores operacionais.[106]

Outro ponto, interessante, é que na sociedade da informação, o tratamento de dados pessoais é inevitável não apenas da área de tecnologia da informação, mas de todos os setores, e é inegável que esses dados representam ativos extremamente relevantes, inclusive em uma perspectiva econômica. Cabe, portanto, aos administradores e demais agentes envolvidos nas companhias, independentemente da indústria em que atuam, prezar pelo tratamento adequado desses dados, de acordo com as normas sobre proteção de dados pessoais que vêm se desenvolvendo, tendo em vista a geração e manutenção do valor de suas instituições, em momentos de crise ou não.[107]

É neste contexto criador que todos os setores de atividade que compõem a economia estão a viver, e o setor financeiro, em geral, e em particular os bancos digitais, não são exceção. A questão é: será que a análise de dados não será uma vantagem competitiva, mas sim uma desvantagem competitiva para aqueles que não a adotem? E o mais importante, como as empresas do setor financeiro podem assegurar a privacidade dos dados dos clientes e reforçar a confiança no setor?[108]

Nesse ambiente altamente dinâmico o fato é que dados de usuários são constantemente coletados e comercializados. Seja por meio de geoposicionamento, troca de mensagens e, basicamente, qualquer uso de aplicativos e programas de computadores, *tablets* ou *smartphones*. Hoje é sabido que qualquer informação pode ser vendida e monetizada. A verdade é que a fonte de receita de diversas companhias (como *Google, Facebook* etc.) vem dos dados de usuários. A sorte é que as coisas estão mudando e, futuramente, você mesmo poderá vender essas informações. Ou, pelo menos, receber uma comissão por elas: a verba destinada para a compra de dados poderá ser dividida entre a instituição e o indivíduo que gerou a informação. Ponto muito discutido atualmente e que levou à criação de leis como o Regulamento Geral de Proteção de Dados – *General Data Protection*

---

[106] GARTNER. **Insight Report 10 Strategic Technology Trends for 2019.** Disponível em: < https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2019/>. Acesso em: 09 set. 2020.

[107]CIRILLO, Maria Eugenia. **Monetizando dados pessoais.** Disponível em: < https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/regulacao-e-novas-tecnologias/monetizando-dados-pessoais-06062020>. Acesso em: 09 set. 2020

[108] CHISHTI, Susanne; BARBERIS, Janos. **A Revolução *Fintech*:** o manual das *startups* financeiras. Tradução: Samantha Batista. Rio de janeiro: Alta Books, 2017, p.228.

Regulation (GDPR) –, na União Europeia, e a Lei Geral de Proteção de Dados Pessoais (LGPD), no Brasil.[109]

Nota-se, portanto, que cada vez mais, os dados dos cidadãos, dispersos na rede, dizem mais sobre eles e quem os manipula sabe até mais sobre eles mesmos. Assim, essa capacidade de identificar os mais diversos padrões de comportamentos e prever a sua recorrência no futuro é uma verdadeira "mina de ouro".[110] Por certo, a oportunidade de se inovar com os dados, buscando novas formas de exploração, torna-se absolutamente necessária dentro do novo conceito de monetização dos dados, que os leva a um patamar de maior importância do que um simples combustível de processos. Ou seja, é preciso ampliar a forma de uso desses recursos, a fim de torná-los ainda mais valiosos e encaixá-los como um ativo significativo das instituições.[111]

Por esse motivo, Augustin Rubini explica que: "a monetização de dados também se tornará uma área lucrativa para os bancos, que têm uma infinidade de informações de clientes, e que as novas tecnologias permitirão encontrar o equilíbrio certo entre informações valiosas e anonimato."[112]

A título de exemplo, os melhores monetizadores de dados do mundo, como Facebook, Google e Twitter, poderiam naturalmente prometer pagar para você, o portador dos dados, em alguma forma de crédito financeiro. Ou eles ainda vão um passo além? A nova promessa ao portador poderia ser realmente: "se você confiar em mim para manter seus dados seguros, eu otimizarei seu valor ajudando-o a monetizá-lo". Ainda, é claro, serviços financeiros gratuitos.[113]

De igual modo, o que se vê no mercado é que as empresas de serviços financeiros sabem muito sobre seus clientes. Porém, quando se trata de monetizar este conhecimento – ou, mais precisamente, estes dados – as empresas de tecnologia estão na liderança. O motivo? Elas vão além das bases de dados estáticas e combinam informações diversificadas e valiosas de múltiplas fontes e

---

[109] PELLINI, Rudá. **O futuro do dinheiro: banco digital, *fintechs, criptomoedas* e *blockchain*:** entenda de uma vez por todos esses conceitos e saiba como a tecnologia dará liberdade e segurança para você gerar riqueza. São Paulo: Editora Gente, 2019, p.81-100.

[110] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. Rio de janeiro: Forense, 2020, p.38.

[111] BARBIERI, Carlos. **Governança de dados:** práticas, conceitos e novos caminhos. Rio de Janeiro: Alta Books, 2019, p.13.

[112] RUBINI, Agustin. **A Fintech em um Flash**. Tradução: Fernanda Belokurows. Babelcube Inc., 2017. Livro eletrônico, não paginado.

[113] CHISHTI, Susanne; BARBERIS, Janos. **A Revolução *Fintech*:** o manual das *startups* financeiras. Tradução: Samantha Batista. Rio de janeiro: Alta Books, 2017, p.32.

utilizam-nas em tempo real. O potencial desta abordagem também se aplica à indústria de serviços financeiros, em especial os bancos digitais. Em um contexto em que os dados são cada vez mais importantes, as empresas começam a coletá-los em fluxos contínuos em detrimento de retratos de momentos específicos – como dados de localização de clientes coletados por telefones celulares ao invés de transações com cartões. As empresas também procuram expandir suas bases de dados de clientes. Uma maneira é fazer com que a experiência digital seja mais envolvente, com mais dados coletados durante o processo. Outra possibilidade é firmar parcerias com outras empresas, oferecendo aos clientes um valor adicional em troca de suas informações. Em síntese, as empresas de serviços financeiros utilizam uma combinação de estratégias para alcançar o mesmo nível das empresas de tecnologia e se diferenciar. No entanto, a propriedade e o controle dos dados são uma questão chave,[114] para entender melhor os pontos fracos e as necessidades não atendidas do consumidor.

Dessa forma, é importante destacar que, a revolução dos dados chegou ao mundo financeiro, com dados de confiança, quantificáveis e melhor de tudo, monetizáveis, através de uma tecnologia inovadora, oferecendo APIs (*Application Programming Inferfaces* ou Interface de programação de Aplicações)[115] bem estruturados e seguros para abrir seus dados e serviços para os desenvolvedores inovadores. APIs de dados têm o potencial de permitir que as empresas de tecnologia, bancos e seus clientes se beneficiem de um ecossistema cada vez mais valioso de soluções inovadoras que gerarão novos fluxos de receita, mas, mais importante ainda, permite que a indústria financeira lidere a disrupção iminente de seu setor. Em outras palavras, estão proporcionando conveniência, velocidade e volume em quantidades que nunca vimos antes, tornando as transações financeiras mais fáceis, baratas e convenientes. Um bom exemplo disso está nas *Fintechs* que

---

[114] DELOITTE. **Além da *fintech*:** oito forças que mudam o cenário competitivo. Disponível em: < https://www2.deloitte.com/content/dam/Deloitte/br/Documents/financial-services/Al%C3%A9m%20das%20Fintechs%20-%20Oito%20For%C3%A7as%20que%20Mudam%20o%20Cen%C3%A1rio%20Competitivo.pdf>. Acesso em: 09 set. 2020.

[115] APIs é o termo usado para descrever um conjunto de ferramentas que permitem que diferentes componentes de software ou sistemas se comuniquem eficazmente uns com os outros, em uma linguagem muito simples, são interfaces de programação de aplicativos, que fazem com que um sistema converse com o outro e podem ser entendidas como programas ou sistemas que funcionam como uma ponte que conecta aplicações, sendo também utilizadas para os mais variados tipos de negócios. Proporcionam a integração entre sistemas que possuem linguagem totalmente distinta de maneira ágil e segura.

estão, de fato, remodelando a indústria de serviços financeiros, o que amanhã parecerá, sem dúvida, muito diferente do que é hoje.[116]

Em paralelo, não seria nenhum exagero afirmar que, a Tecnologia da Informação alterou definitivamente a forma como vivemos, trabalhamos e nos comunicamos. Inúmeras são as inovações que permitem a geração, a troca, o armazenamento e o cruzamento de imensos volumes de dados para criação de perfis pessoais. Novos modelos de negócio passam a ser explorados, tendo como bem mais valioso a informação. Embora esse avanço tecnológico tenha por finalidade a contribuição para o progresso econômico e social, não se pode esquecer que a privacidade de cada indivíduo deve ser respeitada e, para tanto, limites devem ser impostos, a fim de prevenir abusos e garantir o equilíbrio nessa relação. Ou seja, um programa de *compliance* bem constituído – apoiado em mecanismos de controle interno, eficazes e alinhado com as melhores práticas de governança corporativa – pode trazer uma série de benefícios.[117]

Para entender a abrangência do *compliance* é necessário tecer alguns comentários sobre sua origem. No século XX, com o surgimento das grandes corporações e da modalidade de investimento nas empresas de capital aberto criou-se um cenário para a conhecida crise de 1929. Entre outras razões a crise se originou pela utilização inadequada dos meios existentes para investimento e pela falta de confiança no sistema financeiro, no mercado e nas empresas. Essa crise foi um marco importante não só para o *compliance* e o combate a corrupção, mas para o progresso de princípios fundamentais da atividade empresária como transparência e o controle financeiro.

Antes de seguir, porém, faz-se necessário apresentar a definição de *compliance*:

> *Compliance* é um termo incorporado ao nosso idioma que significa, na melhor das traduções, conformidade. Diz-se conformidade, no sentido da conformação (ação de tomar uma forma), da observância (cumprimento) e da adequação a leis, normas e preceitos éticos. Essa conformidade não se atinge tão simplesmente pela observância de leis. Se dá, também, por meio da adoção de um conjunto de disciplinas e estratégias voltadas a que se faça cumprir as normas legais e regulamentares que se sujeita uma organização. Ainda se atinge a conformidade por meio do estabelecimento

---

[116] CHISHTI, Susanne; BARBERIS, Janos. **A Revolução *Fintech*:** o manual das *startups* financeiras. Tradução: Samantha Batista. Rio de janeiro: Alta Books, 2017, p.226-234.

[117] JIMENE, Camilla do Vale; VAINZO, Rony. **Cinco pontos fundamentais de *compliance* digital para o seu programa de *compliance*.** Disponível em: < https://d335luupugsy2.cloudfront.net/cms/files/28354/1521065508Compliance_Digital.pdf>. Acesso em: 09 set. 2020.

> e cumprimento, *motu próprio,* de políticas e diretrizes de natureza procedimental e ética estabelecidas pela organização. É evidente que o papel do *compliance*, ou de programas de *compliance*, como ferramenta de regulação em proteção de dados, é o que há de mais atual, significativo e transformador nas discussões acerca de políticas públicas em matéria de privacidade e proteção de dados pressionada pelas rápidas transformações sociais e tecnológicas. Portanto, conformidade ou *compliance* é a adoção de um conjunto de disciplinas e estratégias voltadas a que se faça cumprir as normas (proteção de dados, por exemplo) a que se sujeita uma organização de negócios, bem como do estabelecimento e cumprimento, *motu próprio,* de políticas e diretrizes de natureza procedimental e ética estabelecidas pela própria organização. Tudo isso devidamente monitorado pelo órgão regulador.[118]

Acrescenta-se, também, a definição de Éderson Garin Porto sobre o *compliance*:

> A expressão "*compliance*" tem origem na língua inglesa, a partir do verbo *"to comply"* que expressa a ideia de cumprir, satisfazer, executar. A ideia central é, portanto, cumprir ou satisfazer as determinações jurídicas impostas pelo ordenamento, assim como as normas internas daquela organização. O objetivo do *compliance* é assegurar que a corporação esteja aderente às normas vigentes, fazendo com que riscos sejam afastados ou mitigados. Acredita-se que uma empresa comprometida com a cultura do *compliance* estará menos exposta a riscos e assim terá um ambiente corporativo impróprio para o surgimento de condutas irregulares ou ilícitas.[119]

No entendimento de Assi[120], *compliance* é a ferramenta de governança corporativa[121], no que se refere a sistemas, processos, regras e procedimentos adotados para gerenciar os negócios da instituição, proporcionando o aprimoramento da relação com os investidores. Logo, estar em *compliance* é estar em conformidade com leis e regulamentos internos e externos, e é, acima de tudo, uma obrigação de cada colaborador dentro da instituição.

Neste caso, as definições de *compliance* encontradas fazem menção a um sistema, um conjunto de medidas tomadas com o intuito de fazer a empresa operar em conformidade com as normas internas, destinadas à conduta de seus integrantes, procedimentos internos de eficiência etc., e externas, como obediência

---

[118] CARVALHO, André Castro; ALVIM, Tiago Cripa et al. **Manual de *Compliance.*** Rio de janeiro: Forense, 2019, p. 495-512. ISBN 978-85-309-8315-4.

[119] PORTO, Éderson Garin. ***Compliance* & Governança Corporativa:** uma abordagem prática e objetiva. Porto Alegre: Lawboratory, 2020, p.33.

[120]ASSI, Marcos. **Gestão de Compliance e Seus Desafios**: como implementar controles internos, superar dificuldades e manter a eficiência dos negócios. São Paulo: Saint Paul Editora, 2013, p. 19.

[121]Governança corporativa é o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessas. As boas práticas de governança corporativa convertem princípios básicos em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor econômico de longo prazo da organização, facilitando seu acesso a recursos e contribuindo para a qualidade da gestão da organização, sua longevidade e o bem comum.

às leis, requisitos técnicos para o funcionamento, conformidade com a Organização Internacional de Normatização (ISO) etc.[122]

Como se vê, com o surgimento de grandes mudanças, emergem grandes responsabilidades, pois para que um programa de *compliance* de proteção de dados seja efetivo, antes de aderir a novas tecnologias, as instituições devem obedecer, primordialmente, as normas de conformidade e as leis que as regulam. O objetivo é proteger a privacidade dos titulares dos dados e impedir que instituições abusem da informação. Também, parte relevante é o *compliance* digital, principalmente quando o assunto em questão for a proteção de dados pessoais e privacidade, sobretudo, para estabelecer e manter a confiança dos clientes de bancos digitais.

Por certo, são algumas as razões para isso: (i) há urgência em adotar programas de *compliance*, a partir da sanção da nossa Lei Geral de Proteção de dados (LGPD), a qual passou a vigorar em 18/09/2020; (ii) independentemente da LGPD, o tema envolve riscos reputacionais importantes, na medida em que o tratamento de dados pessoais potencialmente afeta diretamente a vida de clientes e, indiretamente, os negócios de parceiros; (iii) os riscos regulatórios atuais, inclusive de multas, são significativos, e o serão ainda mais no futuro; (iv) a matéria é crucial para o desenvolvimento de negócios baseados no processamento e fluxo de dados pessoais (economia baseada em dados); e (v) o conteúdo comportamental ético do tema é relevantíssimo e, por isso mesmo, a implementação completa de programa efetivo leva tempo.[123]

Por essa razão, é interessante observar que o investimento na prevenção, *compliance* e na segurança do serviço que uma *fintech* presta, traz a ela, além do viés preventivo de proteção contra o risco inerente ao negócio, mais credibilidade, confiabilidade perante os clientes e quaisquer terceiros, contribuindo, assim, não apenas para a liquidez e robustez do sistema financeiro com um todo, bem como um incremento efetivo nos resultados e na valorização da própria *fintech*.[124]

Conforme demonstrado, pode-se concluir que os dados estão permeando o mundo físico e digital, dentro de um verdadeiro ecossistema que abrange desde a sua produção até o seu descarte, impactando diretamente no desenvolvimento da

---

[122] TEIXEIRA, Tarcisio; LOPES, Alan Moreira; TAKADA, Thalles. **Manual jurídico da inovação e das startups.** 2.ed. Salvador: Editora JusPodivm, 2020, p.247.
[123] CARVALHO, André Castro; ALVIM, Tiago Cripa et al. **Manual de *Compliance.*** Rio de janeiro: Forense, 2019, p. 497. ISBN 978-85-309-8315-4.
[124] EROLES, Pedro. ***Fintechs*, Bancos Digitais e Meios de Pagamento:** aspectos regulatórios das novas tecnologias financeiras. São Paulo: Quartier Latin, 2019, p.243.

economia, da promoção e estabilidade social, espalhados em todo mundo, oferecendo oportunidades e ameaças. Novas tecnologias, processos e competências surgem e são necessárias para a aplicação consciente e transformadora dos dados. A sociedade está mais consciente do poder transformador da tecnologia e do valor e necessidade de segurança do uso dos dados, já que eles permitem a comunicação entre máquinas, ferramentas, sistemas e pessoas que estão interligadas para a produção e busca de bens e serviços que nortearão o desenvolvimento das próximas gerações. É importante lembrar que, para gerar valor, obter vantagem competitiva e se consolidar na quarta revolução industrial é fundamental a utilização de dados como ativos estratégicos, por meio de análises e recursos que permitam transformar os dados em informações e conhecimento, que identificam propósitos da sociedade, de forma ética, onde tais dados sejam considerados ativos cada vez mais valiosos.

2.4 NOVAS TECNOLOGIAS DIGITAIS

Esclarecido alguns pontos importantes e relevantes sobre os dados, cabe, agora, analisar, de maneira sucinta, as novas tecnologias digitais, fruto da Revolução 4.0. No entanto, será analisado, no presente trabalho, pontos relevantes a respeito do *Big Data, Blockchain*, Inteligência Artificial e Internet das Coisas; tecnologias que chegaram para ficar e que estão remodelando a proposta de valor dos produtos e serviços financeiros, a ponto de melhorar a tomada de decisão, o planejamento, o controle e a governança, na coleta e tratamento de dados. É o que se verá a seguir.

2.4.1 *Big Data*

Para iniciar o raciocínio, precisa-se, antes de mais nada, entender o significado do termo “*Big Data*” para assim compreender a sua importância e relevância.

Big Data tornou-se um termo popular para descrever o crescimento, a disponibilidade e o uso exponencial de informações, tanto estruturados quanto não estruturados. Muito já se escreveu a respeito da tendência *Big Data* e como ela pode servir como base para inovação, diferenciação e crescimento. Para superar os

desafios tecnológicos no gerenciamento do grande volume de dados provenientes de múltiplas fontes, às vezes em ritmo acelerado, novas tecnologias adicionais acabaram sendo desenvolvidas. O uso do termo *Big Data* está geralmente associado a tais tecnologias. Como uma das principais aplicações desses dados armazenados é a geração de *insights* por meio de análise de dados, às vezes o termo *Big Data* é ampliado como análise de *Big Data*. O *Big Data* é tipicamente definido por três Vs: volume, variedade e velocidade.[125]

Por essa razão, desde o início de 2010, o termo “Big Data “é usado para descrever uma nova geração de tecnologias e abordagens para gestão de dados. Essa tecnologia foi criada por grandes *players* da indústria *web* porque tecnologias tradicionais não eram capazes de adaptar-se a um número imprevisível de usuários, volumes de dados de crescimento rápido e necessidades crescentes de processamento de capacidades. À medida que a tecnologia *Big Data* evoluiu progressivamente no setor *web*, adaptou-se para suportar as exigências e os desafios únicos da indústria financeira.[126]

Além disso, a definição *Big Data* varia de acordo com a indústria, dependendo dos tipos de ferramentas de *software* utilizadas e do tamanho dos conjuntos de dados que precisam ser armazenados e analisados. Considera-se que o setor de serviços financeiros possui os maiores conjuntos de dados devido à natureza do setor, logo nesse setor, o *Big Data* pode ser referido em *petabytes* (1000 *terrabytes*).

Há também que se falar que “*Big Data*” são conjuntos de dados extremamente vastos, que podem ser analisados computacionalmente para revelar padrões, tendências e associações, especialmente aqueles relacionados ao comportamento e interações humanas.[127]

A partir dessa perspectiva, acrescenta-se a conceituação de Felipe Morais:

> *Big Data* é a análise e a interpretação de grandes volumes de dados de grande variedade. Para isso, são necessárias soluções especificas que permitam a profissionais de TI trabalhar com informações não estruturadas a uma grande velocidade. As ferramentas de *Big Data* são de grande importância na definição de estratégias. Com elas, é possível, por exemplo, aumentar a produtividade, reduzir custos e tomar decisões de negócios

---

[125] SHARDA, Ramesh; DELEN, Dursun; TURBAN, Efraim. ***Business intelligence* e análise de dados para gestão do negócio.** Tradução: Ronald Saraiva de Menezes. 4.ed. Porto Alegre: Bookman, 2019, p.439-440.

[126] CHISHTI, Susanne; BARBERIS, Janos. **A Revolução *Fintech*:** o manual das *startups* financeiras. Tradução: Samantha Batista. Rio de janeiro: Alta Books, 2017, p.100.

[127] EROLES, Pedro. ***Fintechs*, Bancos Digitais e Meios de Pagamento:** aspectos regulatórios das novas tecnologias financeiras. São Paulo: Quartier Latin, 2019, p.181.

> mais inteligentes. Em resumo, é uma ferramenta de competitividade estratégica muito importante para o futuro do negócio.[128]

Também cabe destacar a conceituação dada por Carlos Barbieri, consultor em governança e gestão de dados – CDMP:

> *Big Data* nada mais é do que a representação de um novo momento da sociedade, quando diversas mudanças de tecnologia acabaram por gerar uma profunda produção de dados, de variados tipos e com volumes e velocidades de dimensões diferentes. Assim, *Big Data*, muito mais do que tecnologias especificas, representa um novo estado das tecnologias existentes, algumas agora evoluídas e outras relativamente novas, tudo em função deste novo momento. Fenômenos como a internet, redes sociais, portabilidade, "*devices"* mais inteligentes (*smart devices*), suas respectivas produções de dados e novas formas de trata-los (como Inteligência Artificial com aprendizado de máquina) compuseram esse mosaico de fatores do que hoje é chamado simplificadamente de *Big Data*.[129]

Augustin Rubini, explica em sua obra que:

> *Big Data* refere-se a grandes conjuntos de dados que não podem ser armazenados e analisados por ferramentas regulares de *software* de bancos de dados. Embora não haja um tamanho predeterminado que torne um conjunto de dados qualificado como *Big Data*, o conjunto de dados deve ser suficientemente grande para que as ferramentas de aprendizado automático sejam as únicas que possam analisa-los. Normalmente, o *Big Data* excede um certo número de *terrabytes* e é armazenado em várias máquinas diferentes. No entanto, não é somente o volume de dados. Para entender o *Big Data* corretamente, também é importante entender o tipo de variedade, velocidade e a veracidade dos dados.[130]

Esse mesmo autor ainda relata em sua obra alguns pontos importantes a respeito do surgimento da Big Data:

> Em 1663, a introdução dos princípios contábeis por Graunt abriu o caminho para o uso do *Big Data* na era moderna. Em 1865, a *Devens* usou o termo "*business intelligence*" pela primeira vez para descrever como a coleta e análise de dados podem oferecer uma vantagem competitiva. Então, em 1880, Hollerith, um funcionário do US Census Bureau, gerou a Hollerith Tabulating Machine, que se tornaria o pai da computação automatizada. Em meados da década de 1950, Daveerport apresentou o *Analytics* 1.0, com análise descritiva e dados de relatórios em análise de dados estruturados. Em 1965, o governo dos EUA lançou um plano para o primeiro centro de dados federal, com o objetivo de armazenar 742 milhões de declarações de impostos e 175 milhões de impressões digitais em fita magnética. Na década de 1990, surgiram as primeiras menções de *Big Data*, sendo o primeiro um artigo escrito por Cox e Ellsworth para uma conferência sobre visualização. Em 2000, Lyman e Varian lançaram "Quanta informação", o primeiro estudo abrangente sobre quantificação de informação em termos de armazenamento informático. Hoje em dia, o termo *Analytics* 3.0 está sendo usado por organizações que aspiram integrar o *Analytics* 1.0

---

[128] MORAIS, Felipe. **Transformação digital.** São Paulo: Saraiva educação, 2020, p.114.
[129] BARBIERI, Carlos. **Governança de dados:** práticas, conceitos e novos caminhos. Rio de Janeiro: Alta Books, 2019, p.107-108.
[130] RUBINI, Agustin. **A Fintech em um Flash**. Tradução: Fernanda Belokurows. Babelcube Inc., 2017. Livro eletrônico, não paginado.

> (analítica tradicional) com o *Analytics* 2.0 (Big Data) para gerar impacto comercial mensurável.[131]

Ainda, assim, é importante mencionar que a tecnologia *Big Data* pode facilitar a implementação de sistemas de informação de risco e *compliance*, em um contexto financeiro, transformando restrições em oportunidades de negócios. Um único sistema *Big Data* pode fornecer uma solução transacional, de inteligência de negócios e de *compliance*, ou seja, tecnologia *Big Data* é a melhor tecnologia para implementar sistemas de *compliance*. Contudo, essa tecnologia não fornece consistência de dados em tempo real, o que é um problema. Além disso, *Big Data* padrão em tempo real também precisa ser melhorado, pois tem significados diferentes no mundo da *internet* e na indústria financeira. Resumindo, tecnologias *Big Data* resolvem dois grandes inconvenientes de tecnologias antigas: a falta de flexibilidade e de elasticidade e a escalabilidade, onde a *Big Data* é capaz de reduzir a complexidade de dados e detectar sinais fracos em enormes conjuntos de informações.[132]

Note-se ainda que aumenta a cada dia a quantidade de dados capturados nos processos que envolvem o sistema financeiro, seja sob a forma de transações financeiras por meios eletrônicos, solicitações de serviços, análises de comportamento, dados sobre histórico de consumo de produtos e serviços, entre outros. Assim, as grandes bases de dados digitais oferecem uma incrível oportunidade de examinar as tendências que vão mudar fundamentalmente a relação entre as instituições de serviços financeiros e seus clientes, ou como produtos e serviços na área financeira podem ou devem ser oferecidos.[133]

Diante disto, é inegável, que nos últimos anos, temos assistido mudanças muito significativas no setor de serviços financeiros por força de constantes transformações no domínio das tecnologias de informação. A vida nas sociedades atuais, principalmente nos países desenvolvidos, implica a produção massiva de dados, onde a informação é gerada, recolhida, armazenada, tratada e usada. É o *Big Data*, que vem sendo considerado o petróleo do século XXI.[134]

---

[131] RUBINI, Agustin. **A Fintech em um Flash**. Tradução: Fernanda Belokurows. Babelcube Inc., 2017. Livro eletrônico, não paginado.
[132] CHISHTI, Susanne; BARBERIS, Janos. **A Revolução *Fintech*:** o manual das *startups* financeiras. Tradução: Samantha Batista. Rio de janeiro: Alta Books, 2017, p.100-102.
[133] PALHARES, Felipe. et al. **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020, p.130.
[134] CORDEIRO, António Menezes; DE OLIVEIRA, Ana Perestrelo; DUARTE, Diogo Pereira. ***Fintech*:** desafios da tecnologia financeira. 2º ed. Almedina, 2019, p.19-20.

Nesta mesma direção, é importante mencionar que no âmbito do mercado financeiro, esta realidade tem assumido grande importância, principalmente quanto a proteção de dados pessoais dos clientes, que tem sido apontada como um dos desafios associados à introdução de novas tecnologias na área financeira, a prestação de serviços financeiros através de canais digitais e a participação de novas entidades (*Fintechs*). Com efeito, muitos dos *incomers* baseiam a sua atividade no *profiling* com recursos ao *Big Data* como forma de oferecer produtos e serviços financeiros "*tailor made*" e "*customer centric*", ou seja, adequados as preferências e necessidades dos clientes.[135] A indústria de *software* financeiro está mudando rapidamente, com vários recém-chegados que são capazes de entregar serviços financeiros e de *Big Data* ao mesmo tempo.[136]

Por isso, o catalizador das mudanças que hoje testemunhamos não é mais o motor a vapor, ou o tear mecânico, mas a combinação de tecnologia digital, *Big Data* e o conceito de '*mobile'*.[137]

É importante destacar que a era *Big Data*, porém, tem sido marcada pela profusão de novos tipos de dados não estruturados – informações que são registradas, mas não se encaixam com facilidade em fileiras e colunas bem organizadas. Embora a ascensão do *Big Data* esteja influenciando todos os setores de atividade, inclusive o financeiro, ainda restam alguns mitos e equívocos sobre essa tecnologia: (1) O algoritmo resolve tudo: o mito do algoritmo mágico; (2) Correlação é tudo o que importa: a identificação de um padrão não (nem sempre) é suficiente; (3) Todos os "*good data*" são "*Big Data*": seria um equívoco confundir *Big Data* com estratégia de dados.[138]

Como se pode perceber, empresas de serviços financeiros estão entre os exemplos primordiais em que a análise de fluxo de *Big Data* pode oferecer decisões melhores e mais rápidas, vantagem competitiva e supervisão regulatória. A capacidade de analisar um fluxo de dados acelerado e de alto volume sobre

---

[135] CORDEIRO, António Menezes; DE OLIVEIRA, Ana Perestrelo; DUARTE, Diogo Pereira. ***Fintech*:** desafios da tecnologia financeira. 2º ed. Almedina, 2019, p.26.

[136] CHISHTI, Susanne; BARBERIS, Janos. **A Revolução *Fintech*:** o manual das *startups* financeiras. Tradução: Samantha Batista. Rio de janeiro: Alta Books, 2017, p.105.

[137] CALICCHIO, Nicola; DIAS, Yran. O futuro do futuro. **McKinsey&Company.** Disponível em: < https://www.mckinsey.com/br/our-insights/blog-made-in-brazil/o-futuro-do-futuro>. Acesso em: 09 set. 2020.

[138] ROGERS, David L. **Transformação digital:** repensando o seu negócio para a era digital. Tradução: Afonso Celso da Cunha Serra. 1º ed. São Paulo: Autêntica Business, 2019. p.132-139.

transações financeiras a uma baixíssima latência ao longo de diferentes mercados e países oferece uma tremenda vantagem para a tomada de decisões de compra/venda em questão de segundos e que podem se traduzir em enormes ganhos monetários. Além da otimização de decisões de compra/venda, a análise de fluxos também pode ajudar empresas de serviços financeiros no monitoramento de transações em tempo real para a detecção de fraudes e outras atividades ilegais.[139] Contudo, um desafio fundamental para as empresas de serviços financeiros está ganhando uma visão de 360 graus dos seus clientes (informações valiosas sobre o cliente) através de um amplo uso de *Big Data*. Neste contexto, é necessária uma cultura baseada em dados.[140]

2.4.2 *Blockchain*

Preliminarmente tem-se que entender os pontos chaves dessa tecnologia, é o momento de compreender melhor, sua conceituação e características, conforme se discorrerá a seguir.

O *blockchain*, nada mais é do que um livro razão – protocolo de confiança, isto é, um sistema informatizado e descentralizado (espaço de dados na rede), em que seus usuários podem "trocar" informações em tempo real no sistema computacional (rede *peer-to-peer*[141], ocasião em que todos possuem cópia dos históricos de transações), seguro e de transparência aos seus integrantes, sem participação Estatal, de órgãos reguladores ou intermediários.[142]

Segundo Gartner:

> *Blockchain* é um tipo de livro-razão distribuído, uma lista em expansão ordenada cronologicamente de registros transacionais irrevogáveis e assinados criptograficamente, compartilhada por todos os participantes em uma rede. O *Blockchain* permite que as empresas rastreiem uma transação e trabalhem com partes não confiáveis sem a necessidade de uma parte centralizada (ou seja, um banco). Isso reduz muito o atrito comercial e tem

---

[139] SHARDA, Ramesh; DELEN, Dursun; TURBAN, Efraim. ***Business intelligence* e análise de dados para gestão do negócio.** Tradução: Ronald Saraiva de Menezes. 4.ed. Porto Alegre: Bookman, 2019, p.487.

[140] RUBINI, Agustin. **A Fintech em um Flash**. Tradução: Fernanda Belokurows. Babelcube Inc., 2017. Livro eletrônico, não paginado.

[141] *Peer-to-peer* é a arquitetura de rede em que cada computador tem funcionalidades e responsabilidades equivalentes. Difere da arquitetura cliente/servidor, em que alguns dispositivos são dedicados a servir outros. Esse tipo de rede é normalmente implementado via *softwares* P2P, que permitem conectar o computador de um usuário ao de outro para compartilhar ou transferir dados, como MP3, jogos, vídeos, imagens etc.

[142] EROLES, Pedro. ***Fintechs*, Bancos Digitais e Meios de Pagamento:** aspectos regulatórios das novas tecnologias financeiras. São Paulo: Quartier Latin, 2019, p.49.

> aplicativos que começaram nas finanças, mas se expandiram para governo, saúde, manufatura, cadeia de suprimentos e outros. O *Blockchain* pode reduzir custos, reduzir os tempos de liquidação de transações e melhorar o fluxo de caixa. Essa tecnologia criará $ 3,1T em valor de negócios até 2030.[143]

Também cabe destacar a definição de *blockchain* dada por Felipe Morais:

> O *blockchain* é uma rede que funciona com blocos encadeados muito seguros que sempre carregam um conteúdo junto a uma impressão digital. Cada bloco de dado contém uma espécie de assinatura digital, chamada *hash,* que, basicamente, funciona como uma impressão biométrica. Em suma, o *hash* é a garantia criptográfica de que informações desse bloco de dados não serão violadas. Logo, o blockchain é considerada uma camada de segurança encriptada da rede, por onde documentos e transações são validadas de forma a evitar fraudes, *hacking* e ilicitudes de várias naturezas. É a malha global de uma nova verdade digital certificada.[144]

Augustin Rubini, explica em sua obra que:

> A tecnologia *blockchain* promete ser usada de várias formas em nossas vidas diárias, por exemplo, na criação de contratos inteligentes, na melhoria dos pagamentos, na manutenção dos registros médicos e na digitalização de nossas identidades. Além disso, essa tecnologia pode fornecer uniformidade e segurança no compartilhamento de dados. É o modelo de banco de dados mais seguro, sobre o qual as transações financeiras no mundo digital podem ser construídas através de um sistema descentralizado, no qual existem muitos computadores interdependentes envolvidos no gerenciamento dos dados. Os sistemas *blockchain* são tipicamente compostos por dois componentes principais: uma rede *peer-to-peer* (rede composta por muitos computadores – nódulos) e um banco de dados (conjunto de transações históricas). O *blockchain* também pode ajudar com fraudes e prevenção de riscos.[145]

Em síntese, trata-se de um sistema baseado em um protocolo de rede que permite o registro de informações organizadas em blocos com base em criptografia[146] e assinaturas digitais[147], ordenadas cronologicamente, em forma de cadeia (daí a expressão "*blockchain*" ou "cadeia de blocos"). Seria uma espécie de livro diário ou livro-razão com registro de transações, mas com uma particularidade fundamental: enquanto em um sistema tradicional de contabilidade os registros são centralizados em uma ou um conjunto de pessoas, que são responsáveis por validar

---

[143] GARTNER. **Insight Report 10 Strategic Technology Trends for 2019.** Disponível em: < https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2019/>. Acesso em: 09 set. 2020.

[144] MORAIS, Felipe. **Transformação digital.** São Paulo: Saraiva educação, 2020, p.252.

[145] RUBINI, Agustin. **A Fintech em um Flash**. Tradução: Fernanda Belokurows. Babelcube Inc., 2017. Livro eletrônico, não paginado.

[146]Criptografia é um método de codificação de dados que permite o acesso apenas de pessoas autorizadas, possuidoras de chave de acesso. Ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas. É usada, entre outras finalidades, para autenticar a identidade de usuários e autenticar transações bancárias; proteger a integridade de transferências eletrônicas de fundos e proteger o sigilo de comunicações pessoais e comerciais.

[147]Assinatura digital é o código utilizado para verificar a integridade de um texto ou mensagem. Também pode ser utilizado para verificar se o remetente de uma mensagem é mesmo quem diz ser.

suas entradas e saídas e também por fazer a guarda dos próprios livros, no *blockchain* o registro das transações é público e descentralizado e compartilhado por todos que transacionam nos seus termos. Cada computador ou "nó de rede" conectado ao sistema mantém uma cópia desse livro-razão, que é validado e replicado em todos os nós (*nodes*) cada vez que um novo bloco é adicionado à cadeia. Assim, por ser uma tecnologia descentralizada, funciona em computadores fornecidos por voluntários (ou membros de um sistema fechado ou proprietário) em todo o mundo; então não existe um banco de dados central que possa ser copiado, roubado ou desligado. Desse modo, pode-se enviar informações ou bens diretamente e de forma segura entre os nós da cadeia sem a necessidade de validação por um terceiro confiável ou quaisquer outros intermediários.[148]

Ou seja: na rede descentralizada *blockchain*, a verificação, validação e implementação de operações depende do consenso de nós (por uma prova matemática de *proof of work*, feita de forma não identificada) que fazem parte da rede, de modo que o controle da rede não cabe a um único ente isolado (*trusted third party*). Os nós verificam e validam informações e, uma vez que uma operação e suas informações (chaves privadas e públicas de acordo, saldos e demais itens cabíveis) seja verificada, há um consenso que determina a validade da operação e que a mesma deve ser incluída no bloco de operações. Uma vez que seja parte do bloco minerado (processado) pela rede, não há, via de regra, como alterar ou eliminar a operação. Logo, um nó em si não tem poderes suficientes para efetuar uma operação. Consequentemente, não há um único nó, central, que pode ser responsabilizado pelas alterações feitas no livro-razão. Esse ponto, por mais que pareça uma questão meramente tecnológica, tem um impacto jurídico claro: não há, na rede, uma pessoa a ser responsabilizada. Não há a quem endereçar um pedido e, ainda que algum pedido fosse acatado, não há como se assegurar ou forçar o consenso, que é obtido por uma prova matemática.[149]

De acordo com Klaus Schwab, pode-se resumir, sinteticamente, da seguinte forma as principais características da tecnologia *blockchain*:

> - É uma forma de contabilidade digital e partilhada que torna possível compartilhar registros digitais e informações de forma segura e com a

[148] OIOLI, Erik Frederico. **Manual de direito para startups**.2. ed. ver., atual. e ampl. São Paulo: Thomson Reuters, 2020, 205.
[149] PALHARES, Felipe. et al. **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020, p.113-114.

> confiabilidade da não existência de várias cópias desses registros exclusivos, preservando assim o valor do objeto digital ou das informações.
> - É uma força descentralizadora, porque nenhuma autoridade central é responsável pela manutenção do sistema. Em vez disso, incentivos colaborativos exigem que as diversas partes ajam de boa-fé e tornem matematicamente improvável que o sistema seja *hackeado*.
> - É útil para criação de criptomoedas, identidades digitais, rastreamento de objetos físicos com o uso de criptografia e identificadores digitais e outras áreas em que a origem dos objetos físicos ou virtuais precisa ser autenticada. A possibilidade de verificação desses bens permite formas completamente novas de nos relacionarmos com os dados que criamos como usuários de dispositivos, serviços e aplicativos digitais.
> - Ajuda na distribuição de benefícios para aqueles que são tradicionalmente excluídos das recompensas econômicas, como os indivíduos e pequenos grupos que precisariam criar consórcios para conseguir participar de processos comerciais maiores.
> - Apresenta obstáculos relacionados a falta de normas, regulamentação de dados nacionais e transacionais. Por exemplo, as criptomoedas ainda estão em seus estágios iniciais e há externalidades não resolvidas, como seu impacto ambiental, sua utilização por organizações criminosas e a resolução de litígios em geral.[150]

É importante destacar, ainda, que o *blockchain* é uma das tecnologias revolucionárias da arquitetura social então vigente, motivando inovações jurídicas ao:

> (i) não ter um ente controlador (administrador) que possa ser responsabilizado nos termos mais tradicionais da lei, de forma que na plataforma, por sua estrutura horizontal, todos os usuários de uma mesma categoria são em geral operacionalmente iguais;
> (ii) não ter termos e condições de uso ou quaisquer documentos que expressem suas regras aos usuários, sendo que o uso de tecnologia se assemelha a uma adesão tácita aos usos e costumes da plataforma, ainda que o usuário possa ser incapaz ou hipossuficiente;
> (iii) ser pseudoanônimo *by design* e não permitir customizações ou interferências do usuário fora de contextos operacionais pré-determinados pela programação da plataforma, o que nos leva a refletir sobre os níveis de anonimato e privacidade; e
> (iv) impossibilitar direitos que só vieram recentemente à voga, como o direito de esquecimento (que, apesar de dificilmente exequível na internet, passa a ser impossível no *blockchain*).[151]

Pelo exposto, verifica-se que o foco principal desta tecnologia é fornecer relações transparentes e confiáveis entre os participantes numa rede, sem a necessidade de ter uma monitorização centralizada. Quanto ao setor financeiro, a sua implementação levou ao desenvolvimento de aplicações transformadoras no setor de serviços financeiros: a capacidade de processamento de transações em tempo real *blockchain* estão a acelerar a validação e finalização dessas transações, permitindo pagamentos instantâneos; a eliminação da necessidade de

---

[150] SCHWAB, Klaus; DAVIS, Nicholas. **Aplicando a quarta revolução industrial**. Tradução: Daniel Moreira Miranda. São Paulo: Edipro, 2018, p.145-146.
[151] PALHARES, Felipe. et al. **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020, p.123-124.

intermediários, criando uma rede descentralizada, que está a reduzir drasticamente os custos de transação. Trata-se, portanto, de uma tecnologia excitante que pode revelar-se uma inovação disruptiva, em tudo semelhante a outras tecnologias, como a máquina a vapor e a internet, que desencadearam revoluções industriais anteriores, e com o poder de alterar os modelos econômicos e empresariais existentes.[152]

Dessa forma, o *Blockchain* é visto como a próxima revolução em serviços financeiros no mundo, prometendo democratizar o sistema financeiro global, o que significa que todos com dispositivos móveis receberão acesso igual. À medida que a tecnologia evolui, as autoridades financeiras acabarão tremendo com o enorme impacto do *blockchain* em todas as facetas do cotidiano, tornando obsoletos as metodologias tradicionais de realização de transações, criando um sistema financeiro mais eficiente e flexível, onde, através do *blockchain*, a nossa capacidade como consumidor de fazer transações está sendo levado do mundo físico para o digital.

Pois bem, com tudo isso, percebe-se que a tecnologia *blockchain* mudará a natureza das transações financeiras, uma vez que leva a mudanças fundamentais na arquitetura financeira global. A gestão de dados financeiros atuais é impulsionada por bancos de dados[153] discretos dentro de empresas de serviços financeiros que se comunicam umas com as outras por meio de canais de comunicações seguros, e o futuro do processamento de transações financeiras será um mundo de uma ou várias bases de dados de ativos globais. Essas bases de dados armazenarão todos os dados financeiro dos participantes do mercado financeiro que optam por utilizar esses motores de transação mais baratos e mais fáceis de usar. Seguindo a lógica *blockchain,* essas bases de dados serão distribuídas ao redor do globo, e as transações, para serem executadas, exigirão a validação de todos ou, pelo menos, de uma maioria qualificada desses bancos de dados.[154]

Neste ponto é possível dizer que a tecnologia *blockchain* permite que duas partes que não se conhecem cheguem a um acordo (consenso) através de uma história digital comum. Essa história digital comum é importante porque os ativos e

---

[152] ALCARVA, Paulo. **Banca 4.0. Revolução Digital:** *fintechs, blockchain*, criptomoedas, *robo-advisers* e *crowdfunding*. Coimbra: Conjuntura Actual Editora, 2018, p.18-19.

[153] Banco de dados é o *arquivo* composto de registros, contendo cada um deles campos, com um conjunto de operações para pesquisa, classificação, recombinação e outras funções.

[154] CHISHTI, Susanne; BARBERIS, Janos. **A Revolução *Fintech*:** o manual das *startups* financeiras. Tradução: Samantha Batista. Rio de janeiro: Alta Books, 2017, p.229.

as transações digitais são teoricamente fáceis de falsificar ou duplicar. Logo, essa tecnologia resolve esse problema sem usar um intermediário financeiro.[155] Ou seja, ela oferece tanta segurança para os usuários que permite retirar os intermediários da transação sem comprometer a confiança entre as partes interessadas, com isso, teremos a possibilidade, em alguns casos, de não precisarmos mais de um banco ou instituição mediando a troca de dinheiro, pois a rede garante a proteção da transação (financeira ou monetária).[156] Ainda assim, a permissão de *blockchains* podem contribuir para a redução do risco e proteger adequadamente os interesses financeiros dos consumidores.[157]

Cabe agora fazer a seguinte pergunta: Pode o mercado financeiro brasileiro e mundial vir a alterar seu modo de atuação, se utilizando da plataforma *blockchain*? Ao meu ver, sim, mas não é fácil. É positivo tal pensamento, dado ao fato que se trata de uma tecnologia segura, interligada a determinado número de participantes, transparente e que oferece sim controle total do ocorrido em seus contornos. No mesmo sentido que parece ser possível tal uso, alerta-se ser difícil tal implementação no momento, ante ser algo novo, que destoa de controle social forte e Estatal, bem como, da ausência de sinergia com regramentos diversos existentes e necessários, vide prevenção a lavagem de dinheiro sob incumbência do UIF[158] –

---

[155] ALCARVA, Paulo. **Banca 4.0. Revolução Digital:** *fintechs, blockchain*, criptomoedas, *robo-advisers* e *crowdfunding*. Coimbra: Conjuntura Actual Editora, 2018, p.67.

[156] PELLINI, Rudá. **O futuro do dinheiro: banco digital, *fintechs, criptomoedas* e *blockchain*:** entenda de uma vez por todos esses conceitos e saiba como a tecnologia dará liberdade e segurança para você gerar riqueza. São Paulo: Editora Gente, 2019, p.75.

[157] Revista CIAB - FEBRABAN. 2020. **A gestão dos riscos cibernéticos e a crise da covid-19.** Disponível em: < https://noomis.febraban.org.br/especialista/patricia-peck-pinheiro/a-gestao-dos-riscos-ciberneticos-e-a-crise-da-covid-19>. Acesso em: 09 set. 2020.

[158] Unidade de Inteligência Financeira (UIF) é um órgão vinculado administrativamente ao Banco Central, mas com autonomia técnica e operacional, sendo responsável por produzir e gerir informações de inteligência financeira que sirvam para prevenir e combater crimes como lavagem de dinheiro, financiamento de terrorismo, financiamento da proliferação de armas de destruição em massa etc.; sendo também responsável por estabelecer uma interlocução institucional com órgãos e entidades nacionais, estrangeiros e internacionais que tenham conexão com a matéria. Assim, a Unidade de Inteligência é um grande banco de dados que recebe informações dos bancos, das seguradoras, dos cartórios de registro de imóveis, de joalherias. Em seguida, cruza dados e produz relatórios que poderão ser encaminhados à Receita Federal e aos órgãos de persecução penal em caso de indícios de ilícitos tributários ou de infrações penais. A UIF faz atualmente as mesmas funções que eram desempenhadas pelo Conselho de Controle de Atividades Financeiras (COAF). A MP 893/2019 transformou o COAF na Unidade de Inteligência Financeira. Vale ressaltar que a UIF não checa a veracidade das informações nem abre investigações. A UIF não pode quebrar o sigilo bancário e fiscal por conta própria. Pode trabalhar a informação, produzir relatório, identificar a irregularidade e mandar para os demais órgãos, como a Receita e o Parquet. A partir disso, a UIF analisa a comunicação recebida com o objetivo de identificar se existe nela algum indício de lavagem de dinheiro, de financiamento do terrorismo ou de outros crimes. Caso seja identificado algum indício de crime, é elaborado um Relatório de Inteligência Financeira (RIF), com natureza jurídica equivalente à de “peças de informação”, que é encaminhado às autoridades competentes (Receita

Unidade de Inteligência Financeira, que conta com participação efetiva dos intermediários (bancos e financeiras), demais fiscalizações monetárias e outros. Em linhas gerais, o que diverge o *blockchain* do mundo real para o digital é que o proposto pelo mundo digital abarca plataformas especificas, sem interferência Estatal, intermediários ou órgão reguladores, com entes que ingressam no mesmo por conta própria, sem necessitar de um banco para tal administração monetária. O que, se torna um risco muito grande e uma atitude incorreta afastar a regulamentação Estatal e o mercado financeiro em si (com intermediários).[159]

É importante ressaltar ainda que o *Blockchain* permitirá o acesso a novos *insights* e novos entendimentos sobre o que é verdadeiro, o que é permanente e o que é legal. Mas a descentralização e a desregulamentação apresentam um novo desafio, em que os desenvolvedores têm dificuldade em trabalhar juntos ou até mesmo encontrar estrutura. Para que um sistema totalmente descentralizado e não hierárquico funcione, todas as partes interessadas devem participar de todas as decisões – uma estrutura empolgante conceitualmente, mas desafiadora na prática.[160]

Deste modo, não restam dúvidas de que a tecnologia *blockchain* apresenta vantagens e desvantagens para o setor de serviços financeiro, vejamos:[161]

- Vantagens: (a) Processamento de transferências em tempo real e sem risco de liquidação; (b) Várias fontes de liquidação (bancárias ou não); (c) Redução dos custos operacionais em cerca de 60% do custo atual.
- Desvantagens: (a) Inexistência de privacidade, que garanta o sigilo bancário; Escalabilidade (ainda) limitada.

Da análise do trecho acima citado, cabe destacar ainda outros benefícios revolucionários dessa tecnologia, para indústria financeira, bem como para demais setores, como por exemplo: a coordenação confiável de dados, resistência a ataques, infraestrutura de tecnologia da informação compartilhada e *tokenização* (transformar um documento físico em digital) de ativos. Além disso, a *blockchain* é

Federal, Polícia Federal, Ministério Público Federal). Ademais, não raras vezes a atuação da Receita começa com informações dadas pela UIF.

[159] EROLES, Pedro. ***Fintechs*, Bancos Digitais e Meios de Pagamento:** aspectos regulatórios das novas tecnologias financeiras. São Paulo: Quartier Latin, 2019, p.54-55.

[160] CHEVAL, Saif. **Exploring non-financial use cases of blockchain.** *District* 3. Disponível em: < https://medium.com/district3/exploring-non-financial-use-cases-of-blockchain-2839bacd50a4>. Acesso em: 09 set. 2020.

[161] ALCARVA, Paulo. **Banca 4.0. Revolução Digital:** *fintechs, blockchain*, criptomoedas, *robo-advisers* e *crowdfunding*. Coimbra: Conjuntura Actual Editora, 2018, p.73.

considerada uma tecnologia disruptiva devido a sua capacidade de proteger informações pessoais, reduzir intermediários, desbloquear ativos digitais e potencialmente abrir a economia global para milhões de participantes que estão à margem do sistema financeiro tradicional.[162]

Ademais, a título de curiosidade, hoje, uma das maiores fontes de receita de companhias é a atenção dos usuários, ou seja, atenção, ou trafego, é o que empresas de mídia, ferramentas de busca ou plataformas como *Facebook* precisam para monetizar ou vender produtos. Já existem *startups* que utilizam *blockchains* para recompensar os usuários, dividindo a receita de anunciantes e remunerando quem consome esses anúncios.[163]

Pois bem, com o desenrolar da Quarta Revolução Industrial, o *blockchain* surge para permitir que as memórias dos produtos digitais sigam os objetos físicos e os orientem por toda a cadeia de valor. Quando combinado com rótulos criptograficamente seguros, criará identificações (Ids)[164] verdadeiramente únicas e registros imutáveis, facilitando e tornando menos dispendiosas as transações verificáveis entre fornecedores e clientes.[165]

Como foi dito, essas são apenas algumas informações a respeito dessa tecnologia. E pelo teor relatado, fica claro que o *blockchain* é importante e que carece de melhor avaliação e estudo para eventual implantação no ramo financeiro, principalmente quanto a falta de órgãos reguladores atuantes e de intermediários financeiros.

Cabe agora fazer uma breve análise de maneira clara e objetiva da inteligência artificial, conforme se discorrerá a seguir.

---

[162] PELLINI, Rudá. **O futuro do dinheiro: banco digital, *fintechs, criptomoedas* e *blockchain*:** entenda de uma vez por todos esses conceitos e saiba como a tecnologia dará liberdade e segurança para você gerar riqueza. São Paulo: Editora Gente, 2019, p.78.

[163] PELLINI, Rudá. **O futuro do dinheiro: banco digital, *fintechs, criptomoedas* e *blockchain*:** entenda de uma vez por todos esses conceitos e saiba como a tecnologia dará liberdade e segurança para você gerar riqueza. São Paulo: Editora Gente, 2019, p.80-81.

[164] Ids, *do* inglês *Intrusion Detection System*. Programa, ou um conjunto de programas, cuja função é detectar atividades maliciosas ou anômalas.

[165] SCHWAB, Klaus; DAVIS, Nicholas. **Aplicando a quarta revolução industrial**. Tradução: Daniel Moreira Miranda. São Paulo: Edipro, 2018, p.139.

2.4.3 Inteligência Artificial (IA) ou *Artificial Intelignce* (AI)

Não se pretende neste trabalho abordar questões técnicas ou fornecer uma introdução à Inteligência Artificial (IA), o que seria algo relativamente longo, e sim procurar-se-á analisar os pontos mais relevantes a respeito do assunto, de maneira clara e objetiva, principalmente quanto ao seu conceito, definições e a importância para o setor de serviço financeiros.

A Inteligência Artificial está transformando a maneira como interagimos com o mundo – para não mencionar a maneira como o mundo interage conosco. Com capacidades como análise avançada de dados, visão computacional, processamento de linguagem natural, aprendizado de máquina e capacidade de analisar e obter valor de milhões de *Terabytes* de dados todos os dias, ou seja, a IA está revolucionando mercados inteiros com sua implementação. O que costumava levar dias ou mesmo semanas para ser realizado agora pode ser entregue em segundos – e não há nenhum segmento que pode se beneficiar mais disso do que o setor financeiro.[166]

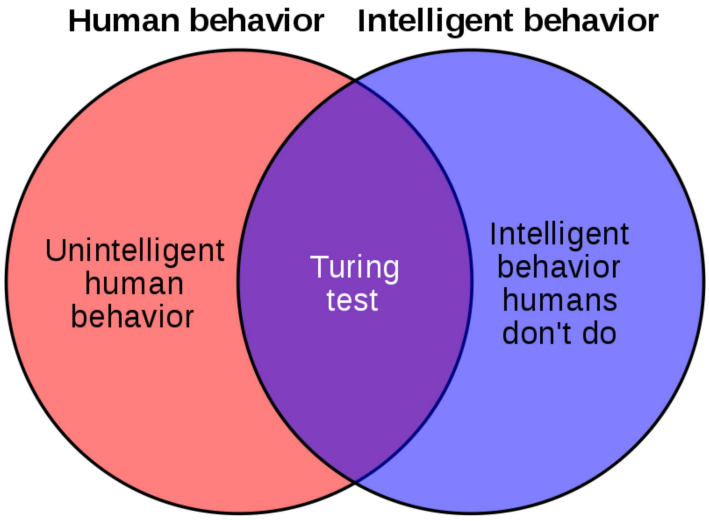
Isto posto, a título de curiosidade, o inglês e matemático Alan Mathison Turing, considerado o pai da computação foi um dos primeiros a pensar na possibilidade de uma máquina se tornar inteligente e criou um modelo teórico para um computador universal, o “Teste de Turing”, criado com o objetivo de verificar se o computador é capaz de imitar e pensar como o cérebro humano, ou seja, uma espécie de inteligência artificial com possibilidade de enganar qualquer um. O teste consistia em pedir a uma pessoa que mandasse uma série de perguntas para o computador e, depois de analisar as respostas dadas por ele, tentar diferenciar se a resposta dada pelo sistema foi elaborada pelo ser humano ou pela máquina.[167]

---

[166] DE ALMEIDA, Cristian Machado. **Inteligência Artificial no Setor Financeiro.** Disponível em: < https://www.industria40.ind.br/artigo/18361-inteligencia-artificial-no-setor-financeiro>. Acesso em: 09 set. 2020.

[167] FONTOURA, Paula Renata. **Alan Turing, o pai da computação.** Disponível em: < http://www.invivo.fiocruz.br/cgi/cgilua.exe/sys/start.htm?infoid=1370&sid=7>. Acesso em: 09 set. 2020.

Figura 1 – Teste de Turing



Fonte: IMGBIN[168]

Esse teste mostrou que será alcançado as verdadeiras oportunidades de desenvolvimento tecnológico quando uma máquina puder enganar um grupo de especialistas humanos. Ainda não passamos nesse teste, mas iremos. De fato, a IA está se desenvolvendo tão rápido que pode acontecer antes do que muitos esperam. Estamos à beira da IA geral – onde as máquinas podem executar várias tarefas – a esperança é que consigamos alcançar a super IA – onde as máquinas são mais inteligentes que os humanos – o que deve ser alcançada antes de 2040.[169]

Nesse ponto é possível ter uma certeza, a inteligência artificial (IA) está finalmente trazendo uma infinidade de capacidades para máquinas que há muito se pensava pertencer exclusivamente ao reino humano, como o processamento de linguagem natural ou informação visual.[170]

A título de exemplo, um dos segmentos com adoção mais avançada da IA é na relação com clientes. Serviços de atendimento de diversas empresas passaram a funcionar com robôs de conversa, ou *chat bots*, para receber as demandas, fornecer respostas e somente repassar a um atendente em casos em que os sistemas não

---

[168]IMGBIN. **Computing Machinery And Intelligence Turing Test Venn Diagram Bletchley Park**. Disponível em: < https://imgbin.com/png/3LQxAx7m/computing-machinery-and-intelligence-turing-test-venn-diagram-bletchley-park-png>. Acesso em: 09 set. 2020.

[169] Revista CIAB - FEBRABAN. 2020. **A IA irá potencializar a humanidade, não destruir.** Disponível em: < https://noomis.febraban.org.br/especialista/chris-skinner/a-ia-ira-potencializar-a-humanidade-nao-destruir>. Acesso em: 12 set. 2020.

[170] *MCKINSEY&COMPANY*. **[Report]** Smartening up with artificial intelligence (AI). Disponível em:<https://www.mckinsey.com.br/industries/semiconductors/our-insights/smartening-up-with-artificial-intelligence>. Acesso em: 29 ago. 2020.

conseguiram resolver. De acordo com o Bradesco, seu assistente virtual possuía em 2019 uma taxa de resolução de 95%.[171]

Segundo, Armando Kirwin, cofundador da Artie, empresa de tecnologia, o objetivo mais buscado pelos desenvolvedores e curadores da IA é imitar o cérebro humano e se tornar um *bot*[172], avatar ou entidade, cada vez mais próximos das interações com as quais os seres humanos estão acostumados. Talvez, por isso, tantos *bots* estejam presentes em todos os mercados, inclusive o financeiro. SARA, do Santander; Assistente Inteligente do BB; BIA, do Bradesco; ORI, do Banco Original, AVI, do Banco Itaú; BABI, do Banco Inter; DIN, do Banco Central são alguns exemplos de assistentes virtuais.[173]

Diante disso, é claro que as máquinas, como por exemplo, os computadores podem fazer muitas coisas tão bem ou melhor que os humanos, incluindo aquelas que as pessoas acreditam que exigem grande perspicácia e compreensão humana. No entanto, isso não significa que os computadores utilizam a perspicácia e a compreensão na execução dessas tarefas. Evidentemente, também é verdade que existem muitas tarefas em que os computadores não têm desempenho excelente (para sermos benevolentes), incluindo a tarefa de Turing de desenvolver uma conversação ilimitada.[174]

É importante frisar que o termo Inteligência Artificial (IA) foi cunhado nos EUA, em um *workshop* no Dartmouth College, em 1956, por John MacCarthy. Para melhor ilustrar cabe destacar o marco histórico da IA:

> 1956: *workshop* em Dartmouth, USA, reunindo os principais interessados no assunto: John McCarthy, Allen Newell, Herbert Simon, Marvin Minsky. Pré-história da IA: cibernética, inteligência de máquina, previsão de que em 10 anos os computadores seriam tão inteligentes quanto as pessoas, criação do termo “Inteligência Artificial”.

---

[171] Revista CIAB - FEBRABAN. 2020. **Brasil está atrasado na corrida por inteligência artificial.** Disponível em: < https://noomis.febraban.org.br/temas/inteligencia-artificial/brasil-esta-atrasado-na-corrida-por-inteligencia-artificial?pesquisa=prote%C3%A7%C3%A3o%20de%20dados>. Acesso em: 12 set. 2020

[172] *Bot* é um programa que, além de incluir funcionalidades de *worms*, sendo capaz de se propagar automaticamente por meio da exploração de vulnerabilidades existentes ou falhas na configuração de *software*s instalados em um computador, dispõe de mecanismos de comunicação com o invasor, permitindo que o programa seja controlado remotamente. O invasor, ao se comunicar com o *bot*, pode orientá-lo a desferir ataques contra outros computadores, furtar dados, enviar *spam* etc.

[173] CANTARINO BRASILEIRO. Anuário Brasileiro de Bancos (ABB) 2019. **Relatório Bancário**, 14 ed. São Paulo, 2019. Disponível em: < https://cantarinobrasileiro.com.br/publicacoes/anuariodebancos19/download/>. Acesso em: 12 set. 2020.

[174] RUSSELL, Stuart J.; NORVIG, Peter. **Inteligência Artificial.** Tradução: Regina Célia Simille. 3.ed. Rio de Janeiro: Elsevier, 2013. Livro eletrônico, não paginado.

> 1956-1970: programas universais (métodos fracos): tradução automática, demonstração automática de teoremas, resolução de problemas (General Problem Solver). Proposta de modelos de redes neurais artificiais: Frank Rosenblatt. The perceptron: A probabilistic model for information storage and organization in the brain (1958), Marvin Minsky e Seymour Papert. Perceptrons (1969).
> 1970 - 1980: sucesso dos primeiros sistemas especialistas: Mycin, Dendral. Métodos fortes: restrição do domínio, introdução do conhecimento e forma de raciocínio do especialista. Pesquisa: IA distribuída, raciocínio baseado em casos, algoritmos genéticos; "renascer" das redes neurais. James McClelland e David Rumelhart. Parallel Distributed Processing (1986) – uso da IA em larga escala nas instituições.
> **Observações:**
> - Os anos 70 constituem a década romântica da IA, quando se pretendeu simular a inteligência humana em situações pré-determinadas, envolvendo conhecimento de senso comum. Houve um grande impulso, com a criação de formalismos de representação de conhecimento mais adaptados ao domínio do problema. Mas, ocorreram diversos fracassos porque se subestimou a quantidade de conhecimento necessária para tratar o mais banal problema de senso comum.
> - A década de 80 é a idade moderna da IA, onde se observa amadurecimento em função das dificuldades enfrentadas com a tentativa de simulação da inteligência humana e sucesso no desenvolvimento de sistemas especialistas. A pesquisa em IA volta-se para a tentativa de simular o comportamento de um especialista humano ao resolver problemas em um domínio específico. Foi subestimada a complexidade do problema de aquisição de conhecimento ao se lidar com domínios com incerteza e uma reintensificação do interesse na pesquisa, na IA Conexionista, função do aparecimento de novos métodos de aprendizagem de redes neurais.
> - A partir dos anos 90, começa a época de ouro, com a explosão da pesquisa e avanços substanciais em aprendizagem de máquina, sistemas tutores inteligentes, raciocínio baseado em casos, sistema multiagente, raciocínio com incerteza, mineração de dados, processamento de linguagem natural, visão por computador, realidade virtual, jogos, robótica, redes neurais e vida artificial. O foco da IA passa a ser entender, do ponto de vista computacional, o comportamento inteligente e construir artefatos que apresentem esse comportamento inteligente.[175]

Ainda, assim, é importante mencionar que tendo em vista a sua influência e impacto no mundo moderno, a IA é considerada por muitos especialistas a tecnologia mais disruptiva do século, em uso atualmente, com tendências a seguir, sendo a mais relevante pela próxima década.

Por certo, definir a Inteligência Artificial não é algo fácil. Em poucas palavras, diríamos que trata de um sistema que utiliza a combinação de várias tecnologias, que ajuda o *software*[176] a "pensar" e encontrar soluções tal qual ou melhor do que um humano poderia fazer, ou seja, é uma tecnologia que permite que as máquinas percebam, compreendam, encontrem padrões, executem e aprendam por conta própria ou complementem atividades realizadas por humanos, sempre com o intuído

---

[175]ENGEL, Paulo Martins. **Inteligência Artificial.** Disponível em: < http://www.inf.ufrgs.br/~engel/data/media/file/inf01048/introducao.pdf>. Acesso em: 09 set. 2020.
[176]Software, programas de computador; instruções que o computador é capaz de entender e executar.

de aperfeiçoar sua operação.[177] Ou seja, a Inteligência Artificial (IA) é a combinação de múltiplas tecnologias que permitem que as máquinas percebam, compreendam e atuem – e aprendam por conta própria ou complementem as atividades humanas.[178] Logo, é a capacidade de pensamento das máquinas, de forma autônoma e similar ao pensamento humano. Seria a variável da razão humana, aplicada a um programa de computador, criado para tomar decisões e raciocinar. Ao analisarem dados e cruzarem informações, as máquinas são capazes de fazer escolhas muito mais precisas, com base em parâmetros previamente estabelecidos, de forma autônoma e similar ao pensamento humano.

Vale transcrever a definição de Luís Moniz Pereira sobre Inteligência Artificial:

> Inteligência Artificial é a ciência que resulta de uma estreita simbiose entre a forma de pensar do homem e a máquina, vale-se da capacidade do computador para processar símbolos, automatizando faculdades mentais perceptivas, cognitivas e manipulativas até hoje desconhecidas das máquinas.[179]

Também cabe destacar a definição de Inteligência Artificial feita pelo professor e pesquisador Gilson Schwartz:

> Inteligência artificial é um conjunto de programas que executam tarefas e gerenciam memórias cuja governança, legitimidade e controle social dependem do contexto. Trata-se de automação, digitalização e centralização dos sistemas de informação supostamente distribuídos ou descentralizado, cujo propósito é a automação, ou seja, a garantia de regularidade com aumento da eficiência e produtividade dos sistemas econômicos independente da vontade de cada indivíduo.[180]

Marvin Minsky, explica em sua obra que: “a IA é a ciência de fazer com que máquinas façam coisas que requereriam inteligência se feitas pelos homens”.[181]

Dessa forma, o que se percebe é que com a Revolução Industrial houve a substituição da força animal e, posteriormente, do próprio trabalho humano por

---

[177] TEIXEIRA, Tarcisio; LOPES, Alan Moreira; TAKADA, Thalles. **Manual jurídico da inovação e das startups.** 2.ed. Salvador: Editora JusPodivm, 2020, p.37.

[178] ACCENTURE. **Inteligência Artificial:** o que significa e porque é o futuro do crescimento? Disponível em: < https://www.accenture.com/br-pt/insight-artificial-intelligence-future-growth>. Acesso em: 12 set. 2020.

[179] PEREIRA, Luís Moniz. **Inteligência Artificial: mito e ciência.** ResearchGate. Disponível em: < https://www.researchgate.net/publication/242109725_INTELIGENCIA_ARTIFICIAL_-_MITO_E_CIENCIA>. Acesso em: 09 set. 2020.

[180] MACHADO, Ricardo. Crise sanitária coloca em causa o “*hype*” da Inteligência Artificial e revela suas fragilidades estruturais. Entrevista com Gilson Schwartz. 08 jun. 2020. **IHU On-Line Revista Instituto Humanitas Unisinos,** São Leopoldo. Disponível em: < http://www.ihu.unisinos.br/159-noticias/entrevistas/599715-crise-sanitaria-coloca-em-causa-o-hype-da-inteligencia-artificial-e-revela-suas-fragilidades-estruturais-entrevista-especial-com-gilson-schwartz>. Acesso em: 12 set. 2020.

[181]ENGEL, Paulo Martins. **Inteligência Artificial.** Disponível em: < http://www.inf.ufrgs.br/~engel/data/media/file/inf01048/introducao.pdf>. Acesso em: 09 set. 2020.

máquinas, agora é nossa inteligência que vai sendo trocada por dispositivos eletrônicos cada vez mais potentes.[182]

De certo, hoje, a transformação digital e a ascensão do uso de dados possibilitam que os *insights* obtidos por meio da Inteligência Artificial (IA) solucionem de forma eficaz diferentes problemas e desafios. No ambiente dos negócios, a IA também proporciona benefícios, dentre eles, desenvolvimento de novos produtos e melhor experiência de compra do consumidor.[183]

Neste ponto, a Inteligência Artificial (IA) permite e precisa trabalhar com grandes volumes de dados, o que os torna sua principal matéria-prima e todo ser humano em uma mina de dados.[184] Isso porque, o mundo está gerando volumes antes inimagináveis do combustível que alimenta a IA – dados.[185] Uma regra simples para lembrar: 80% de suas análises virão de 20% de seus dados. Mas os 20% restantes, a análise exploratória baseada em IA, virão de 80% dos seus dados.[186] O avanço exponencial e combinatório do poder computacional difundido nos mais variados tipos de objeto não amplia só a magnitude das informações coletadas. Amplia também, e sobretudo, a capacidade dos algoritmos[187] de analisar e interpretar esses dados.[188]

Cabe destacar, ainda, que algoritmos inteligentes já são capazes de prever a intenção estratégica das corporações com base em cada pedaço de informação que

---

[182] ABRAMOVAY, Ricardo. Inteligência artificial pode trazer desemprego e fim da privacidade **Instituto Humanista UNISINOS,** São Leopoldo, 30 abr. 2017**.** Disponível em: < http://www.ihu.unisinos.br/78-noticias/566403-inteligencia-artificial-pode-trazer-desemprego-e-fim-da-privacidade>. Acesso em: 09 set. 2020.

[183] KPMG. **Inteligência Artificial:** conheça os cinco pilares que conduzem a aplicação. Disponível em: < https://home.kpmg/br/pt/home/insights/2020/02/inteligencia-artificial-pilares.html>. Acesso em: 13 set. 2020.

[184] TOLCACHIER, Javier. Inteligência artificial a serviço da especulação financeira. **Instituto Humanista UNISINOS,** São Leopoldo, 25 jul. 2019. Disponível em: < http://www.ihu.unisinos.br/78-noticias/591067-inteligencia-artificial-a-servico-da-especulacao-financeira>. Acesso em: 09 set. 2020.

[185] BUGHIN, Jacques. et al. Artificial intelligence can deliver real value to companies. **McKinsey&Company.** Disponível em: < https://www.mckinsey.com.br/business-functions/mckinsey-analytics/our-insights/how-artificial-intelligence-can-deliver-real-value-to-companies>. Acesso em: 13 set. 2020.

[186]GARTNER. **Fact vs Fiction: Finance Use of AI.** Disponível em: < https://www.gartner.com/smarterwithgartner/fact-vs-fiction-finance-use-of-ai/>. Acesso em: 13 set. 2020.

[187] Algoritmos são conjuntos de regras que os computadores seguem para resolver problemas e tomar decisões sobre um determinado curso de ação. Em termos mais técnicos, um algoritmo é uma sequência lógica, finita e definida de instruções que devem ser seguidas para resolver um problema ou executar uma tarefa, ou seja, uma receita que mostra passo a passo os procedimentos necessários para a resolução de uma tarefa.

[188] ABRAMOVAY, Ricardo. Inteligência artificial pode trazer desemprego e fim da privacidade **Instituto Humanista UNISINOS,** São Leopoldo, 30 abr. 2017**.** Disponível em: < http://www.ihu.unisinos.br/78-noticias/566403-inteligencia-artificial-pode-trazer-desemprego-e-fim-da-privacidade>. Acesso em: 09 set. 2020.

possam encontrar e entender.[189] Com isso, maior tem se tornado a possibilidade de captar dados para tomada de decisões. Também, o uso de Inteligência Artificial para monitoramento do fluxo de dados coletados e recebidos de equipamentos inteligentes tem sido utilizado com sucesso nas ferramentas de proteção de dados.[190]

Segundo o Instituto de Pesquisa *Gartner,* ainda em 2020, o *deep learning* corresponderá a 44% do valor global dos negócios derivados de inteligência artificial. *Deep learning* nada mais é do que redes neurais que permitem a realização de mineração de dados (*data mining*) e reconhecimento de padrões em grandes conjuntos de dados, possibilitando que os algoritmos preditivos – algoritmos que identificam padrões – trabalhem diretamente com as informações. Isso impacta na capacidade das instituições de automatizar processos de decisão e interação.

Outro ponto importante é que o desenvolvimento das inteligências artificiais permite automatizar profissões muito qualificadas. Os *chatbots*[191] (robôs falantes capazes de responder às perguntas de clientes e detectar emoções sem que os clientes percebam que estão se comunicando com não humanos) são um exemplo espetacular, assim como Watson, a inteligência artificial da IBM, ou as caixas de som inteligentes domésticas (Alexa, da Amazon).[192] Neste ponto, interações por *chatbot*s cresceram 212% em 2019, quando chegaram a 248 milhões. Entre janeiro e abril, deste ano, o aumento foi de 78% no setor de serviços financeiros.[193] Ainda

---

[189] CHISHTI, Susanne; BARBERIS, Janos. **A Revolução *Fintech*:** o manual das *startups* financeiras. Tradução: Samantha Batista. Rio de janeiro: Alta Books, 2017, p.259.

[190] RIBEIRO, Janete. **IoT e Leis de Privacidade.** ABINC. Disponível em: < https://abinc.org.br/iot-e-leis-de-privacidade/>. Acesso em: 13 set. 2020.

[191] *Chatbot* (ou *chatterbot* ou *verbot*) é um programa de computador que tenta simular um ser humano na conversação com as pessoas. O objetivo é responder perguntas de tal forma que as pessoas tenham a impressão de estar conversando com outra pessoa e não com um programa de computador. Após o envio de perguntas em linguagem natural, o programa consulta uma base de conhecimento e, em seguida, fornece uma resposta que tenta imitar o comportamento humano. A palavra *chatterbot* foi inventada por Michael Mauldin (fundador da Lycos, Inc. e criador do primeiro chatterbot Julia) em 1994, para descrever estes robôs de conversação. Os chatbots otimizam serviços digitais de muitos bancos, para realizar cobranças e oferecer serviços financeiros, ajudar os usuários a tomarem decisões, e informar sobre saldo na conta, transações recentes, histórico de pagamentos e limite de crédito. Mas é preciso investir em proteção de dados e ter estratégias de segurança, pois o segmento financeiro está na mira do cibercrime.

[192] SANTOS, João Vitor. Capitalismo no século XXI e a força cerebral no cerne da cadeia do valor. Entrevista com Yann Moulier Boutang. **IHU On-Line Revista Instituto Humanitas Unisinos**, São Leopoldo, ano 18, n. 525, p.49-55, 30 jul. 2018. Disponível em: < http://www.ihuonline.unisinos.br/artigo/7350-capitalismo-no-seculo-xxi-e-a-forca-cerebral-no-cerne-da-cadeia-do-valor>. Acesso em: 30 ago. 2020.

[193] CANTARINO BRASILEIRO. Anuário Brasileiro de Bancos (ABB) 2020. **Relatório Bancário**. São Paulo, 2020. Disponível em: <

mais impressionante, é como a robótica financeira está evoluindo da simples automação de tarefas individuais para a automação completa de processos que podem melhorar a precisão das análises e previsões financeiras reduzindo custos, minimizando esforços e melhorando a velocidade e a precisão. Cerca de 80% dos líderes financeiros implementaram ou estão planejando implementar a RPA (automação de processos robóticos).[194]

A título de curiosidade, outra área em que a IA vem crescendo é a do direito. Partindo da capacidade de compreensão de textos escritos, sistemas passaram a ser utilizados em análises de processos. O Supremo Tribunal Federal (STF) criou um projeto denominado Victor para exame de casos de repercussão geral, como parte de seu programa de transformação digital. Segundo a corte, verificações que levavam cerca de 45 minutos por funcionários do Tribunal passaram a ser processadas em cinco segundos pelo sistema.

Como se vê, a utilização da Inteligência Artificial pode gerar diversos benefícios, entre eles estão a redução de custos, aumento da produtividade, entrega de produtos, serviços mais ágeis e flexíveis, aumento dos lucros e maior rapidez na concretização da venda.[195]

Mas como em tudo na vida, as vantagens têm sempre a contraposição de risco. Por exemplo, robôs controlados por IA terão dificuldade para prever o impacto da reorganização de competências e empregos, criando tensões pesadas na sociedade. Além disso, o funcionamento dos algoritmos do aprendizado automático ainda é muito obscuro para a maioria das pessoas, e esses mecanismos podem refletir preconceitos socialmente indesejáveis que precisarão ser corrigidos. As previsões de longo prazo dizem que não devemos subestimar as ameaças existenciais se o alinhamento entre valores da IA e os valores humanos fracassar. Elas também advertem sobre os riscos de segurança cibernética que poderão ocorrer se os criminosos conseguirem *hackear* ou confundir os aplicativos IA. Assim, serão necessários esforços para garantir que as decisões tomadas por máquinas

---

https://cantarinobrasileiro.com.br/publicacoes/anuariodebancos20/download/>. Acesso em: 29 ago. 2020.

[194] GARTNER. **Robotic Process Automation (RPA) Role in Finance Automation.** Disponível em: < https://www.gartner.com/en/finance/insights/robotics-in-finance>. Acesso em: 13 set. 2020.

[195] TEIXEIRA, Tarcísio; LOPES, Alan Moreira; TAKADA, Thalles. **Manual jurídico da inovação e das startups.** 2.ed. Salvador: Editora JusPodivm, 2020, p.39

sejam programadas de forma segura, resistentes à sabotagem ou exploração por meio de ataques cibernéticos.[196]

De igual modo, uma ameaça em particular é digna de maiores considerações: as máquinas ultra inteligentes podem levar a um futuro que é muito diferente de hoje – podemos não gostar dele e, nesse ponto, podemos não ter mais escolha. Tais considerações conduzem inevitavelmente à conclusão de que é preciso pesar cuidadosamente, e logo, as possíveis consequências da pesquisa em IA.[197]

Como se pode perceber, o uso da inteligência artificial não se limita apenas a *softwares* e robôs, como também em *nanorobôs*, androides, avatares e similares.[198] Não há dúvidas de que a evolução da inteligência artificial e sua forma de utilização, tem sido cada vez mais rápida, e vem provocando impactos relevantes no setor de serviços financeiro. Essa tecnologia pode até ajudar com o gerenciamento do risco de crédito ao prever com precisão quais clientes são mais propensos a cancelar o serviço ou ter inadimplência em seus empréstimos. Sua análise de perfil de dados pode determinar se alguém é de alto ou baixo risco ao vasculhar através de variáveis e relações, interações, dependências, associações e muito mais.[199] Nota-se, portanto, que um dos mercados em que a inteligência artificial está ganhando cada vez mais relevância é o financeiro, com aumento de 72% de investimentos nessa tecnologia. Diversos empreendimentos desse setor estão começando a adotar soluções tecnológicas de ponta, incluindo as ferramentas de IA.[200]

De olho na crescente demanda por soluções digitais, impulsionada ainda mais durante o período de isolamento social, o setor financeiro para aferir o grau de conveniência e satisfação dos clientes, está implementando vários pontos de captação de informação para serem trabalhados por sistemas baseados em IA, para aprimorar a experiência do cliente. A IA aprenderá sobre os hábitos de consumo do cliente, por exemplo, ao rastrear e analisar as transações dos seus cartões. Com

---

[196] SCHWAB, Klaus; DAVIS, Nicholas. **Aplicando a quarta revolução industrial**. Tradução: Daniel Moreira Miranda. São Paulo: Edipro, 2018, p.178-187.
[197] RUSSELL, Stuart J.; NORVIG, Peter. **Inteligência Artificial.** Tradução: Regina Célia Simille. 3.ed. Rio de Janeiro: Elsevier, 2013. Livro eletrônico, não paginado.
[198] TEIXEIRA, Tarcísio; LOPES, Alan Moreira; TAKADA, Thalles. **Manual jurídico da inovação e das startups.** 2.ed. Salvador: Editora JusPodivm, 2020, p.44.
[199] DE ALMEIDA, Cristian Machado. **Inteligência Artificial no Setor Financeiro.** Disponível em: < https://www.industria40.ind.br/artigo/18361-inteligencia-artificial-no-setor-financeiro>. Acesso em: 09 set. 2020.
[200] SIMPLY. **Desmistificando a inteligência artificial.** Disponível em: < https://rdstation-static.s3.amazonaws.com/cms%2Ffiles%2F18483%2F1590000458Ebook_Inteligncia_Artificial.pdf>. Acesso em: 12 set. 2020.

base nesses dados, as instituições ficam capazes de planejar o seu orçamento e de criar uma oferta personalizada, ao mesmo tempo que ajudará na conexão com os sistemas internos para fornecer rapidamente o acesso aos dados certos ou para inserir informações do cliente; além disso, a IA conversacional no setor financeiro também é usada na prevenção de fraudes, pois pode ser programada para monitorizar e reconhecer sinais de alerta de atividades fraudulentas e enviar notificações.[201]

A vista disso, de acordo com os dados do relatório The Art of Customer-Centric Artificial Intelligence: How organizations can unleash the full potential of AI in the customer experience, divulgados pelo Instituto de Pesquisa Capgemini, o Brasil é vice-campeão no *ranking* de países com maior interação diária com inteligência artificial entre os clientes. Só perde para Suécia, e está à frente dos EUA e da média mundial. O índice de interações diárias ativadas por IA é de 64% entre os brasileiros, enquanto globalmente a média é de 54%. No caso dos suecos, chega a 70%. Ainda, sete em cada dez clientes brasileiros (71%) também esperam aumentar, no pós-covid, as interações sem contato, com uso de IA por meio de assistentes virtuais, soluções de reconhecimento facial, *app*, entre outros meios. O percentual supera a média mundial, de 62%. Com relação à satisfação, 62% dos clientes brasileiros se dizem satisfeitos, mas ainda sentem falta de algo que os surpreenda nesse contato. O nível de satisfação na média global é de 57% em 2020. Há dois anos esse índice era de 69%. Por setor, o nível de satisfação dos clientes que utilizam IA em suas interações com as organizações é maior no setor financeiro e de seguros (61%). Na sequência estão o automotivo (58%) e a administração pública (58%).

Assim, é inegável que o objetivo das instituições ao apostarem em IA é levar conveniência aos clientes e chegar a um atendimento individualizado e customizado. Deles, 50% acreditam que a tecnologia propicia mais capacidade aos canais e 40% confiam em sua eficiência na contratação de crédito.[202]

Em uma pesquisa (publicada em julho de 2020), feita pela *Price waterhouse Coopers* (PwC), prestadora de serviços profissionais nas áreas de auditoria e consultoria, revelou que:

---

[201] ALCARVA, Paulo. **Banca 4.0. Revolução Digital:** *fintechs, blockchain*, criptomoedas, *robo-advisers* e *crowdfunding*. Coimbra: Conjuntura Actual Editora, 2018, p.18.

[202] CANTARINO BRASILEIRO. Anuário Brasileiro de Bancos (ABB) 2020. **Relatório Bancário**. São Paulo, 2020. Disponível em: < https://cantarinobrasileiro.com.br/publicacoes/anuariodebancos20/download/>. Acesso em: 29 ago. 2020.

> A transformação digital também levanta a questão da confiança. Por exemplo, a crescente aplicação da inteligência artificial na consultoria de investimentos e na aprovação de empréstimos torna importante prover asseguração aos clientes sobre como seus dados são usados e como esses novos sistemas podem beneficiá-los. Medidas de segurança cibernética eficazes também são uma parte crítica da manutenção da confiança.[203]

É importante observar, ainda, que incorporar tecnologias de IA, como aprendizado de máquina (*machine learning*), aprendizado profundo e raciocínio de máquina baseado em algoritmo – diretamente em aplicativos de gerenciamento financeiro será transformador. Um caso de uso potencial para IA incorporada ilustra esse impacto. A maioria dos aplicativos de gerenciamento financeiro pode combinar pagamentos recebidos com faturas de contas a receber (AR) pendentes, desde que o valor do pagamento corresponda à fatura. No entanto, dados de remessa incompletos, pagamentos parciais e pagamento de várias faturas em uma única remessa podem causar discrepâncias que levam tempo e esforço para serem resolvidas. A incorporação de tecnologias de IA em aplicativos financeiros pode enfrentar esses desafios, modelando combinações de pagamentos e faturas em diferentes situações.

Cabe destacar também que, ao contrário do que muitos pensam, a IA não vem necessariamente para substituir a mão-de-obra humana, pelo contrário: sua maior vantagem é potencializar o trabalho dos profissionais.[204] Logo, os trabalhos do futuro serão baseados em máquinas que potencializam os seres humanos, com serviços escaláveis sem que, para isso, novas contratações precisem ser realizadas. Transformando profundamente a forma como trabalhamos hoje, onde, máquinas cuidam de tarefas e processos burocráticos, enquanto os colaboradores poderão se dedicar a tarefas que exigem capacidades e competências que as máquinas não possuem. Exemplo disso é a criatividade, a empatia e o julgamento crítico. Essas são características humanas que as máquinas dificilmente poderiam superar. São essas as características que garantirão empregos e oportunidades de trabalho. Para a consultoria e auditoria *Price waterhouse Coopers* (PwC), os robôs serão

---

[203] PRICE WATERHOUSE COOPERS (PWC). **Tendências do setor de bancos e mercado de capitais em 2020:** lançando as bases para o crescimento. Disponível em: < https://www.pwc.com.br/pt/estudos/setores-atividade/financeiro/2020/tendencias-do-setor-de-bancos-e-mercado-de-capitais-em-2020-lancando-as-bases-para-o-crescimento.html>. Acesso em: 13 set. 2020.

[204] HORN, Guilherme. As tendências e benefícios da Inteligência Artificial em Serviços Financeiros. **Instituto Humanista UNISINOS,** São Leopoldo, 20 jul. 2017**.** Disponível em: < http://www.ihu.unisinos.br/78-noticias/569800-as-tendencias-e-beneficios-da-inteligencia-artificial-em-servicos-financeiros>. Acesso em: 09 set. 2020.

responsáveis por substituir 38% das vagas de trabalho nos Estados Unidos até 2030. No Reino Unido serão 30% e no Japão 21% no mesmo período. E mesmo com a substituição de diversos cargos pelas máquinas, isso não significa que as pessoas ficarão sem emprego.

Com isso, as perspectivas acerca do uso da IA no mercado de trabalho são positivas. Segundo a pesquisa CEO Outlook 2019, da KPMG, cerca de 73% dos CEOs apontam que a IA criará mais oportunidades de trabalho do que eliminará.

Como se pode observar, a inteligência artificial promete penetrar no mercado de serviços financeiros, como por exemplo, os bancos digitais de forma intensa e beneficiá-lo das mais variadas formas, com algoritmos inteligentes capazes de tomar decisões que reduzem custos e oferecem novas possibilidades a consumidores e investidores. Onde, máquinas aprenderão a pensar com inteligência embarcada e sensores estarão em todos os lugares, coletando bilhões de dados.

De acordo com a segunda edição da Pesquisa *Fintech Deep Dive 2019*, da PwC, conduzida em parceria com a Associação Brasileira de *Fintechs* (ABFintechs), a IA é uma tecnologia essencial para ajudar as *fintechs* a gerenciar riscos, prevenir fraudes e combater a lavagem de dinheiro, com base no monitoramento e na análise dos dados de comportamentos dos clientes. Ela permite também a automação de processos para reduzir custos administrativos, a identificação precoce de novas demandas de mercado e o desenvolvimento de previsões sobre a curva de preço dos ativos para os gestores de investimentos.

Conforme demonstrado, o que se conclui é que a combinação de abordagens digitais e humanas é absolutamente crucial em um mundo no qual os consumidores ainda valorizam as interações pessoais, mas também esperam ter experiências avançadas baseadas na tecnologia.[205] Além disso, o potencial da IA foi além de ser uma mera automação de tarefas simples para ser uma ferramenta de colaboração poderosa entre funcionários humanos e máquinas. As empresas, inclusive as do setor financeiro, bem-sucedidas compreenderão a importância do contexto na interação homem-máquina e aproveitarão os avanços que as ajudam a colaborar em

[205] PRICE WATERHOUSE COOPERS (PWC). **Tendências do setor de bancos e mercado de capitais em 2020:** lançando as bases para o crescimento. Disponível em: < https://www.pwc.com.br/pt/estudos/setores-atividade/financeiro/2020/tendencias-do-setor-de-bancos-e-mercado-de-capitais-em-2020-lancando-as-bases-para-o-crescimento.html>. Acesso em: 13 set. 2020.

maior escala. Isso as posicionará para reimaginar todos os aspectos de todo o seu negócio, do zero.[206]

Entendida a Inteligência Artificial, cabe agora, demonstrar os pontos mais relevantes sobre a Internet das Coisas, conforme se verá a seguir.

2.4.4 Internet das Coisas (IoC) ou *Internet of Things* (IoT)

É importante ressaltar que para melhor abordagem do tema será apresentada, de maneira clara e objetiva, algumas noções básicas sobre Internet das Coisas, para melhor compreensão do assunto.

Primeiramente é relevante definir o termo “Internet das Coisas ou *Internet of Things*”, afim de que seja possível compreender posteriormente o conteúdo aqui apresentado.

Esse termo foi usado inicialmente por Kevin Ashton, pesquisador britânico do Massachusetts Institute of Technology (MIT), em 1999. É utilizado para designar a conectividade entre vários tipos de objetos do dia-a-dia sensíveis à internet, desde eletrodomésticos, carros, roupas, sapatos, remédios, etc., com sensores capazes de captar aspectos do mundo real e enviá-los a plataformas que recebem estas informações e as utilizam de forma inteligente, moldando uma rede de objetos interligados. Conceptualmente é a possibilidade de conectar o mundo físico com o mundo digital através da *internet*.[207] Assim, será possível registar dados ligados às nossas ações de maneira mais assertiva e usar essas informações a nosso favor, de forma a integrar processos, serviços e aplicações.[208]

Nesse ponto, vale transcrever a explicação dada por Kevin Ashton sobre IoT em entrevista concedida a Revista Inovação em Pauta nº 18, edição de dezembro/2014:

> A *internet* das coisas se baseia na ideia de que estamos presenciando o momento em que duas redes distintas – a rede de comunicações humana

---

[206] ACCENTURE. **Technology Vision Consumer Survey 2020**. Disponível em: < https://www.accenture.com/us-en/insights/technology/technology-trends-2020>. Acesso em: 30 ago. 2020.

[207] Internet é a *rede* mundial de computadores e outros dispositivos interligados que possibilitam acesso à informação nela disponibilizada.

[208] SANTOS, Pedro Miguel Pereira. **Internet das coisas:** o desafio da privacidade. Dissertação (mestrado em sistemas de informação organizacionais) – Escola Superior de Ciências Empresariais, Instituto Politécnico de Setúbal, Setúbal, 2016. Disponível em: < https://comum.rcaap.pt/bitstream/10400.26/17545/1/Disserta%C3%A7%C3%A3o%20Pedro%20Santos%20140313004%20MSIO.pdf>. Acesso em: 09 set. 2020.

> (exemplificada na *internet*) e o mundo real das coisas – precisam se encontrar. Um ponto de encontro onde não mais apenas "usaremos um computador", mas onde o "computador se use" independentemente, de modo a tornar a vida mais eficiente. Os objetos – as "coisas" – estarão conectados entre si e em rede, de modo inteligente, e passarão a "sentir" o mundo ao redor e a interagir. Isso porque, os computadores – e, por conseguinte, a *internet* – são quase que completamente dependentes dos seres humanos para obter informação. Quase a totalidade dos dados disponíveis na *internet* foram, primeiramente, coletados e criados por pessoas – seja digitando um teclado, pressionando um botão de gravação, tirando uma foto digital ou escaneando um código de barras. Os diagramas convencionais que ilustram a *internet* incluem computadores, servidores, roteadores e outras máquinas, mas omitem os mais numerosos roteadores de todos – gente. O problema é que as pessoas têm tempo, atenção e precisão limitados. Contudo, se tivéssemos computadores que conhecessem tudo o que existe para se saber sobre as coisas reais – usando dados que eles mesmos agrupem, sem nossa ajuda – poderíamos, por exemplo, acompanhar tudo, o que reduziria imensamente o desperdício, perdas e custos.[209]

Já Augustin Rubini, define em sua obra que:

> Internet das Coisas (IoT), é simplesmente um conjunto de tecnologias e aplicativos que permitem que dispositivos com sensores incorporados sejam conectados à *Internet* e troquem dados, usando o mesmo Protocolo de *Internet* (*IP Protocol*). Esses dispositivos conectados são usados no mundo físico e procuram melhorar a qualidade de vida e reduzir gastos. Além disso, o *smartphone* é um dos dispositivos, cujo o crescimento, impulsiona a IoT, armazenando dados de rastreadores físicos, gerenciando aparelhos inteligentes e outros usos. A IoT frequentemente está associada, ao *Blockchain,* que pode expandir o uso de dados criptográficos no espaço da IoT, tornando as informações do cliente mais seguras e as transações mais rápidas.[210]

Numa definição mais ampla, podemos dizer que internet das coisas é um termo utilizado para definir um complexo de "objetos inteligentes", que são conectados à *internet*, captando informações dos usuários, e transmitindo essas informações de modo a fornecer um serviço personalizado, possibilitando que o consumidor tenha um papel mais ativo e também que os objetos possuam funcionalidades adaptáveis, de modo que estes estejam perfeitamente integrados à vida e ao dia a dia do usuário, mas também afetando a sua privacidade, de modo que legislações como a LGPD e a GDPR são importantíssimas para regular o dever de transparência dos fornecedores quanto aos dados coletados, bem como o direito

---

[209] FINEP. A revolução da Internet das Coisas. Entrevista com Kevin Ashton. **Revista Inovação em Pauta**, Rio de janeiro, n. 18, p.04, dez. 2014. Disponível em: < http://finep.gov.br/images/revista/revista18/index.html#p=6>. Acesso em: 13 set. 2020.

[210] RUBINI, Agustin. **A Fintech em um Flash**. Tradução: Fernanda Belokurows. Babelcube Inc., 2017. Livro eletrônico, não paginado.

à privacidade e segurança do usuário, especialmente tendo em vista atualizações de sistema e roubo de dados por *hackers.*[211]

Dessa maneira, é importante destacar que não existe um conceito único para a IoT. De maneira geral, pode ser entendido como o fenômeno de conectar o mundo físico à *internet*, em contraste à internet das pessoas, que conecta nós humanos uns aos outros por meio da tecnologia. Na IoT, dispositivos físicos são conectados a sensores que coletam dados sobre a operação, a localização e o estado de um dispositivo. Esses dados são processados usando-se várias técnicas de análise de dados para monitorar o dispositivo remotamente a partir de um escritório central ou para prever futuras falhas. Trata-se de um dos setores de crescimento mais acelerado no ramo de tecnologia da informação (TI) e um componente-chave da indústria da análise de dados.[212]

Ou seja, é a revolução na forma como as pessoas se conectam com as marcas, por meio de tudo, absolutamente tudo, que possa ser conectado à *internet*, desde seu *smartphone* até sua caneta, passando pela geladeira, TV, carro, roupa e muitos outros itens do dia a dia, que, em breve, estarão conectados entre si, ajudando, assim, as marcas a entender mais as pessoas e a vender mais. Assim, a difusão da IoT deve ser acompanhada de uma quantidade enorme de dispositivos conectados e, para isso, vamos precisar de soluções que extraiam valor dos dados gerados.[213]

Ainda, assim, é importante mencionar que mais do que uma evolução da tecnologia da informação, a internet das coisas redefine a maneira como interagimos com o mundo físico e também viabiliza formas – até então impossíveis – de fazer negócios, de gerenciar a infraestrutura pública e de organizar a vida das pessoas.[214]

De acordo com Klaus Schwab, pode-se resumir, sinteticamente, da seguinte forma as principais características da tecnologia IoT:

> 1. A IoT consiste em uma gama de sensores inteligentes e conectados que reúnem e comunicam dados para outros dispositivos ou indivíduos pela *internet*, com diversas finalidades, aprimorando as interações entre

---

[211] TEIXEIRA, Tarcísio; LOPES, Alan Moreira; TAKADA, Thalles. **Manual jurídico da inovação e das startups.** 2.ed. Salvador: Editora JusPodivm, 2020, p.57-58.

[212] SHARDA, Ramesh; DELEN, Dursun; TURBAN, Efraim. ***Business intelligence* e análise de dados para gestão do negócio.** Tradução: Ronald Saraiva de Menezes. 4.ed. Porto Alegre: Bookman, 2019, p.495-496.

[213] MORAIS, Felipe. **Transformação digital.** São Paulo: Saraiva educação, 2020, p.102.

[214] ELLEN, Patrícia. Internet das coisas já é realidade, porém falta regulamentá-la. **McKinsey&Company.** Disponível em: < https://www.mckinsey.com.br/our-insights/blog-made-in-brazil/internet-das-coisas-ja-e-realidade-porem-falta-regulamenta-la>. Acesso em: 13 set. 2020.

> humanos e máquinas, e a economia de dados entre máquinas crescerá até ficar maior que a economia entre humanos. Dezenas de bilhões de dispositivos serão adicionados à IoT na próxima década e, por meio de aplicações industriais, sua interação poderá adicionar até US$ 14 trilhões à economia global em 2030.
> 2. A distribuição de sensores e dispositivos apresenta desafios transacionais em relação aos dados, como a privacidade, a propriedade, a disponibilidade, entre outros. O estabelecimento de políticas e regulamentos sobre os fluxos de dados globais da IoT será um grande desafio da Quarta Revolução industrial.
> 3. A IoT vai muito além dos aparelhos inteligentes conectados à internet e dos serviços que eles fornecem. O valor real do desenvolvimento da IoT reside na coleta, análise e gestão de dados, no encontro de oportunidades e correlações inesperadas e na antecipação das tendências de disrupção.
> 4. A utilização de sensores para obtenção de dados quase em tempo real poderia ajudar a criar uma economia de atração (*pull economy*) com espirais de resultados positivos, devido à otimização e aos incentivos aos comportamentos de consumidores e cidadãos. Isso significa que a IoT pode ser muito importante na abordagem de problemas sistêmicos, tais como o uso eficiente da energia, os sistemas de tráfego, as emissões globais, entre outros.
> 5. A IoT envolve o impacto social do emprego e das competências quando combinada com a IA e a robótica, uma vez que reduz a necessidade de trabalhos manuais ou rotineiros. No entanto, costuma-se imaginar que os principais riscos dos sistemas de IoT são aqueles relacionados à segurança cibernética, em razão da falta de dispositivos seguros e da falta de padrões definidos para a transferência de dados entre países.[215]

Segundo Gartner, empresa especializada em consultorias e pesquisas no ramo da tecnologia, no estudo Top Strategic IoT Trends and Technologies Through 2023", se analisou as principais tendências e tecnologias estratégicas para a Internet das Coisas (IoT) até 2023:

> 1. Inteligência artificial (IA): cada vez mais, IA se consolida como uma tendência que veio para ficar, estima-se que até 2021, haverá mais de 25 bilhões de "coisas" conectadas ao redor do mundo. E são elas e o gigantesco volume de dados que produzem, os combustíveis que alimentam a Internet das Coisas. Também a junção entre IA e IoT é um potente catalisador de resultados que, se aplicado de forma sistemática e estratégica, promete alavancar a escalabilidade dos projetos ainda mais rapidamente.
> 2. IoT social, legal e ética: com o avanço da IoT e o seu amplo uso, uma série de questões sociais, legais e éticas passam a ganhar relevância, tais como: propriedade dos dados e as deduções feita a partir deles; tendência algorítmica; privacidade e conformidade com regulamentos como RGPD e LGPD.
> 3. Valor da informação: cada vez mais, a monetização de dados ganha valor. A teoria da *infonomics*[216] leva essa monetização de dados ainda mais

[215] SCHWAB, Klaus; DAVIS, Nicholas. **Aplicando a quarta revolução industrial**. Tradução: Daniel Moreira Miranda. São Paulo: Edipro, 2018, p.161-162.

[216] A infonomia é valorização e tratamento da informação como um ativo e transmissão de dados, ou seja, trata da disciplina emergente de gestão e contabilização de informações com o mesmo rigor e formalidade ou semelhante a outros ativos e passivos tradicionais (como ativos financeiros, físicos e intangíveis e capital humano). A infonomia postula que a informação em si atende a todos os critérios dos ativos formais da empresa e, embora ainda não seja reconhecida pelo GAAP, é cada vez mais responsabilidade das organizações se comportar como se a informação fosse um ativo real.

> adiante, vendo-a como um ativo comercial estratégico. Até 2023, a compra e venda de dados da IoT tornar-se-ão parte essencial de muitos sistemas de IoT.
> 4. *Hardware* confiável e sistema operacional: a segurança é a área mais significativa de preocupação técnica para as organizações que implantarem sistemas IoT. Isso porque as organizações geralmente não têm controle sobre a origem e a natureza do *software* e do *hardware* que estão sendo utilizados nas iniciativas de IoT. Até 2023, a expectativa é de que novas combinações de *hardware* e *software* que, juntas, criem sistemas de IoT mais confiáveis e seguros.
> 5. A governança da IoT: À medida que a IoT continuar a se expandir, a necessidade de uma estrutura de governança que garanta o comportamento apropriado na criação, armazenamento, uso e exclusão de informações relacionadas a projetos de IoT se tornará cada vez mais importante.[217]

De fato, o nível de conectividade do ecossistema tecnológico da Internet das Coisas está mais fortemente relacionado aos operadores de rede móvel que oferecem conectividade de celulares padrão. Um pequeno número de *startups* bem financiadas definiu esse nível do ecossistema tecnológico como alvo e avançou em subsegmentos como conectividade de grande alcance e baixa potência. A tecnologia de conectividade ocupa um mercado ainda em expansão e muito influenciado pela padronização internacional nesse nível de tecnologia. Também surgiram ferramentas computacionais e modelos analíticos complementares para interpretar, visualizar e produzir *insights* a partir de dados de equipamentos. Juntas, essas plataformas proliferaram e se desenvolveram nos últimos cinco anos, hoje simplificando a integração entre aparelhos e a implementação de aplicações – uma perspectiva de crescimento favorável para os principais participantes do mercado.[218]

A título de curiosidade, segundo estudo desenvolvido pelo Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), em parceria com o Banco Nacional de Desenvolvimento Econômico e Social (BNDES), estima-se que o mercado de internet das coisas deve injetar US$ 50 bilhões (cerca de R$ 200 bilhões) à economia brasileira até 2025, quantia que pode chegar a US$ 200 bilhões (cerca de R$ 800 bilhões).[219]

---

[217] ABINC. **A Gartner identificou as dez principais tecnologias e tendências de IoT.** Disponível em: < https://abinc.org.br/a-gartner-identificou-as-10-principais-tecnologias-e-tendencias-de-iot/>. Acesso em: 13 set. 2020.
[218] DAHLQVIST, Fredrik. et al. Growwing opportunities in the internet of things. **McKinsey&Company.** Disponível em: < https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things/pt-br>. Acesso em: 13 set. 2020.
[219] Revista CIAB - FEBRABAN. 2019. **Sofisticação abre as portas para o 'banco das coisas'.** Disponível em: < https://noomis.febraban.org.br/temas/internet-das-coisas/sofisticacao-abre-as-portas-para-o-banco-das-coisas>. Acesso em: 13 set. 2020.

Antes de seguir adiante, vale ressaltar que em 26 de junho de 2019, foi publicado o Decreto Federal nº 9.854 instituindo o Plano Nacional de Internet das Coisas dispondo sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas nos termos que, resumidamente, seguem:

> O Plano foi instituído na finalidade de implementar e desenvolver a Internet das Coisas (IoT) no país, com base na livre concorrência e na livre circulação de dados, observadas as diretrizes de segurança da informação e de proteção de dados pessoais, tem como objetivos: (i) melhorar a qualidade de vida das pessoas e promover ganhos de eficiência nos serviços; (ii) promover a capacitação profissional relacionada ao desenvolvimento de aplicações de IoT e a geração de empregos na economia digital; (iii) incrementar a produtividade e fomentar a competitividade das empresas brasileiras desenvolvedoras de IoT; (iv) buscar parcerias com os setores público e privado para a implementação da IoT; e (v) aumentar a integração do país no cenário internacional nos moldes especificados. O Decreto Federal estabelece, ainda, os seguintes temas que integrarão plano de ação destinado a identificar soluções para viabilizar o Plano Nacional de Internet das Coisas: (i) ciência, tecnologia e inovação; (ii) inserção internacional; (iii) educação e capacitação profissional; (iv) infraestrutura de conectividade e interoperabilidade; (v) regulação, segurança e privacidade; e (vi) viabilidade econômica. Além do mais, segundo este Decreto Federal, considera-se: (i) Internet das Coisas (IoT): a infraestrutura que integra a prestação de serviços de valor adicionado com capacidades de conexão física ou virtual de coisas com dispositivos baseados em tecnologias da informação e comunicação existentes e nas suas evoluções, com interoperabilidade; (ii) coisas: objetos no mundo físico ou no mundo digital, capazes de serem identificados e integrados pelas redes de comunicação; (iii) dispositivos: equipamentos ou subconjuntos de equipamentos com capacidade mandatória de comunicação e capacidade opcional de sensoriamento, de atuação, de coleta, de armazenamento e de processamento de dados; e (iv) serviço de valor adicionado: atividade que acrescenta a um serviço de telecomunicações que lhe dá suporte e com o qual não se confunde novas utilidades relacionadas ao acesso, ao armazenamento, à apresentação, à movimentação ou à recuperação de informações, nos termos que menciona.[220]

Cabe destacar, também, que o Plenário do Senado aprovou no dia 19/11/2020, o PL nº 6.549/2019, Projeto de Lei que tem o objetivo de incentivar a Internet das Coisas. Esse projeto reduz a zero as taxas de fiscalização de instalação e as taxas de fiscalização de funcionamento dos sistemas de comunicação máquina a máquina[221]. A isenção tributária tem prazo de cinco anos a partir de janeiro de

---

[220] PRICE WATERHOUSE COOPERS (PWC). **Plano Nacional de Internet das Coisas - Decreto Federal nº 9.854/2019.** Disponível em: < https://www.pwc.com.br/pt/sinopse-legislativa/outros-assuntos/plano-nacional-internet-coisas-decreto-federal-9854-2019.html>. Acesso em: 13 set. 2020.

[221] São considerados sistemas máquina a máquina os dispositivos que, sem intervenção humana, utilizam redes de comunicações para transmitir dados a aplicações remotas para monitorar, medir e controlar o próprio dispositivo, o ambiente ao seu redor ou sistemas de dados a ele conectados por meio dessas redes. Na agricultura, por exemplo, sensores em máquinas agrícolas podem transmitir

2021. O texto também dispensa a licença para esses equipamentos funcionarem. Dispositivos com conectividade 5G também estarão isentos.

É importante observar, ainda, que no que diz respeito ao setor financeiro, a IoT será essencial para transformar os negócios e manter as instituições competitivas no mercado nos próximos anos. Na visão de analistas, a internet das coisas ganhará ainda mais importância na estratégia de negócios das instituições de serviços financeiros com a chegada da rede 5G, já que essa tecnologia deve impulsionar o uso massivo de IoT e a oferta de produtos e serviços inovadores e mais personalizados. Por meio da IoT, os bancos, inclusive os digitais, poderão ter informações do cliente desde quando ele entra na agência ou no aplicativo, por exemplo, e poderão prestar um atendimento mais personalizado. Logo, a Internet das Coisas está preparando o caminho para a integração bem sucedida da tecnologia no setor financeiro, reduzindo os riscos e aumentando o valor do cliente.

Inclusive, o que se vê é que no Brasil a IoT começa a ser usada em grande escala pelas *fintechs* (*startups* financeiras). Estas empresas estão em massa recorrendo à Internet das Coisas para vender mais e oferecer melhores serviços financeiros aos clientes. Um dos focos do uso da IoT em transações financeiras são os serviços de pagamentos e recebimentos feitos pelas instituições. Companhias nacionais especializadas na Internet das Coisas, como a DEV Tecnologia, já estão trabalhando no desenvolvimento de *hardware* e *software* especialmente para tais tarefas. E os clientes que elas terão não serão poucos, no Brasil e no restante do mundo. Além disso, as f*intechs*, estão usando IoT e *blockchain* para construir sua cadeia de valor. Um exemplo é a PINbank, *startup* que oferece um banco virtual aos seus clientes. Ricardo Barletti, seu CEO, fala a respeito: “A PINbank já vem utilizando IoT há alguns anos em seus aplicativos. Para nós a utilização de soluções *mobile* para pagamentos ou outros serviços já é uma realidade, e para tanto dependemos da Internet das Coisas. É algo que só vai se acentuar”, acredita ele.

A título de curiosidade, a partir de 2021, o BNDES (Banco Nacional de Desenvolvimento Econômico e Social) e a Qualcomm, fabricante americana de *chips*

---

para um computador informações sobre o solo, orientando as ações de plantio, correção de acidez e irrigação da terra.

para celulares, vão investir em *startups* que atuam com tecnologia de IoT (internet das coisas).[222]

Por certo, a Internet das Coisas – provavelmente é a aplicação mais transformadora e impressionante dentre as tecnologias inovadoras hoje disponível para consumidores e instituições.[223] Pois, cria valor por meio de duas alavancas econômicas principais: geração de receita adicional e aumento da eficiência operacional; redução de custos. Assim, novas formas de interação com os clientes podem ser criadas, como assistência em tempo real, além de novos produtos e serviços de melhor qualidade que podem ser desenvolvidos a partir da coleta e da análise de informações de padrões de uso e da experiência do cliente. Além disso, determinados tópicos devem ser mais bem explorados para que a internet das coisas de fato atinja seu máximo impacto socioeconômico, o que inclui a responsabilidade por dados, segurança, privacidade, e *hardware* de melhor qualidade com baixo consumo de energia. Ou seja, baixo custo e melhor conectividade.

Contudo, embora a IoT ofereça grande oportunidades, especialmente no setor de serviços financeiros, há desafios que precisam ser abordados, como por exemplo: (a) Comércio de alta frequência: o comércio de algorítmico e de alta frequência (HFT) pode ser automatizado com o uso da IoT e assim, eliminar o envolvimento humano, permitindo o uso mais abrangente de dados algorítmicos em tempo real, mais rápido e preciso ;e (b) Gestão de dados: a falta de gestão de dados especialmente no setor financeiro, que exige integridade e processamento cuidadoso, pode causar a interrupção do fluxo de informações.[224]

Com base nessas informações, pode-se concluir que a questão central gira em torno de como “pegar carona” nessas novas tecnologias para nelas embarcar soluções que empoderem o cidadão com um controle mais efetivo e seguro sobre seus dados. Essas tendências tecnológicas estão mostrando seu potencial nessa nova realidade, nos dando uma pista de como podemos seguir com o

---

[222] Revista CIAB - FEBRABAN. 2020. **Fundo de investimento vai acelerar startups de IoT.** Disponível em: < https://noomis.febraban.org.br/noomisblog/fundo-de-investimento-vai-acelerar-startups-de-iot>. Acesso em: 13 set. 2020.

[223] LAMARRE, Eric; MAY, Brett. Ten trends shaping the Internet of things business landscape. **McKinsey&Company.** Disponível em: < https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/ten-trends-shaping-the-internet-of-things-business-landscape/pt-br>. Acesso em: 13 set. 2020.

[224] RUBINI, Agustin. **A Fintech em um Flash**. Tradução: Fernanda Belokurows. Babelcube Inc., 2017. Livro eletrônico, não paginado.

direcionamento da nossa busca pela transformação digital ideal.[225] Dessa forma, o que se percebe é que o avanço dessas novas tecnologias disruptivas está impulsionando uma mudança de paradigma no mercado financeiro mundial e brasileiro, que cada vez mais investe no uso de tecnologias inovadoras, conforme se verifica nos dados, da FEBRABAN em 2020, onde: aumentou em 72% o investimento relacionado a IA; 35% relacionado ao *Blockchain* e 20% relacionado a *IoT*.

Assim, a previsão, para os próximos anos é que essas tecnologias devem ser desenvolvidas, cada vez mais, para atender as necessidades e exigências do mercado, na medida em que agilidade, eficiência e competitividade são requisitos indispensáveis para o crescimento.

Entendida a dinâmica acerca da transformação digital, quarta revolução industrial, dados e as novas tecnologias, cabe agora, enfrentar, ainda, a questão do Mercado Financeiro, *Startups* e *Fintechs/*Bancos Digitais. Para a devida compreensão, deve-se fazer uma análise sobre o assunto, questionando-se alguns pontos importantes, como se verá a seguir.

2.5 MERCADO FINANCEIRO

É importante ressaltar que para melhor abordagem do tema será apresentada, de maneira clara e objetiva, algumas noções básicas sobre o Mercado Financeiro e o Sistema Financeiro Nacional, para melhor compreensão do assunto.

O mercado financeiro ou setor financeiro, em sentido amplo, abrange o mercado bancário (mercado financeiro em sentido estrito), o de câmbio e o de capitais (mercado de valores mobiliários). Caracterizando-se, assim, pela chamada intermediação financeira, entendida como a operação na qual determinada instituição é, simultaneamente, sujeito ativo e passivo: (a) tomando recursos emprestado dos poupadores (operação passiva) e comprometendo-se a devolvê-los, nas condições contratuais e podendo implicar o pagamento de juros; (b)

[225] Revista CIAB - FEBRABAN. 2020. **Novo mundo:** quais tendências vão te guiar? Disponível em: < https://noomis.febraban.org.br/especialista/gustavo-fosse/novo-mundo-quais-tendencias-vao-te-guiar?pesquisa=internet%20das%20coisas>. Acesso em: 13 set. 2020.

emprestando estes recursos para novos tomadores (operação ativa), tendo direito de cobrá-los acrescidos de juros.[226]

A vista disso, o mercado financeiro pode ser dividido em quatro segmentos: mercado monetário, mercado de câmbio, mercado de capitais e mercado de crédito, como se pode observar na (figura 2):

Figura 2 – Divisão do Mercado Financeiro

Fonte: Top-CVM[227]

É curioso notar que recentemente se incluiu nessa lista as *fintechs,* que hoje, também compõem o mercado financeiro e que será analisada mais adiante.

Cabe ressaltar, que o mercado de capitais tem uma grande importância no desenvolvimento do país, pois estimula a poupança e o investimento produtivo, o que é essencial para o crescimento de qualquer sociedade econômica moderna.[228]

Nesse contexto, o Sistema Financeiro Nacional (SFN) é o conjunto de instituições e instrumentos que viabilizam o fluxo financeiro entre os poupadores e os tomadores na economia,[229]que integram o mercado financeiro. Ou seja, é por

---

[226]TOP-DIREITO DO MERCADO DE VALORES MOBILIARIOS. Comissão de Valores Mobiliários, Comitê - Consultivo de Educação. 1º ed. Rio de Janeiro: CVM, 2017. Disponível em: < https://www.investidor.gov.br/portaldoinvestidor/export/sites/portaldoinvestidor/publicacao/Livro/Livro_top_Direito.pdf>. Acesso em: 26 jun. 2020.p. 34

[227]TOP-DIREITO DO MERCADO DE VALORES MOBILIARIOS. Comissão de Valores Mobiliários, Comitê - Consultivo de Educação. 4º ed. Rio de Janeiro: CVM, 2019. Disponível em: < https://www.investidor.gov.br/portaldoinvestidor/export/sites/portaldoinvestidor/publicacao/Livro/livro_TOP_mercado_de_valores_mobiliarios_brasileiro_4ed.pdf>. Acesso em: 26 jun. 2020.p.30

[228]TOP-DIREITO DO MERCADO DE VALORES MOBILIARIOS. Comissão de Valores Mobiliários, Comitê - Consultivo de Educação. 4º ed. Rio de Janeiro: CVM, 2019. Disponível em: < https://www.investidor.gov.br/portaldoinvestidor/export/sites/portaldoinvestidor/publicacao/Livro/livro_TOP_mercado_de_valores_mobiliarios_brasileiro_4ed.pdf>. Acesso em: 26 jun. 2020.p.35

[229]TOP-DIREITO DO MERCADO DE VALORES MOBILIARIOS. Comissão de Valores Mobiliários, Comitê - Consultivo de Educação. 4º ed. Rio de Janeiro: CVM, 2019. Disponível em: < https://www.investidor.gov.br/portaldoinvestidor/export/sites/portaldoinvestidor/publicacao/Livro/livro_TOP_mercado_de_valores_mobiliarios_brasileiro_4ed.pdf>. Acesso em: 26 jun. 2020.p.29

meio do sistema financeiro que as pessoas, as empresas e o governo circulam a maior parte dos seus ativos, pagam suas dívidas e realizam seus investimentos.[230]

O SFN é organizado por agentes normativos, supervisores e operadores. Os órgãos normativos determinam regras gerais para o bom funcionamento do sistema. As entidades supervisoras trabalham para que os integrantes do sistema financeiro sigam as regras definidas pelos órgãos normativos. Os operadores são as instituições que ofertam serviços financeiros, no papel de intermediários.

Os principais operadores do SFN são: (a) instituições financeiras captadoras de depósito à vista (bancos comerciais, bancos múltiplos com carteira comercial e cooperativas de crédito); (b) bancos de investimento; (c) corretoras e distribuidoras de valores; (d) corretoras de câmbio; (e) bolsas de valores e mercadorias; (f) *Clearing houses* (entidades de compensação e liquidação); (g) sociedades seguradoras; (h) sociedades de capitalização; (i) entidades abertas de previdência complementar; (j) entidades fechadas de previdência complementar.[231]

A estrutura do Sistema Financeiro Nacional (SFN) foi definida pela Lei nº 4.595, de 31 de dezembro de 1964, que em seu Art. 1º indicou seus principais integrantes:

Art. 1º O Sistema Financeiro Nacional, estruturado e regulado pela presente Lei, será constituído: I - do Conselho Monetário Nacional; II - do Banco Central da República do Brasil ou Banco Central do Brasil; III - do Banco do Brasil S. A.; IV - do Banco Nacional do Desenvolvimento Econômico; V - das demais instituições financeiras públicas e privadas.[232]

Os órgãos normativos do SFN são: o Conselho Monetário Nacional (CMN), o Conselho Nacional de Seguros Privados (CNSP) e o Conselho Nacional de Previdência Complementar (CNPC). São todos órgãos colegiados e integrantes do Poder Executivo da União. Estes conselhos possuem poder normativo, ou seja, editam normas gerais para os agentes e participantes do mercado, mas sob os

---

[230]BANCO CENTRAL DO BRASIL. **Sistema Financeiro nacional (SFN).** Disponível em: < https://www.bcb.gov.br/estabilidadefinanceira/sfn>. Acesso em: 26 jun. 2020.

[231]TOP-DIREITO DO MERCADO DE VALORES MOBILIARIOS. Comissão de Valores Mobiliários, Comitê - Consultivo de Educação. 1º ed. Rio de Janeiro: CVM, 2017. Disponível em: < https://www.investidor.gov.br/portaldoinvestidor/export/sites/portaldoinvestidor/publicacao/Livro/Livro_top_Direito.pdf>. Acesso em: 26 jun. 2020.p. 40-41

[232]TOP-DIREITO DO MERCADO DE VALORES MOBILIARIOS. Comissão de Valores Mobiliários, Comitê - Consultivo de Educação. 1º ed. Rio de Janeiro: CVM, 2017. Disponível em: < https://www.investidor.gov.br/portaldoinvestidor/export/sites/portaldoinvestidor/publicacao/Livro/Livro_top_Direito.pdf>. Acesso em: 26 jun. 2020.p. 38

limites da legalidade, ou seja, da lei em sentido estrito (ato emanado do poder legislativo).[233]

O Banco Central, seguindo diretrizes emitidas pelo Conselho Monetário Nacional (CMN), tem o papel de regulador, juntamente com a Comissão de Valores Mobiliários (CVM)[234], nas suas respectivas esferas de competência atuando no sentido de converter as políticas estabelecidas em regras a serem aplicadas ao Fundo Monetário Internacional (IMF), além de adequar o arcabouço normativo brasileiro, quando relevante, ao que recomendam os organismos internacionais concernentes, como é o caso do Comitê de Pagamentos e Infraestruturas do Mercado do Banco de Compensações Internacionais (CPMI/BIS) e do Comitê Técnico da Organização Internacional de Comissões de Valores (TC/IOSCO).[235]

Entendido as noções básicas do Mercado Financeiro e o Sistema Financeiro Nacional passamos agora a ver o mercado financeiro em relação a inovação digital[236] e ao momento atual, de dúvidas, inseguranças e incertezas por conta da pandemia do Covid-19.

Por décadas, os bancos tiveram que competir primariamente com outros bancos. Esses eram os tempos de abertura em massa de agências, campanhas de *marketing* audaciosas e competição contínua pela poupança mais rentável.[237]

Nos primeiros anos desse milênio e, principalmente, após o sentimento de desconfiança no mercado financeiro ante a crise de 2008, vimos a combinação do crescimento, popularização e barateamento de novas tecnologias aliar-se à demanda dos usuários por melhores experiências de consumo e serviços menos burocráticos e mais transparentes. A soma desses fatores influenciou o surgimento de produtos e serviços financeiros totalmente novos. Passamos, então, a ter o vislumbre de um mercado financeiro cada vez mais desintermediado e menos dependente das antigas estruturas, além do consequente surgimento de novos

---

[233]TOP-DIREITO DO MERCADO DE VALORES MOBILIARIOS. Comissão de Valores Mobiliários, Comitê - Consultivo de Educação. 1º ed. Rio de Janeiro: CVM, 2017. Disponível em: < https://www.investidor.gov.br/portaldoinvestidor/export/sites/portaldoinvestidor/publicacao/Livro/Livro_top_Direito.pdf>. Acesso em: 26 jun. 2020.p. 39

[234] Comissão de Valores Mobiliários é entidade supervisora do mercado de capitais.

[235]BANCO CENTRAL DO BRASIL. **Infraestruturas do mercado financeiro.** Disponível em: < https://www.bcb.gov.br/estabilidadefinanceira/infraestruturamercado>. Acesso em: 26 jun. 2020.

[236] Inovação digital é o uso da tecnologia digital durante o processo de inovar. Pode ser usada para descrever, total ou parcialmente, o resultado da inovação, mudando radicalmente a natureza e a estrutura de novos produtos e serviços, gerando criação de valor, caminhos novos, coletivos de inovação.

[237]Susanne; BARBERIS, Janos. **A Revolução Fintech:** o manual das startups financeiras. Tradução: Samantha Batista. Rio de janeiro: Alta Books, 2017, pag.13

entrantes em um ambiente anteriormente dominado pelos bancos.[238]O tempo em que as instituições financeiras podiam juntar seus serviços sem transparência e ainda desfrutar de lealdade total de seus clientes está chegando ao fim. [239]

O ano de 2020 termina com as instituições financeiras de ponta apostando, cada vez mais, na consolidação dos canais *on-line* e móveis como principais meios de interação com seus clientes. A disponibilidade dos serviços digitais é uma exigência crescente. Nesse aspecto, as empresas do setor financeiro competem não apenas entre si, mas com a economia digital como um todo,[240] afetando economias inteiras, acelerando processos e influenciando de forma significativa no comportamento do consumidor.

Tendo em vista os avanços tecnológicos identificados no mercado brasileiro, que possibilitam, entre outros benefícios, uma redução na burocracia e uma maior agilidade na prestação dos serviços e no atendimento aos clientes, o Conselho Monetário Nacional (CMN) e o Banco Central do Brasil (BACEN)[241] têm caminhado para adaptar suas normas e possibilitar uma atuação mais concentrada das instituições financeiras por eles reguladas, por meios eletrônicos.[242]

Os principais bancos de varejo do mundo gozam de enormes vantagens, inclusive em termos de sua base de clientes coletiva e dos dados que possuem de seus clientes. Esses “bancos prósperos” migrarão a maioria de seus clientes para seus próprios serviços bancários digitais. Eles se reposicionarão na cadeia de valor, passando de fornecedores de infraestrutura e produtos para o coração do relacionamento com o cliente em um ambiente digital seguro e holístico. Com efeito, se tornarão lojas de aplicativos financeiros apresentando uma gama de soluções financeiras de diferentes provedores. Ao fazer isso, permanecerão relevantes para os clientes como uma fonte única para as melhores soluções financeiras globais.[243]

---

[238]DINIZ, Bruno. **O Fenômeno *Fintech*:** tudo sobre o movimento que está transformando o mercado financeiro no Brasil e no mundo. Rio de Janeiro: Alta Books, 2019. p.2

[239]CHISHTI, Susanne; BARBERIS, Janos. **A Revolução Fintech:** o manual das startups financeiras. Tradução: Samantha Batista. Rio de janeiro: Alta Books, 2017. p.12

[240] SIMPLY. **Tendências do mercado financeiro para 2020.**Disponível em: < https://rdstation-static.s3.amazonaws.com/cms%2Ffiles%2F18483%2F1578600779Ebook_Tendncias_do_Mercado_Financeiro_Para_2020.pdf >. Acesso em: 26 jun. 2020.

[241] Banco Central do Brasil é entidade supervisora do mercado financeiro.

[242]OIOLI, Erik Frederico. **Manual de direito para startups**.2. ed. ver., atual. e ampl. São Paulo: Thomson Reuters, 2020. p.201.

[243]CHISHTI, Susanne; BARBERIS, Janos. **A Revolução Fintech:** o manual das startups financeiras. Tradução: Samantha Batista. Rio de janeiro: Alta Books, 2017. Pag.8

Assim, o momento não é de pequenas melhorias aqui ou ali, mas de uma completa transformação digital, que rapidamente torna obsoletos processos e estruturas tradicionais, definindo novos modos de lidar com as questões do dia a dia em finanças. Essa transformação tem um caráter absolutamente amplo, pois representa uma mudança cultural tanto para quem fornece, quanto para quem consome produtos e serviços financeiros.[244]

A pandemia do COVID-19 afetou todos os setores produtivos, mas para os bancos pode servir como uma oportunidade para acelerar a transformação digital.[245] A crise sanitária contribuiu para acelerar mais ainda a transformação digital no setor financeiro. Na visão de Dantas, do BTG Pactual, toda crise exige mudanças. Porém, o executivo avalia que o setor financeiro, por ser um dos que mais investe em tecnologia, estava mais preparado para atender os clientes nesse momento de mudança de comportamento em relação ao uso de plataformas digitais.[246] A transformação digital não tem nada a ver com projetos, funções ou processos. Trata-se de repensar o negócio e reconstruí-lo a partir da sua essência,[247] ou seja, transformação digital, não tem a ver com tecnologia, tem a ver com estratégia e novas maneiras de pensar.[248]

Como referência para esse estudo, primeiramente foi utilizada a pesquisa FEBRABAN de tecnologia bancária de 2020, realizada pela Deloitte. A FEBRABAN, Federação Brasileira de Bancos é a principal entidade representativa do setor bancário brasileiro. Ela mostra com clareza na pesquisa a inevitável, contínua e crescente migração dos usuários para os canais digitais em tempos de pandemia do COVID-19. Um surpreendente dado, é que o *Mobile Banking* (transações bancárias realizadas através *Smartphones*), em 2019, tiveram um aumento de 19%, entre janeiro e abril; puxado pelo incremento de 41% nas transações com movimentação financeira tornando-se cada vez mais um canal chave para contratação de produtos

---

[244]SIMPLY. **Tendências do mercado financeiro para 2020.**Disponível em: < https://rdstation-static.s3.amazonaws.com/cms%2Ffiles%2F18483%2F1578600779Ebook_Tendncias_do_Mercado_Financeiro_Para_2020.pdf >. Acesso em: 26 jun. 2020.

[245]Revista CIAB - FEBRABAN. 2020. **O que realmente significa transformação digital?** Disponível em: < https://noomis.febraban.org.br/especialista/chris-skinner/o-que-realmente-significa-transformacao-digital>. Acesso em: 26 jun. 2020.

[246]FEBRABAN. **Pandemia do Covid-19 acelera uso dos canais digitais nos bancos**. Disponível em: < https://portal.febraban.org.br/noticia/3476/pt-br/>. Acesso em: 26 jun. 2020.

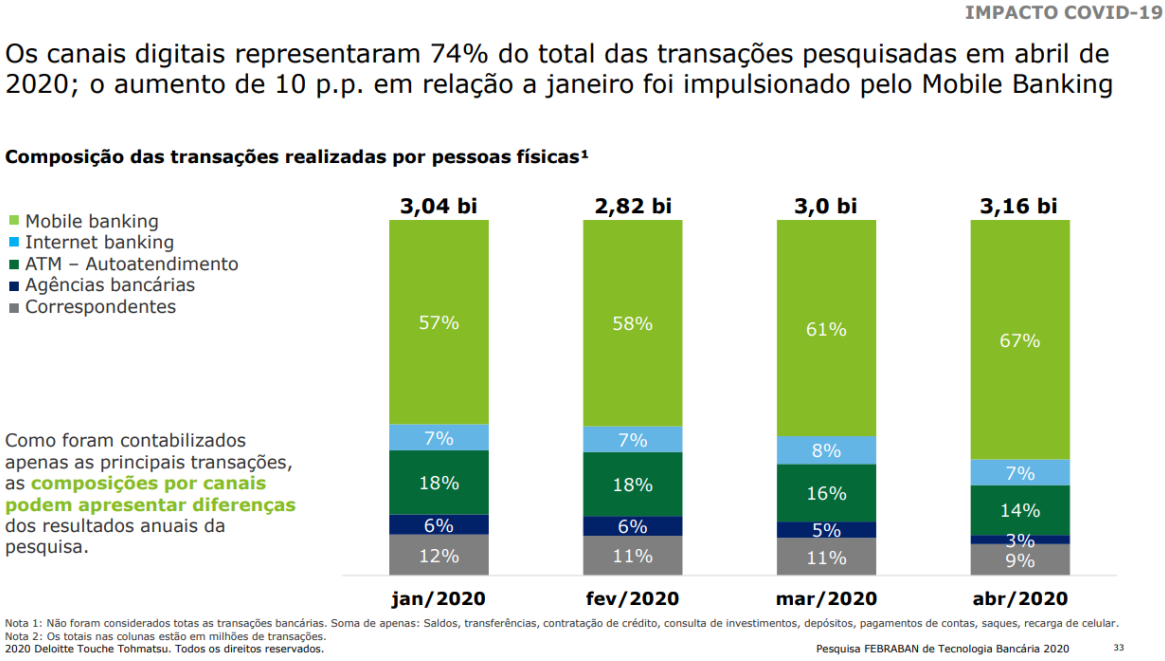
[247]Revista CIAB - FEBRABAN. 2020. **O que realmente significa transformação digital?** Disponível em: < https://noomis.febraban.org.br/especialista/chris-skinner/o-que-realmente-significa-transformacao-digital>. Acesso em: 26 jun. 2020.

[248]ROGERS, David L. **Transformação digital:** repensando o seu negócio para a era digital. Tradução: Afonso Celso da Cunha Serra. 1º ed. São Paulo: Autêntica Business, 2017, p.12.

e transações financeiras, com crescimento acentuado em operações de investimentos, seguros e depósitos virtuais. Além disso, percebe-se que os Bancos aumentaram em 48% os investimentos em tecnologia, tanto por *software* (58%), como por *hardware* (38%), com foco na conveniência para o cliente e na oferta de novos modelos de atendimento.[249]

No seguinte (gráfico 1), percebe-se os impactos da pandemia nas transações financeiras feitas por pessoas físicas pelos canais digitais – *internet* e *mobile banking* – responsáveis por 74% no mês de abril, após o início da quarentena e das medidas de isolamento social. Os *smartphones* representaram 67% das transações analisadas neste mês.[250]

Gráfico 1 – Evolução dos canais digitais



Fonte: Pesquisa FEBRABAN[251]

---

[249] FOSSE, Gustavo; BIAGINI, Sergio. **Pesquisa FEBRABAN de Tecnologia Bancária 2020. Ano-base 2019.** FEBRABAN, [S. l.], p. 1-57, 1 jan. 2020. Disponível em < https://cmsportal.febraban.org.br/Arquivos/documentos/PDF/Pesquisa%20Febraban%20de%20Tecnologia%20Banc%C3%A1ria%202020%20VF.pdf>. Acesso em 26 jun. 2020.

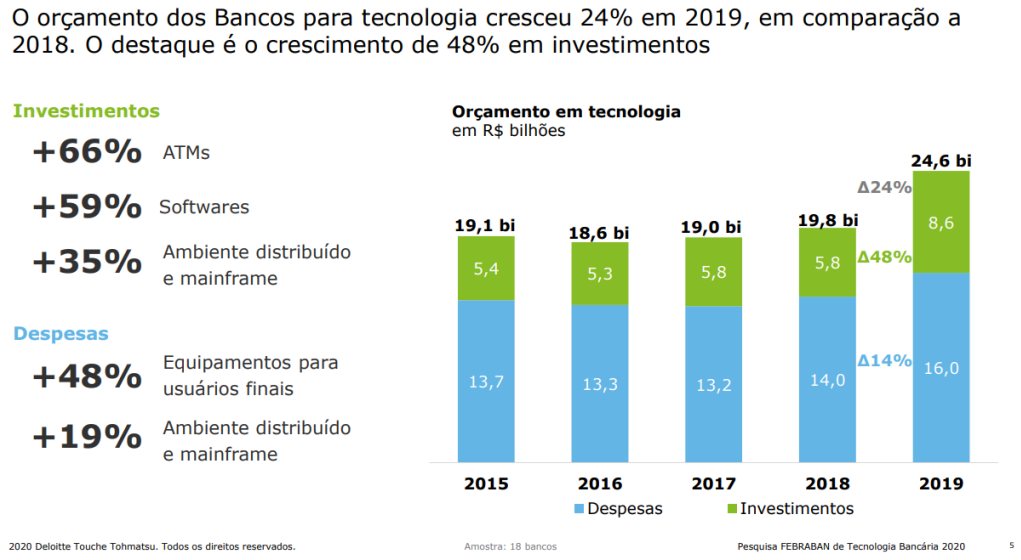
[250] Revista CIAB - FEBRABAN. 2020. **Canais digitais respondem por 74% das transações bancárias em abril**. Disponível em: < https://noomis.febraban.org.br/temas/inovacao/canais-digitais-respondem-por-74-das-transacoes-bancarias-em-abril>. Acesso em: 26 jun. 2020.

[251] FOSSE, Gustavo; BIAGINI, Sergio. **Pesquisa FEBRABAN de Tecnologia Bancária 2020. Ano-base 2019.** FEBRABAN, [S. l.], p. 1-57, 1 jan. 2020. Disponível em < https://cmsportal.febraban.org.br/Arquivos/documentos/PDF/Pesquisa%20Febraban%20de%20Tecnologia%20Banc%C3%A1ria%202020%20VF.pdf>. Acesso em 26 jun. 2020.

Dessa forma, um dos grandes desafios dos bancos para o período pós-pandemia é entregar plataformas digitais que atendam às expectativas dos clientes, que estão usando intensivamente as tecnologias durante a crise sanitária e que ficaram ainda mais exigentes, frente a esse ambiente de inseguranças e incertezas, onde cada vez mais, canais *on-line* seguem crescendo como principal meio de interação entre clientes e empresas; e em contrapartida canais tradicionais, como agências físicas e caixas eletrônicos passam a ocupar papel secundário.

Na mesma linha, chama atenção que a indústria bancária segue como o maior investidor privado em tecnologia, no Brasil e no mundo. O setor bancário brasileiro investiu R$ 8,6 bilhões em tecnologia em 2019, alta de 48% em relação ao ano anterior, quando os investimentos foram de R$ 5,8 bilhões. Somado às despesas, que cresceram 14% (de R$ 14 bilhões para R$ 16 bilhões), o orçamento total do setor chegou a R$ 24,6 bilhões, conforme esclarecido nos (gráficos 2 e 3) abaixo.[252]

Gráfico 2 – Total de investimentos com tecnologia (em R$ bilhões)

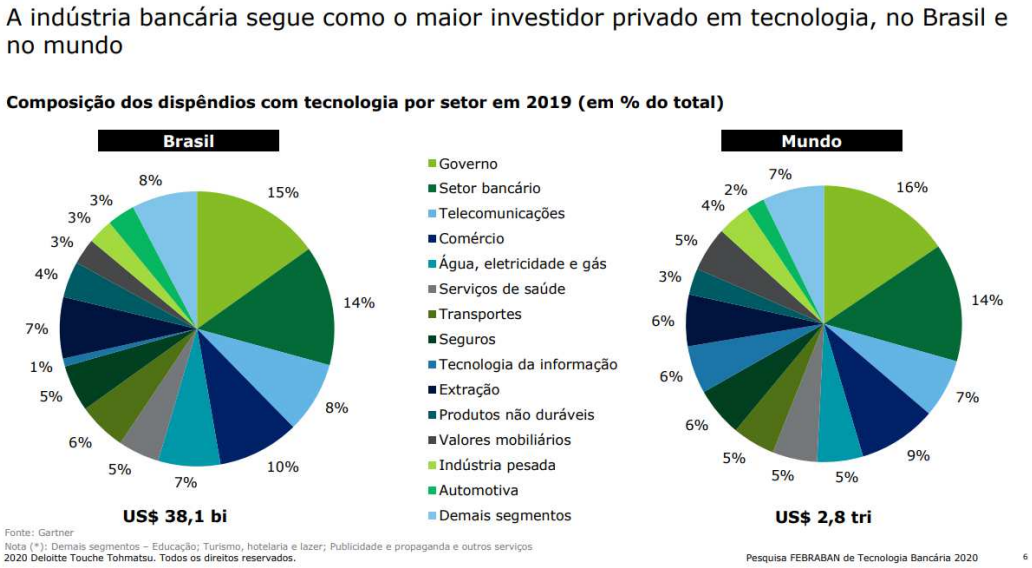


Fonte: Pesquisa FEBRABAN[253]

[252]FOSSE, Gustavo; BIAGINI, Sergio. **Pesquisa FEBRABAN de Tecnologia Bancária 2020. Ano-base 2019.** FEBRABAN, [S. l.], p. 1-57, 1 jan. 2020. Disponível em < https://cmsportal.febraban.org.br/Arquivos/documentos/PDF/Pesquisa%20Febraban%20de%20Tecnologia%20Banc%C3%A1ria%202020%20VF.pdf>. Acesso em 26 jun. 2020.

[253]FOSSE, Gustavo; BIAGINI, Sergio. **Pesquisa FEBRABAN de Tecnologia Bancária 2020. Ano-base 2019.** FEBRABAN, [S. l.], p. 1-57, 1 jan. 2020. Disponível em < https://cmsportal.febraban.org.br/Arquivos/documentos/PDF/Pesquisa%20Febraban%20de%20Tecnologia%20Banc%C3%A1ria%202020%20VF.pdf>. Acesso em 26 jun. 2020.

Gráfico 3 – Total de investimento com tecnologia, no Brasil e no mundo (em % do total)



Fonte: Pesquisa FEBRABAN[254]

Nesse sentido, cabe destacar uma pequena observação: a ampla adoção de novas tecnologias pelo mercado financeiro acabou causando, inicialmente, um efeito adverso do ponto de vista humano. Se por um lado toda essa tecnologia e investimentos serviram ao propósito de redução de custos e eficiência operacional, também é verdade que, por outro lado, provocou um distanciamento na antiga relação banco – cliente, tirando o foco do usuário. [255]

Em linhas gerais, o mercado financeiro, foi responsável por boa parte dos avanços tecnológicos de 2020. O Banco Central apresentou aos brasileiros o *Open Banking*, e em sintonia com a proposta do PIX, novo sistema de pagamento instantâneo, rápido, gratuito, dinâmico que chega ao mercado nacional para democratizar o acesso aos serviços financeiros e minimizar a burocracia comum desses sistemas agilizando assim pagamentos e transferências bancárias. O ano também foi marcado pela atuação das *fintechs*, que tiveram grande importância na contribuição para a inovação, ao apresentarem novas maneiras de integrar a tecnologia ao dia a dia das pessoas ao adotarem práticas e processos alinhados com as necessidades do momento.

---

[254]FOSSE, Gustavo; BIAGINI, Sergio. **Pesquisa FEBRABAN de Tecnologia Bancária 2020. Ano-base 2019.** FEBRABAN, [S. l.], p. 1-57, 1 jan. 2020. Disponível em < https://cmsportal.febraban.org.br/Arquivos/documentos/PDF/Pesquisa%20Febraban%20de%20Tecnologia%20Banc%C3%A1ria%202020%20VF.pdf>. Acesso em 26 jun. 2020.

[255]DINIZ, Bruno. **O Fenômeno *Fintech*:** tudo sobre o movimento que está transformando o mercado financeiro no Brasil e no mundo. Rio de Janeiro: Alta Books, 2019, p. 09-10.

Por certo, algumas importantes tendências se consolidaram no mercado financeiro em 2020. Entre elas, podemos citar: (a) Mercado digital; (b) Modelos de negócios inovadores; (c) Economia compartilhada; (d) *Blockchain*; (e) Foco nos dados do cliente; (f) Automação de processos; (g) Nuvem pública como infraestrutura básica; (h) Segurança; (i) Evolução dos órgãos reguladores.[256] Já para 2021 as previsões são as seguintes: (1) *People Centricity* (centralização nas pessoas): Internet de Comportamentos, Experiência total, Computação que melhora a privacidade; (2) *Location Independence* (independência de localização): Nuvem distribuída, Operações em qualquer lugar, Malha de segurança cibernética; (3) *Resilient Delivery* (entrega resiliente): Negócios inteligentes combináveis, Engenharia de IA, Hiperautomação.[257]

Nesse linear, entendido e definido, o mercado financeiro, é o momento de compreender melhor as *Startups*, conforme se discorrerá a seguir.

2.6 *STARTUPS*

Primeiramente, o termo *startup* ganhou notoriedade no final da década de 1990, com as chamadas empresas ".com", sobretudo no pujante Vale do Silício.[258]

Para tanto, definir uma *startup*, não é algo fácil, devido a diversidade de definições ou conceitos, por isso, a definição mais utilizada é a do autor Eric Ries, segundo o qual "uma *startup* é uma instituição humana projetada para criar novos produtos e serviços sob condições de extrema incerteza".[259] Outra definição parecida, dessa vez de Steve Blank, um dos pioneiros na área diz que "as condições de extrema incerteza têm relação com o caráter inovador do projeto que busca um modelo de negócio repetível e escalável". Diante dessas definições percebe-se que as *startups* não foram limitadas a apenas a um recorte baseado no uso de

---

[256]SIMPLY. **Tendências do mercado financeiro para 2020.** Disponível em: < https://rdstation-static.s3.amazonaws.com/cms%2Ffiles%2F18483%2F1578600779Ebook_Tendncias_do_Mercado_Financeiro_Para_2020.pdf >. Acesso em: 26 jun. 2020.

[257]SIMPLY. **Nove tendências tecnológicas para 2021.** Disponível em: < https://d335luupugsy2.cloudfront.net/cms%2Ffiles%2F18483%2F1605271418Ebook_Tendncias_Tecnolgicas_2021.pdf>. Acesso em: 19 out. 2020.

[258]OIOLI, Erik Frederico. **Manual de direito para startups**.2. ed. ver., atual. e ampl. São Paulo: Thomson Reuters, 2020, p. 13.

[259]RIES, Eric. **A startup enxuta:** como os empreendedores atuais utilizam a inovação contínua para criar empresas extremamente bem-sucedidas. Tradução: Texto Editores. São Paulo: Lua de Papel, 2012, p. 26. Disponível em: < https://edisciplinas.usp.br/pluginfile.php/4453282/mod_resource/content/1/a-startup-enxuta-eric-ries-livro-completo.pdf>. Acesso em: 26 jun. 2020.

Tecnologias de Comunicação e Informação (TIC), mas cabe ressaltar aqui que o uso das TIC está intimamente relacionado aos critérios e escalabilidade e replicabilidade exigidos para o enquadramento dentro do conceito de *startup*.[260]

Èderson Garin Porto, explica em sua obra que:

> *Startup* não é um novo tipo societário, nem uma instituição futurista. Qualquer negócio que se proponha a desenvolver uma ideia nova e que por essa razão a comercialização e o sucesso é cercado de incertezas pode ser considerado uma *Startup*.[261]

Acrescenta-se, também, a definição "*Lean Startup"* ou "Startup Enxuta" de Steve Blank dispõe que:

> A *startup* enxuta é uma organização temporária feita para buscar um modelo de negócios que possa ser reproduzido e ampliado, ou seja, metodologia aplicada aos negócios que preconiza a experimentação, a opinião do cliente e o projeto interativo em contraposição ao modelo tradicional, baseado no planejamento minucioso, na intuição e na concepção de um produto acabado desde o início.[262]

Com uma visão geral, Eric Ries afirma que: "Lean *Startup* ou Startup Enxuta é um conjunto de práticas para ajudar os empreendedores a aumentar suas chances de desenvolver uma *startup* de sucesso".[263]

Como o próprio termo *startup* sugere em sua tradução literal, estamos nos referindo a uma empresa em fase inicial ou de lançamento, ou seja, aquela em estágio inicial de organização da sua atividade.[264] Logo, *startups* são empresas em fase inicial que desenvolvem produtos, ou serviços inovadores, com potencial de rápido crescimento, cuja as principais características são: inovação; escalabilidade; repetibilidade; flexibilidade e rapidez.[265]

---

[260]ABSTARTUPS – Associação Brasileira de *Startups*. **Mapeamento *edtech* 2019.** Disponível em: < https://drive.google.com/file/d/1g2N2NfzMIddIw3dulHc0WCGLg_mhb_Nz/view>. Acesso em: 27 jun. 2020, p.09.

[261] PORTO, Éderson Garin. Manual jurídico da startup: como desenvolver projetos inovadores com segurança. 2.ed. ver. E atual. Porto Alegre: Livraria do Advogado, 2020, p.27.

[262]BLANK, Steve. **Why the lean start-up changes everything.** Harvard Business Review, v. 91, n. 5, p. 63-72, 2013.

[263]RIES, Eric. **A startup enxuta:** como os empreendedores atuais utilizam a inovação contínua para criar empresas extremamente bem-sucedidas. Tradução: Texto Editores. São Paulo: Lua de Papel, 2012, p. 26. Disponível em: < https://edisciplinas.usp.br/pluginfile.php/4453282/mod_resource/content/1/a-startup-enxuta-eric-ries-livro-completo.pdf>. Acesso em: 26 jun. 2020.

[264]OIOLI, Erik Frederico. **Manual de direito para startups**.2. ed. ver., atual. e ampl. São Paulo: Thomson Reuters, 2020, p. 15.

[265]ABSTARTUPS – Associação Brasileira de *Startups*. **O Momento da Startup Brasileira e o Futuro do Ecossistema de Inovação.** Disponível em: < https://abstartups.com.br/PDF/radiografia-startups-brasileiras.pdf>. Acesso em: 27 jun. 2020.

Em outras palavras, *startup*, é uma catalisadora que transforma ideias em produtos. À medida que os clientes interagem com os produtos, geram *feedback* e dados. O *feedback* é tanto qualitativo (por exemplo, o que gostam ou não) como quantitativo (por exemplo, quantas pessoas utilizam o produto e consideram que ele tem valor).[266]

É importante ressaltar ainda que a inovação[267], consiste na implantação de novas ideias que gerem valor, ou seja é uma estratégia que busca não apenas criar diferenciação de produtos que permitam agregar valor para consumidores, mas também a ampliação dos resultados por meio da escalabilidade da sua operação. Daí uma das razões por que muitas *startups* são associadas ao setor de tecnologia, pois é por meio dela, que conseguem alavancar suas receitas com baixo incremento de despesas operacionais, aumentando sua margem de lucro.[268]

Nota-se, portanto, que *startup* é uma empresa em fase inicial de desenvolvimento e busca pela inovação.[269] Nessa seara, percebe-se que quando se trata de agilidade, as *startups* têm uma vantagem sobre as grandes corporações. Uma corporação tem recursos, escala, energia e rotinas necessárias para executar um modelo de negócios comprovado com eficiência. A *startup* não possui nenhuma dessas opções, mas normalmente possui ideias promissoras, agilidade organizacional, vontade de correr riscos e aspirações de crescimento rápido. *Players* de *startups,* hoje, estão em uma situação que lhes permite trazer suas ideias ao mercado, em grande parte, por um custo mais baixo do que no início dos anos 2000. Além disso, todo um sistema de apoio de instituições está pronto para ajudar a dirigir um novo empreendimento nos seus primeiros dias.[270]

Em paralelo, é impossível deixar de mencionar que nesse momento de dúvida, insegurança e incerteza por conta da pandemia do Covid-19, moram

---

[266]RIES, Eric. **A startup enxuta:** como os empreendedores atuais utilizam a inovação contínua para criar empresas extremamente bem-sucedidas. Tradução: Texto Editores. São Paulo: Lua de Papel, 2012, p. 57. Disponível em: < https://edisciplinas.usp.br/pluginfile.php/4453282/mod_resource/content/1/a-startup-enxuta-eric-ries-livro-completo.pdf>. Acesso em: 26 jun. 2020.

[267] A inovação envolve não só as empresas de um sector e as suas decisões, mas também flui conhecimentos e processos de aprendizagem, a configuração institucional em que tais decisões são tomadas, e outros atores que estão ligados através de redes e processos de feedback.

[268]OIOLI, Erik Frederico. **Manual de direito para startups**.2. ed. ver., atual. e ampl. São Paulo: Thomson Reuters, 2020, p. 17.

[269]OIOLI, Erik Frederico. **Manual de direito para startups**.2. ed. ver., atual. e ampl. São Paulo: Thomson Reuters, 2020, p. 18.

[270]WEIBLEN, Tobias; CHESBROUGH, Henry W. Engaging with startups to enhance corporate innovation. California Management Review, v. 57, n. 2, p. 66-90, 2015.

diversas oportunidades para *startups* com cenários que elas já sabem atuar: com equipes enxutas, baixos custos, agilidade e potencial caminho de sucesso para negócios que antes não habitavam o universo digital. Obviamente, assim como toda situação de extremos, alguns setores se destacam em detrimento a outros, como por exemplo, soluções de educação, saúde, logística, finanças e telecomunicações em destaque. Afinal, mais do que nunca, a inovação é necessária para continuarem operando.[271]

Cabe destacar, ainda, que as empresas estão começando a enxergar as *startups* como parceiras e motores para impulsionar a inovação coorporativa. Mas, como atrair as *startups* afim de que figurem como parceiras da corporação? Destacam-se três pontos básicos: (a) Observar o ecossistema de *startups,* que está cada vez maior e mais disperso globalmente; (b) Demonstrar que a corporação pode agregar valor à *startup*, algo que se torna cada vez mais difícil diante das possibilidades existentes no mercado (investidores-anjo, incubadoras, venture capital, etc...); (c) Definir a relação que pretende ter com a *startup* levando em conta objetivos previamente traçados.[272]

Ainda, assim, é importante mencionar o Marco Legal das *Startups*, projeto de lei complementar 249/2020[273] que traz uma série de medidas para facilitar a criação de empresas de tecnologia, dar mais segurança jurídica aos investidores e até mesmo criar novos modelos de remuneração e contratação de pessoas. Entre as medidas mais esperadas pelos empreendedores está a criação de um novo modelo societário: a sociedade anônima simplificada. A partir da aprovação do Marco Legal das *Startups* será menos burocrático para um investidor conseguir capitalizar as *startups*. Além disso, os custos referentes à abertura de sociedade seriam reduzidos

---

[271]MURITIBA, José. **A resposta do ecossistema de startups à pandemia.** Disponível em: < https://www.jornaldocomercio.com/_conteudo/ge2/noticias/2020/05/738210-a-resposta-do-ecossistema-de-startups-a-pandemia.html>. Acesso em: 27 jun. 2020.

[272]WEIBLEN, Tobias; CHESBROUGH, Henry W. Engaging with startups to enhance corporate innovation. California Management Review, v. 57, n. 2, p. 66-90, 2015.

[273] Projeto de Lei Complementar 249/2020 institui o marco legal das startups e do empreendedorismo inovador. Apresentado pelo Poder Executivo no dia 20/10/2020, o texto começa a tramitar pela Câmara dos Deputados. Os objetivos do governo com a proposta incluem fomentar esse ambiente de negócios; aumentar a oferta de capital para investimento em startups; e disciplinar a licitação e contratação de soluções inovadoras pela administração pública. O projeto fixa outros requisitos para a empresa ser considerada startup: (i) ter faturamento bruto anual de até R$ 16 milhões no ano-calendário anterior ou de R$ 1,3 milhão multiplicado pelo número de meses de atividade no ano-calendário anterior, quando inferior a um ano; (ii) com até seis anos de inscrição no Cadastro Nacional da Pessoa Jurídica (CNPJ); (iii) e que atendam a um dos seguintes requisitos, no mínimo: declaração, em seu ato constitutivo ou alterador, de utilização de modelos de negócios inovadores; ou enquadramento no regime especial Inova Simples.

a zero, assim como o tempo de aprovação convertido a poucos dias, num processo totalmente digitalizado.[274]

Entendido e definido, o que é uma *startup*, é o momento de compreender melhor as *Fintechs*/Bancos digitais, conforme se discorrerá a seguir.

2.7 *FINTECHS*/BANCOS DIGITAIS

Conforme explorado anteriormente, a evolução tecnológica está em tudo, estimulando mudanças e apresentando novas oportunidades constantemente. No mundo das finanças não é diferente. Há pouco tempo, o setor bancário era baseado, quase que exclusivamente, em interações humanas entre clientes e gerentes, por exemplo. Hoje, com a *internet* e os *apps*, os canais que conectam usuário e instituição são muito variados e conferem autonomia ao cliente para cuidar das suas finanças. O acesso à tecnologia mudou o comportamento do usuário. Instituições tradicionais precisaram investir em inovação, no desenvolvimento de aplicativos, na modernização das políticas e canais de atendimento e na atualização de profissionais. É estranho pensar que, apesar de raramente envolver um encontro presencial, a tecnologia aproximou clientes e instituições. Tudo é mais direto e imediato. O usuário exige que respostas, interações e serviços sejam rápidos e precisos.[275]

Como se pode observar, estamos vivendo tempos de transformações significativas do setor bancário. Provavelmente podemos supor que os serviços bancários ao longo dos próximos dez anos experienciem um grau de mudança maior do que nos últimos cem anos. A inovação da tecnologia financeira começou a dar uma sacudida global no setor. Agora a questão mais importante permanece: os bancos serão ou não capazes de abraçar a inovação *Fintech* com sucesso? A *Fintech* está definida para ter um papel maior na sua vida do que pode esperar.[276]

---

[274] DISTRITO. ***Fintech*** **mining report 2020.** Disponível em: < https://rdstation-static.s3.amazonaws.com/cms%2Ffiles%2F65883%2F1593523598FinTech_Report_2020_v7.pdf?utm_campaign=resposta_automatica_da_landing_page_dataminer_fintech_report_-_edicao_2020&utm_medium=email&utm_source=RD+Station>. Acesso em: 19 ago. 2020.

[275] DISTRITO. ***Fintech*** **mining report 2020.** Disponível em: < https://rdstation-static.s3.amazonaws.com/cms%2Ffiles%2F65883%2F1593523598FinTech_Report_2020_v7.pdf?utm_campaign=resposta_automatica_da_landing_page_dataminer_fintech_report_-_edicao_2020&utm_medium=email&utm_source=RD+Station>. Acesso em: 19 ago. 2020.

[276] CHISHTI, Susanne; BARBERIS, Janos. **A Revolução Fintech:** o manual das startups financeiras. Tradução: Samantha Batista. Rio de janeiro: Alta Books, 2017. p.15

De igual modo, se fosse possível viajar no tempo e trazer uma pessoa de 2008 para os dias atuais, certamente essa se surpreenderia com as inovações alcançadas no setor dos serviços financeiros, provocadas por constantes transformações na Tecnologia da Informação (TI), no comportamento do consumidor e em seu estilo de vida. A inovação nos serviços e produtos financeiros, nesse breve espaço de um pouco mais de uma década, deu um salto gigantesco. Da inteligência artificial aos ativos digitais, é inegável que os rápidos avanços tecnológicos estão transformando o segmento financeiro no mundo todo, criando oportunidades e novos desafios.[277]

Embora ainda careçam de um ambiente regulatório mais definido, a emergência das *Fintechs* é fruto da combinação dessas mudanças na demanda por serviços financeiros e no ambiente tecnológico que caracterizam o ambiente da sexta onda de inovação no setor bancário.[278]

As ondas de inovação estão diretamente ligadas à introdução de automação nesses processos relacionados à execução de uma transação bancária. São seis as ondas de inovação: (a) Primeira onda: teve início em 1960, com a introdução de computadores de grande porte – *Mainframes.* Aumento do número de clientes leva ao crescimento do volume de transações processadas em *back-office* (processos mais internos do banco), para obter ganhos de escala e maior eficiência no registro contábil das transações; (b) Segunda onda: teve início ao final da década de 1970, com minicomputadores e a necessidade de processamento no nível da agência, implantação de sistemas *on-line*; (c) Terceira onda: automação das transações iniciadas por clientes - microcomputadores, demanda por autoatendimento, no ambiente da agência, através de caixa eletrônicos em locais públicos; (d) Quarta onda: teve início em meados da década de 1990, abriu a possiblidade do cliente interagir com o banco sem a necessidade de sair de sua casa ou escritório - *Home, office banking, internet banking*; maior interatividade e comodidade para clientes que já dispõem de computadores; (e) Quinta onda: teve início na primeira década dos anos 2000, representou uma oportunidade para diversificação dos canais bancários, com especial foco nos celulares e nos correspondentes bancários, com uso

---

[277]DINIZ, Bruno. **O Fenômeno *Fintech*:** tudo sobre o movimento que está transformando o mercado financeiro no Brasil e no mundo. Rio de Janeiro: Alta Books, 2019, p. 01.
[278]TIGRE, Paulo Bastos; PINHEIRO, Alessandro Maia. **Inovação em serviços na economia do compartilhamento.** São Paulo: Saraiva Educação, 2019, p.201.

estratégico de tecnologia da informação para ampliar a base tradicional de clientes por meio de parcerias com empresas não financeiras. Mercado concentrado em clientes de renda média e alta. Maior capilaridade e ubiquidade para expansão da rede de clientes. Mobilidade e convergência digital; (f) Sexta onda: uso de ferramentas sofisticadas (computação em nuvem, *Big Data*), ferramentas analíticas, redes sociais – tecnologias fundamentais para emergência das *Fintechs* – pagamento por serviço utilizado, agilidade compatível com ambiente de alta conectividade, pressão por preço em detrimento da fidelidade ao fornecedor. Desenvolvimento de tecnologia bancária fora do ambiente dos bancos, com produtos e serviços inovadores.[279]

Mas afinal de contas, o que são *fintechs*? E qual a sua importância e relevância para o mercado financeiro atual?

Diversas são as conceituações dadas as *fintechs*, mas não existi, atualmente uma conceituação única.

Nesse sentido, o termo *fintech* mescla os conceitos de finanças com tecnologia (em inglês, *financial technology*). Assim, o termo pode ser utilizado para se referir a processos, empresas e negócios que apliquem tecnologia para prestar serviços financeiros ou serviços relacionados a serviços financeiros. Muitas vezes, no Brasil esse termo é confundido ou utilizado de forma intercambiável com os termos “instituições de pagamento”.[280]

Segundo a FintechLab, consultoria especializada em inovação e *service design*, de iniciativa de *Clay Innovation*, as *fintechs* são iniciativas que aliam tecnologia e serviços financeiros trazendo inovações para pessoas e empresas. Isso se reflete em: melhores jornadas de utilização de produtos e serviços que trazem melhores experiências de uso; geração de inteligência a partir de volumes inimagináveis de dados e do conhecimento coletivo para otimizar as decisões; e integração dos diferentes elos do mercado de maneira muito mais eficiente, com menos falhas operacionais, aumentando a velocidade de transações e reduzindo custos.[281]

---

[279] TIGRE, Paulo Bastos; PINHEIRO, Alessandro Maia. **Inovação em serviços na economia do compartilhamento.** São Paulo: Saraiva Educação, 2019, p.190-193.
[280]OIOLI, Erik Frederico. **Manual de direito para startups**.2. ed. ver., atual. e ampl. São Paulo: Thomson Reuters, 2020, p.193.
[281]FINTECHLAB. **Report Fintechlab 2016.** Disponível em: < http://fintechlab.com.br/wp-content/uploads/2017/02/Report_FintechLab_2016_alta.pdf >. Acesso em: 26 jun. 2020.

Para maior compreensão a respeito das f*intech* passamos, então, a falar de sua origem, de seus primeiros impactos no mercado financeiro nacional e também a análise de pontos relevantes em que pese o assunto no cenário atual.

O nascimento e a ascensão das *Fintechs* estão profundamente enraizados na crise financeira e na erosão da confiança que ela gerou. A raiva das pessoas com o sistema bancário foi terreno fértil perfeito para a inovação financeira. Na hora certa, porque nativos digitais (também conhecidos como *millenials*[282] ou geração Y) estavam ficando velhos o bastante para serem clientes potenciais e suas preferências apontavam para serviços móveis que eles compreendiam e dominavam, em vez de bancários com quem não conseguiam se relacionar. Nesse cenário favorável, provedores de *Fintech* chegaram, oferecendo serviços novos a custos mais baixos, por meio de plataformas bem projetadas ou aplicativos móveis, mudando a maneira que as pessoas pagam, enviam dinheiro, emprestam e investem.[283]

No mesmo cenário, tivemos um primeiro *"boom"* de *fintechs* em um momento mais estável da economia. Muitas dessas empresas oferecem serviços semelhantes e são ligadas a grandes instituições financeiras, pela dificuldade em conseguir licenças para atuar de forma independente. Isso limita o quanto elas podem ser disruptivas. Hoje, com o PIX[284] (sistema de pagamentos instantâneos) e terminais POS que já aceitam mais de 10 QR Codes diferentes, estamos nos aproximando de uma ampla disputa pela aquisição de usuários.[285]

---

[282]A geração *millenium* (ou *millenials*), nascida a partir de 1990, representará 44% dos novos clientes bancários no Brasil em 2025, exigindo atenção especial, ou seja, são um novo perfil de clientes do sistema financeiro. Esses jovens tomaram conhecimento do mundo por meio da *internet* e veem pouco valor nas agências bancárias. Além disso, é um grupo menos fiel a marcas e mais confiante nos pares, o que abe possibilidades pouco exploradas pelos bancos que ainda participam das redes sociais de forma limitada. Bem informados e exigentes, eles têm maior poder de pressão pelo fato de criarem novas formas de relacionamento, novos hábitos de consumo e formas mais flexíveis de inserção no mundo do trabalho. Compartilham a preferência pelos celulares como principal canal digital de acesso a serviços e relacionamento *on-line*.

[283]CHISHTI, Susanne; BARBERIS, Janos. **A Revolução Fintech:** o manual das startups financeiras. Tradução: Samantha Batista. Rio de janeiro: Alta Books, 2017. p.10.

[284] Lançado pelo Banco Central do Brasil em fevereiro de 2020, o PIX é um novo sistema que facilita a transferência de valores entre pessoas, o pagamento de contas e boletos e até recolhimento de impostos e taxas de serviços, entre outras possibilidades. Com o PIX, o sistema de pagamentos passará a funcionar 24 horas por dia, 7 dias da semana, em ttsegundos, uma vez que elas acontecerão sem intermediação de terceiros.

[285]DISTRITO. ***Fintech* mining report 2020.** Disponível em: < https://rdstation-static.s3.amazonaws.com/cms%2Ffiles%2F65883%2F1593523598FinTech_Report_2020_v7.pdf?utm_campaign=resposta_automatica_da_landing_page_dataminer_fintech_report_-_edicao_2020&utm_medium=email&utm_source=RD+Station>. Acesso em: 19 ago. 2020.

Atualmente, iniciativas *Fintech* estão presentes em todas as áreas de serviços financeiros, mudando a maneira como transferimos dinheiro, realizamos pagamentos, obtemos crédito, controlamos as nossas finanças pessoais e investimos nossas economias, dentre diversos outros serviços. Apoiados em tecnologia, que viabilizam menores custos operacionais e maior escalabilidade, os serviços financeiros estão chegando a um preço mais baixo, permitindo, inclusive, a inclusão financeira de parcelas da população de classes menos favorecidas.[286]

Como bem visto, as *fintechs* possuem clara vantagem competitiva ao atuar por meios digitais, oferecendo aos seus clientes mais agilidade, em oposição à tradicional burocracia das instituições financeiras, porém a Lei 4.595/64, do Sistema Financeiro Nacional, estabelece que determinadas atividades são de competência exclusiva de instituições financeiras, determinando ainda a aprovação prévia, das mesmas, pelo Banco Central para prestação de serviços financeiros. Dada essa restrição, as *fintechs,* enxergando espaço no mercado brasileiro para atuarem e oferecerem seus serviços e inovações tecnológicas, buscaram outras alternativas para atuar sem violar a lei do SFN e as normas do Conselho Monetário Nacional e do Banco Central, como por exemplo: (a) Operações ativas vinculadas, conforme Resolução 2.921, do CMN e o (b) Correspondente bancário de uma instituição financeira, conforme Resolução 3.954, do CMN.[287]

Contudo, é importante destacar que o cenário regulatório das *fintechs* sofreu sua principal alteração em 26 de abril de 2018, com a edição da Resolução 4.656, que foi o marco para operações de empréstimo e financiamento, criando as figuras da Sociedade de Crédito Direto (SCD) e da Sociedade de Empréstimo entre Pessoas (SEP), além disso, estabeleceu os procedimentos para constituição dessas instituições e regularizou as operações realizadas por meio das plataformas digitais. Assim, de acordo com a nova Resolução, tanto a SCD quanto a SEP são consideradas instituições financeiras, sendo aptas a operar exclusivamente por meio de plataformas digitais, ou seja, por meio de sítio na *internet* ou aplicativo.[288]

A vista disso, o Banco Central informou, recentemente, que já autorizou o funcionamento de 30 *fintechs* de crédito entre SCD e SEP desde a edição da norma

---

[286]FINTECHLAB. **Report Fintechlab 2017.** Disponível em: < http://fintechlab.com.br/wp-content/uploads/2017/02/Report_FintechLab_2017.pdf>. Acesso em: 26 jun. 2020.
[287]OIOLI, Erik Frederico. **Manual de direito para startups**.2. ed. ver., atual. e ampl. São Paulo: Thomson Reuters, 2020, p.193-195.
[288]OIOLI, Erik Frederico. **Manual de direito para startups**.2. ed. ver., atual. e ampl. São Paulo: Thomson Reuters, 2020, p.195-196.

reguladora. Isso se deve ao fato, das mesmas, operarem exclusivamente por meio de plataformas eletrônicas, prestando um serviço diferenciado, a custos mais reduzidos, com o uso intensivo e inovador de tecnologia.[289]

No mesmo sentido de aumentar a estabilidade com a criação de um ambiente regulatório para o funcionamento das *Fintechs*, em julho de 2017 a Comissão de valores Mobiliários (CVM) regulamentou as atividade de "*crowdfunding* de investimento", também conhecido como *equity crowdfunding*, permitindo que as empresas desse setor captem até R$ 5 milhões para financiar atividades de empreendedores em plataformas digitais de financiamento coletivo com dispensa automática de registro de oferta e de emissor na CVM.[290]

Apesar dos autos investimentos em tecnologia, como bem visto anteriormente, "o atual sistema bancário não está equiparado para realizar a tarefa desafiadora de adaptar-se ao novo cenário digital. Bancos usam principalmente infraestrutura tecnológica antiga centralizada e dependem muito de agências caras e processos manuais. Além disso, dado seu papel na recente crise financeira, eles continuarão enfrentando cada vez mais restrições capitais e regulamentais e continuarão a se afastar do empréstimo para clientes "arriscados" devido a sua alta base de custos, não poderão pagar para subscrever e emprestar dinheiro em pequenas quantias, como seria conveniente para os clientes".[291]

Cabe ressaltar, no entanto, que "os bancos brasileiros sempre funcionaram como um importante indutor em inovações no país. A crise impulsionou a digitalização dentro e fora das instituições financeiras, mas já estávamos preparados e queremos continuar ajudando o cliente a criar um DNA digital que lhe permita ter acesso a serviços com maior valor agregado, mais eficiência e redução de custos", avalia Isaac Sidney, presidente da FEBRABAN.[292]

Desse modo, para diminuir o impacto dos efeitos da pandemia causado pelo novo coronavírus sobre a economia brasileira, o Banco Central vem adotando uma

---

[289]FINTECHLAB. **BC informa já ter autorizado 30 *fintechs* de crédito entre SCD e SEP.** Disponível em: < https://fintechlab.com.br/index.php/2020/06/29/bc-informa-ja-ter-autorizado-30-fintechs-de-credito-entre-scd-e-sep/>. Acesso em: 26 jun. 2020.

[290]TIGRE, Paulo Bastos; PINHEIRO, Alessandro Maia. **Inovação em serviços na economia do compartilhamento.** São Paulo: Saraiva Educação, 2019, p.196.

[291]CHISHTI, Susanne; BARBERIS, Janos. **A Revolução Fintech:** o manual das startups financeiras. Tradução: Samantha Batista. Rio de janeiro: Alta Books, 2017. p.126-27.

[292] FINTECHLAB. **Febraban revela que contas abertas pelo smartphone cresceram 66% em 2019.** Disponível em: < https://fintechlab.com.br/index.php/2020/06/22/febraban-revela-que-contas-abertas-pelo-smartphone-cresceram-66-em-2019/>. Acesso em: 26 jun. 2020.

série de medidas fundamentais para promover o bom funcionamento do mercado, sem abrir mão da solidez e da estabilidade do Sistema Financeiro Nacional (SFN) e dentre essas medidas esta a Autorização para *fintechs* emitirem cartões de crédito e se financiarem no Banco Nacional de Desenvolvimento Econômico e Social, conforme Resolução nº 4.792, de 26 de março de 2020:[293]

> Altera a Resolução nº 4.656, de 26 de abril de 2018, que dispõe sobre a sociedade de crédito direto e a sociedade de empréstimo entre pessoas, disciplina a realização de operações de empréstimo e de financiamento entre pessoas por meio de plataforma eletrônica e estabelece os requisitos e os procedimentos para autorização para funcionamento, transferência de controle societário, reorganização societária e cancelamento da autorização dessas instituições.[294]

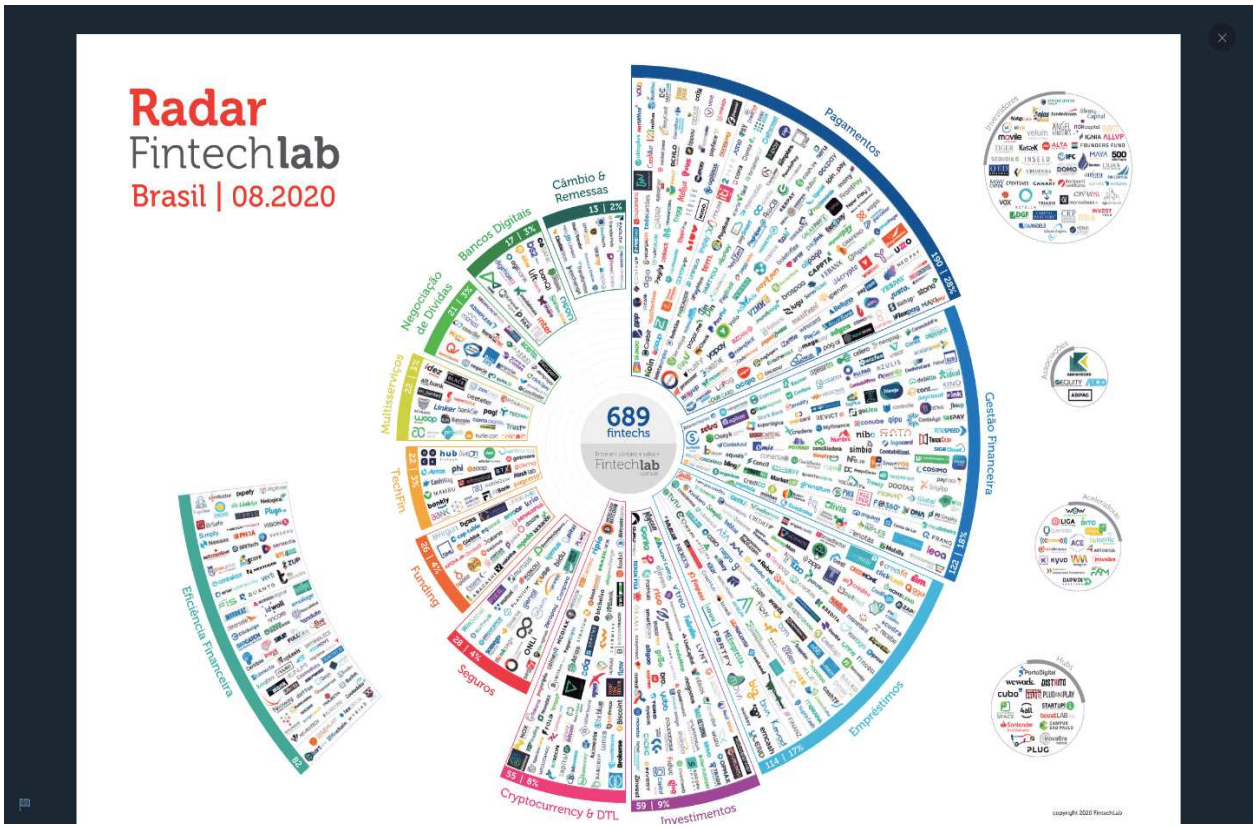
Antes de seguir adiante, vale ressaltar que vivemos um cenário único na economia global, e ainda estamos apenas começando a avaliar seu impacto no mercado de *fintechs.* Em meio a uma pandemia que afeta, em maior ou menor grau, todos os setores, vemos a Organização Mundial da Saúde (OMS) recomendar pagamentos por aproximação para reduzir o risco de contaminação, além das *lives* de artistas popularizando o uso de QR Codes para doações.[295]

Outro ponto, interessante, é o aumento no número de categorias de *fintechs* no Brasil. Segundo levantamento feito pelo Radar FintechLab, que faz parte da maior iniciativa de monitoramento do mercado de *Fintechs* nacional, na edição 2020, registrou mais de 270 novas *fintechs,* saltando de 604 em junho de 2019 para 771 em agosto deste ano, nas categorias Pagamentos, Empréstimos, Gestão Financeira, Investimentos, Seguros, *Cryptocurrency* & DTL*, Funding*, TechFin, Multisserviços, Negociação de Dividas, Câmbio & Remessas, Eficiência Financeira e Bancos Digitais. Atualmente, o setor de pagamentos manteve sua posição como principal motor do crescimento do ecossistema *fintech* brasileiro, com um aumento de 26% em quantidade de representantes. Em paralelo, praticamente no mesmo ritmo de evolução aparecem os bancos digitais que passaram de 12 em 2019 para 17 em 2020, crescendo 50%. Como se percebe na (figura 3) abaixo:

---

[293]BANCO CENTRAL DO BRASIL. **Medidas de combate aos efeitos da COVID-19.** Disponível em: < https://www.bcb.gov.br/acessoinformacao/medidasdecombate_covid19>. Acesso em: 26 jun. 2020.
[294]BANCO CENTRAL DO BRASIL. **Resolução nº 4.792, de 26 de março de 2020.** Disponível em: < https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50959/Res_4792_v1_O.pdf>. Acesso em: 26 jun. 2020.
[295]DISTRITO. ***Fintech*** **mining report 2020.** Disponível em: < https://rdstation-static.s3.amazonaws.com/cms%2Ffiles%2F65883%2F1593523598FinTech_Report_2020_v7.pdf?utm_campaign=resposta_automatica_da_landing_page_dataminer_fintech_report_-_edicao_2020&utm_medium=email&utm_source=RD+Station>. Acesso em: 19 ago. 2020.

Figura 3 – Quantidade de *fintechs* no Brasil em agosto/2020



Fonte: RADAR FINTECHLAB[296]

Em outro levantamento feito por Fintech Mining Report, em julho de 2020, elaborado pelo Distrito, percebe-se ainda uma crescente evolução no número de categorias de *fintechs,* conforme se verá a seguir:

[296]FINTECHLAB. **Novo Radar FintechLab detecta 270 novas fintechs em um ano.** Disponível em: < https://fintechlab.com.br/index.php/2020/08/25/edicao-2020-do-radar-fintechlab-detecta-270-novas-fintechs-em-um-ano/>. Acesso em: 13 set. 2020.

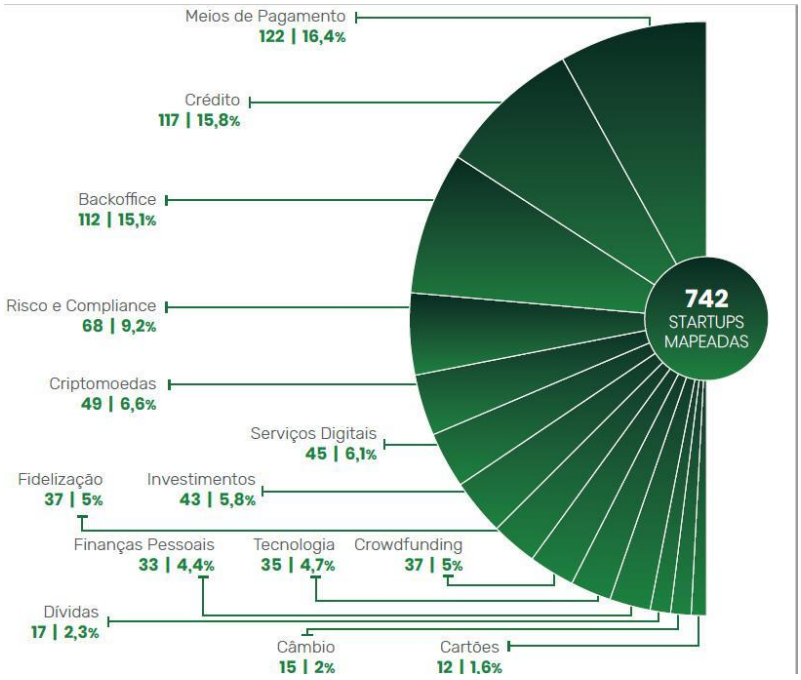
Figura 4 – Categorias de *fintechs* no Brasil

Fonte: DISTRITO FINTECH REPORT 2020[297]

Na divisão das *fintechs* nessas categorias, o Distrito contabiliza 14 categorias, entre elas *backoffice,* criptomoedas, investimentos, *crowdfunding*, dívidas e finanças pessoais. Nelas, o destaque são os meios de pagamento, ou seja, empresas com sistemas de gestão e automação da operação financeira, contam com 122 empresas, ou 16,4%. Em seguida, com 117 (15,8%), estão as de crédito, ou seja, de soluções para intermediar pagamentos, *gateways* e outros agentes de processamento. Em terceiro, estão as *startups* de *backoffice* – que oferecem crédito diretamente, sem conectar a outros provedores – com 112 (15,1%). Em paralelo, praticamente no mesmo ritmo de evolução aparecem os serviços digitais (bancos digitais, contas digitais, *ewallets* – com 45 ou 6,1%), conforme se verá a seguir:

[297]DISTRITO. ***Fintech* mining report 2020.** Disponível em: < https://rdstation-static.s3.amazonaws.com/cms%2Ffiles%2F65883%2F1593523598FinTech_Report_2020_v7.pdf?utm_campaign=resposta_automatica_da_landing_page_dataminer_fintech_report_-_edicao_2020&utm_medium=email&utm_source=RD+Station>. Acesso em: 19 ago. 2020.

Figura 5 – Segmento de negócios das *fintechs* no Brasil (em % do total)



Fonte: DISTRITO FINTECH REPORT 2020[298]

Cabe destacar, ainda, que o Brasil possui 742 startups do sistema financeiro. É o que aponta o novo *Fintech Mining Report* 2020, elaborado pelo Distrito. No relatório do ano anterior, foram mapeadas 553 startups, o que representa um aumento de 34% em um ano. Esse crescimento é consequência de diversos fatores, dentre eles estão as lacunas em nichos do mercado e as soluções digitais que tornam o negócio totalmente escalável, transacionando quantidades massivas de dinheiro.

O crescimento das *Fintechs* pode ser considerado positivo para o mercado, uma vez que amplia a oferta e o alcance dos produtos e serviços financeiros. Elas inovam na forma e no escopo dos serviços, aumentam a competição em determinados nichos de mercado, incentivam o aprimoramento das bases regulatórias e permitem emergência de novos clientes.[299]

Por certo, após compreensão dos dois levantamentos vistos anteriormente, é importante destacar que dentre as diversas categorias de *fintechs* existentes no Brasil, a que tem chamado atenção é a dos bancos digitais, não só pelo crescimento

---

[298]DISTRITO. ***Fintech* mining report 2020.** Disponível em: < https://rdstation-static.s3.amazonaws.com/cms%2Ffiles%2F65883%2F1593523598FinTech_Report_2020_v7.pdf?utm_campaign=resposta_automatica_da_landing_page_dataminer_fintech_report_-_edicao_2020&utm_medium=email&utm_source=RD+Station>. Acesso em: 19 ago. 2020.

[299]TIGRE, Paulo Bastos; PINHEIRO, Alessandro Maia. **Inovação em serviços na economia do compartilhamento.** São Paulo: Saraiva Educação, 2019, p.195.

de 50% em 2020 (Radar FintechLab), mas sim devido opções de acesso pelo aplicativo, na tela do celular, de maneira simples e rápida, com oferta de serviços com mais eficiência e melhores taxas, além disso, é possível ter controle das finanças sem burocracia, tarifas caras e o péssimo atendimento das instituições tradicionais do mercado financeiro, o que em tempos de inseguranças e incertezas, por conta da pandemia de Covid-19, torna-se uma opção mais viável.

Por isso, é fundamental entender que, o banco digital, além de aliviar o trabalho nas 21 mil agências espalhadas pelo Brasil, o que proporcionará melhor atendimento, também elevará a penetração bancária no país. É preciso levar em conta, no entanto, que sua proliferação criará a necessidade de simplificação do e-CPF, o que, mais uma vez, geraria benefício para todos. Para o banco e para o cidadão, a massificação do certificado digital por meio da validação *online* diminuiria os custos. Para o governo, haveria redução da burocracia e do custo de emissão do certificado, com o consequente aumento da segurança jurídica.[300]

De certo, pode-se esperar novidades em um futuro próximo. Novas plataformas digitais e *marketplaces* possivelmente surgirão e trarão experiência e eficiência superior à dos modelos atuais, liberando no limite, o potencial dos modelos colaborativos. E neste momento, clientes estarão cada vez mais satisfeitos com os benefícios visíveis que desfrutam, mais seguros com relação ao uso dos mecanismos digitais, e assim a transformação digital segue seu curso.[301]

Com base nessas informações, pode-se concluir que empresas de *Fintechs*, como por exemplo, bancos digitais são *startups* do mercado financeiro, capazes de oferecer confiança, transparência, tecnologia e serviços a um custo mais baixo de maneira mais transparente, por meio de interfaces fáceis de usar.

---

[300]FEBRABAN. **Como Fazer os Juros Serem mais baixos no Brasil – Uma proposta dos bancos ao governo, Congresso, Judiciário e à sociedade.** 2º edição. São Paulo: Febraban, 2019. Disponível em: < https://jurosmaisbaixosnobrasil.com.br/febraban_ed2.pdf>. Acesso em: 26 jun. 2020. p.117

[301]DISTRITO. ***Fintech* mining report 2020.** Disponível em: < https://rdstation-static.s3.amazonaws.com/cms%2Ffiles%2F65883%2F1593523598FinTech_Report_2020_v7.pdf?utm_campaign=resposta_automatica_da_landing_page_dataminer_fintech_report_-_edicao_2020&utm_medium=email&utm_source=RD+Station>. Acesso em: 19 ago. 2020.

3 METODOLOGIA

Para alcançar os objetivos propostos e entregar uma solução para o problema de pesquisa, a metodologia adotada foi concebida com a combinação de dois métodos de pesquisa, para a definição do tipo de pesquisa relacionado aos fins da investigação e dos meios de investigação.[302] Em relação aos fins de investigação, este estudo na área de ciências sociais aplicadas é caracterizado como descritiva, onde se busca um aprofundamento no tema.[303] De acordo com Rovigati Danilo Alyrio, a pesquisa descritiva busca essencialmente a enumeração e a ordenação de dados, sem o objetivo de comprovar ou refutar hipóteses exploratórias, abrindo espaço para uma nova pesquisa explicativa, fundamentada na experimentação.[304]

Este tipo de pesquisa, aborda quatro aspectos: descrição, registro, análise e interpretação de fenômenos atuais, objetivando o seu funcionamento no presente, segundo Eva Maria Lakatos e Marina de Andrade Marconi. Segundo Dercio Garcia Munhoz, esse tipo de pesquisa visa o conhecimento do comportamento sem necessariamente descer às análises sobre causas e efeitos, ou a tentativa de interpretação.[305]

Quanto ao meio de investigação adotado é caracterizado como uma pesquisa bibliográfica ou revisão literária, interpretada como “[...] o estudo sistematizado desenvolvido com base em material publicado em livros, revistas, jornais, redes eletrônicas, isto é, material acessível ao público em geral [...]”[306]Toda a bibliografia relacionada com a temática é classificada como de valor acrescentado para a investigação, pelo exame bibliográfico.

Esta dissertação utilizou o método de pesquisa bibliográfica e documental com uma abordagem de coleta de dados qualitativa e quantitativa com o intuito de relacionar os dados para a interpretação e responder à seguinte pergunta de

---

[302] ROESCH, S. M. Azevedo. **Projetos de estágio e de pesquisa em Administração:** guia para estágios, trabalho de conclusão, dissertações e estudos de caso. São Paulo: Atlas, 2000.
[303] VERGARA, S. C. **Projetos e relatórios de pesquisa em administração.** São Paulo: Atlas, 2006, p.42-43.
[304] DE ALMEIDA, KATIA. **Análise da evolução da metodologia utilizada nos artigos publicados na revista:** contabilidade & finanças – USP. Disponível em: < http://sistema.semead.com.br/12semead/resultado/trabalhosPDF/642.pdf>.Acesso em: 05 dez. 2020.
[305] DE ALMEIDA, KATIA. **Análise da evolução da metodologia utilizada nos artigos publicados na revista:** contabilidade & finanças – USP. Disponível em: < http://sistema.semead.com.br/12semead/resultado/trabalhosPDF/642.pdf>.Acesso em: 05 dez. 2020.
[306] VERGARA, S. C. **Projetos e relatórios de pesquisa em administração.** São Paulo: Atlas, 2006, p.43-44.

pesquisa “qual o modelo ideal de Contrato de Termos de Uso e de Políticas de Privacidade em conformidade com às disposições legais de proteção na coleta e armazenamento de dados nas relações estabelecidas entre os bancos digitais e seus usuários?”

Durante o processo de coleta, foi realizado um levantamento bibliográfico com dados coletados a partir de obras doutrinárias, artigos publicados em revistas jurídicas, periódicos científicos, anuários, *sites*, publicações eletrônicas e legislações, com destaque para a Constituição Federal, a Lei Geral de Proteção de Dados, com enfoque à proteção da privacidade e dos dados pessoais de clientes de bancos digitais. Também, foram utilizados para referenciar o estudo, dados secundários, capturados em *web sites*, compostos por documentos públicos, arquivos, relatórios, regulamentos; divulgados pelo BACEN, FEBRABAN, bem como, diretrizes nacionais e internacionais de *compliance*, adequados a legislação de proteção de dados.

Importante observar que, como se trata de um assunto recente, e de constante pesquisa e mudança, com poucos estudos abordando o tema, mas com o número de artigos publicados aumentando nos últimos anos, revistas de alta credibilidade no mundo acadêmico, artigos e relatórios de consultorias especializadas, como por exemplo, KPMG, GARTNER, MCKINSEY&COMPANY, bastante relevantes, principalmente em relação ao cenário mundial; foram opções, de pesquisa, valiosas para suprir algumas deficiências nesta questão. Neste aspecto, procurou-se reforçar o referencial teórico adotado com pesquisas atuais, como também as publicadas antes mesmo do início deste estudo.

Nesse sentido, fora realizado um levantamento de dados, por meios virtuais de busca e acesso de dados, através do Portal de Periódicos CAPES, do acervo da Universidade do Vale do Rio dos Sinos – UNISINOS, da ferramenta de artigos acadêmicos “*scholar.google.com*”, do Portal de Legislação do Planalto. As expressões inseridas nos mecanismos de busca foram as seguintes: “Transformação Digital”, “LGPD”, "*Fintech*", "Banco Digital". Além disso, o *site* do Banco Central, CVM, FEBRABAN, Revista CIAB – FEBRABAN, foram de extrema importância para o entendimento do Mercado Financeiro, e para a coleta de dados relativos aos bancos regulados pelos mesmos.

Para análise dos dados optou-se, também, em transformá-los em gráficos, quadros, tabelas para melhor visualização. Assim, os dados foram cruzados e

interpretados tanto em quantidade como em qualidade, com uma legislação fundamentada nos referenciais teóricos desenvolvidos.

Por fim, este trabalho teve como finalidade a realização de um estudo com o objetivo de propor a elaboração de Contratos de Termos de Uso e de Políticas de Privacidade ideal, para *fintechs* de serviços financeiros (bancos digitais), com suas respectivas cláusulas, alinhadas e adaptadas (em conformidade) com à Lei Geral de Proteção de Dados.

4 SEGURANÇA DA INFORMAÇÃO

Para melhor compreensão a respeito do que fora abordado até o momento, é crucial a análise, de maneira clara e objetiva, dos pontos mais relevantes acerca da segurança da informação e sua importância para empresas de serviços financeiros. Ainda, na sequência, apontaremos alguns pontos relevantes, a respeito da Segurança Digital, Cibersegurança e Privacidade.

Antes de mais nada é importante, lembrar que a questão da segurança da informação abrange aspectos legais e técnicos, sendo um pouco mais complexa, de modo que não se pretende aprofundar demais no assunto, seja porque isso demandaria um conhecimento muito especializado. Dessa forma, busca-se compreender, de maneira simples e clara, a dinâmica da segurança da informação para esclarecer algumas questões importantes sobre o assunto.

Do mesmo modo vertiginoso como os avanços nas novas tecnologias chegam, influenciando vidas de indivíduos e de sociedades inteiras, produzindo novos hábitos e sendo substituídos por tecnologias ainda mais recentes, na atualidade temos que lidar a cada dia com grandes volumes de informação, todo este conjunto de tecnologias, conhecimento e interações se traduzindo também numa série de implicações em termos de segurança, em diversos níveis.

Como já mencionado, hoje, sem dúvida, a informação é um dos principais patrimônios do mundo dos negócios. Um fluxo de informação de qualidade é capaz de decidir o sucesso de um empreendimento. Mas esse poder, somado à crescente facilidade de acesso, faz desse "ativo" um alvo de constantes ameaças internas e externas.

Assim, o conceito de segurança da informação ou segurança dos dados tem um valor ligeiramente diferente daquele de “dados” discutido anteriormente, embora ambos compartilhem semelhanças no ponto central que é a preocupação produzida pelos seus efeitos na garantia da integridade e da privacidade dos dados.[307] Dessa forma, podemos definir segurança da informação como a área do conhecimento que visa à proteção da informação das ameaças a sua integridade, disponibilidade e

[307] BARBIERI, Carlos. **Governança de dados:** práticas, conceitos e novos caminhos. Rio de Janeiro: Alta Books, 2019, p.146.

confidencialidade a fim de garantir a continuidade do negócio e minimizar os riscos.[308]

Outra conceituação importante é trazida por Edson Fontes:

> Segurança da informação é um programa organizacional que tem por objetivo permitir e possibilitar que a organização alcance seus objetivos no que depende da informação (bem universal) e dos recursos de informação garantindo assim, uma informação confiável.[309]

Também cabe destacar a definição de segurança da informação dada por Jule Hintzbergen:

> A segurança da informação é alcançada através da implementação de um conjunto adequado de controles, incluindo políticos, processos, procedimentos, estruturas organizacionais e funções de *software* e *hadware*. Esses controles precisam ser estabelecidos, implementados, monitorados, revisados e melhorados, onde necessário, para assegurar que os objetivos específicos de segurança e do negócio da organização sejam atendidos. Isso deve ser feito em conjunto com outros processos de gerenciamento de negócio. A segurança da informação é importante para os negócios públicos quanto para o setor privado, e para proteger infraestruturas críticas. Em ambos os setores ela funcionará como facilitadora – por exemplo, para realizar *e-government* ou *e-business* e para evitar ou reduzir os riscos relevantes.[310]

Ainda, assim, é importante mencionar que quando se trata de manter os ativos de informações seguros, as organizações podem contar com a família ISO / IEC 27000, certificação internacional que trata da segurança da informação. Embora haja mais de uma dúzia de padrões na família ISO / IEC 27000 as mais conhecidas são as ISO 27001 e ISO 27002. A ISO / IEC 27001 é amplamente conhecida, fornecendo requisitos para um sistema de gestão de segurança da informação (SGSI), seu uso permite que organizações de qualquer tipo gerenciem a segurança de ativos, como informações financeiras, propriedade intelectual, detalhes de funcionários ou informações confiadas por terceiros. A (figura 6) abaixo representa a família ISO / IEC 27000.

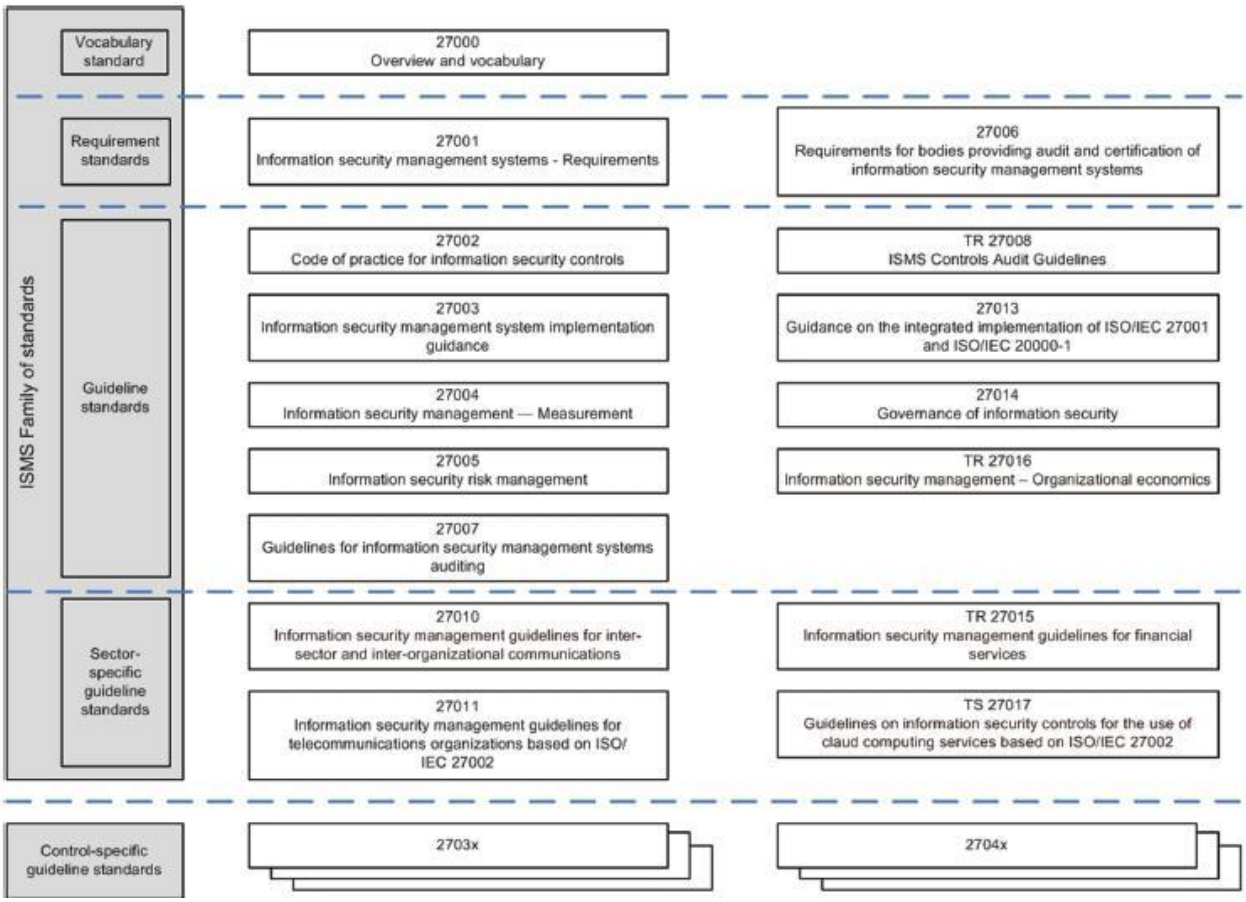
---

[308] NETTO, Abner da Silva; DA SILVEIRA, Marco Antônio Pinheiro. **Information security management:** factors that influence its adoption in small and mid-sized businesses. SciELO, 2007. Disponível em: < https://www.scielo.br/scielo.php?script=sci_arttext&pid=S1807-17752007000300007>. Acesso em: 12 set. 2020.

[309] FONTES, Edison Luiz Gonçalves. **Segurança da Informação:** gestão e governança. 1.ed. São Paulo, 2020. Livro eletrônico, p.20-31.

[310] HINTZBERGEN, Jule et al. **Fundamentos de Segurança da Informação:** com base na ISO 27001 e na ISO 27002.1ºEd. Brasport, 2018. Livro eletrônico, não paginado.

Figura 6 – Família ISO/IEC 27000



Fonte: Márcio Andrey Teixeira[311]

Cabe destacar, que a segurança da informação é responsável por garantir: (a) Confidencialidade, ou seja, garantir que toda informação seja classificada e tratada da forma correta, estando acessível apenas para as pessoas que necessitam acessá-las para desempenhar suas atividades; (b) Disponibilidade, garantir que toda informação esteja acessível, para colaboradores e usuários, no momento em que ela se faz necessária, e; (c) Integridade, garante que as informações não serão alteradas de forma indevida, por pessoas não autorizadas.

É importante observar, ainda, que hoje em dia, se preocupar com a gestão da segurança da informação tem se tornado cada vez mais fundamental e crítico para o sucesso de qualquer negócio.[312] Assim, a segurança da informação deve estar presente em todos os processos e atividades regidas pelas empresas de serviços

[311] TEIXEIRA, Márcio Andrey. **Normas ISO 27000.** Instituto Federal de São Paulo, 2020. Disponível em: < http://200.133.218.36:8005/si-2020/Aula.04-SEG_ISO_27000_NormasSI_MA.pdf>. Acesso em: 12 set. 2020.
[312] TEIXEIRA, Tarcísio; LOPES, Alan Moreira; TAKADA, Thalles. **Manual jurídico da inovação e das startups.** 2.ed. Salvador: Editora JusPodivm, 2020, p.167.

financeiros, pois envolve informações confidenciais dos usuários, protegidas por lei, que devem ser tratadas com cautela e privacidade.

Além disso, o investimento em segurança da informação deve ser na mesma medida que em tecnologias para melhorar o desempenho e expandir as possibilidades de negócios, uma vez que é importantíssima para evitar golpes, violações de dados e por aí vai. Um bom planejamento de segurança, não só vai garantir que as informações estão sendo protegidas, como também pode resultar em redução de custos. Quando olhamos para segurança de forma estratégica, podemos identificar quais informações precisam ser protegidas e quais os melhores controles a serem implementados, evitando investimento em recursos excessivos.

Desta forma, a era da informação em que estamos vivendo é caracterizada pelo acelerado crescimento na quantidade de dados e informações coletadas, armazenadas e disponibilizadas em formato eletrônico.[313] Como se sabe, aumenta a cada dia a quantidade de dados capturados nos processos que envolvem o sistema financeiro, seja sob a forma de transações financeiras por meios eletrônicos, solicitações de serviços, análises de comportamento, dados sobre histórico de consumo de produtos e serviços, entre outros.[314] Portanto, todo o patrimônio está nos dados, por isso a necessidade de haver camadas de proteção com ações que incluem investimentos em políticas, tecnologia, processos e em melhores práticas.

Em geral, quando falamos de dados, como já mencionado anteriormente, estamos falando do grande ativo da sociedade digital, o novo petróleo (*oil*) e o novo solo (*soil*), quando trabalhados visando a transformação de informações, e que exigem certos cuidados quanto a sua segurança. Atualmente, o que tem preocupado, bastante, quando o assunto é dado, são os roubos e o sequestros dos mesmos, por *hackers*, ocasionado por falhas de sistema ou até mesmo de pessoal que resultam no vazamento de informações privadas dos usuários.

Segundo o Gartner, empresa de pesquisa e consultoria, estima que uma variedade louca de cerca de 21 bilhões de “coisas” conectadas estão neste

---

313 SHARDA, Ramesh; DELEN, Dursun; TURBAN, Efraim. ***Business intelligence* e análise de dados para gestão do negócio.** Tradução: Ronald Saraiva de Menezes. 4.ed. Porto Alegre: Bookman, 2019, p.297.

314 PALHARES, Felipe. et al. **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020, p.130.

momento coletando dados e realizando todo tipo de tarefas.[315] Nunca se teve acesso à tanta informação utilizando as mais diversas tecnologias e as mais poderosas formas de comunicação.[316]

Conforme demonstrado ao longo do trabalho, como parte da transformação digital, o setor financeiro está, cada vez mais, a utilizar aplicativos para *smartphones*, e também outros meios tecnológicos, como um investimento substancial para alavancar o seu crescimento futuro e a rentabilidade do seu negócio. Tais tecnologias tornam mais fácil a interação e a realização das atividades bancárias dos seus clientes, oferecendo uma maior fiabilidade e eficiência nos processos em toda a cadeia de negócio. No entanto, se uma solução traz consigo o potencial de apresentar falhas de segurança, rapidamente se torna inútil e pode pôr em risco todo o negócio/instituição.[317] Neste sentido, é crucial garantir os mais altos níveis de segurança em um mercado cada vez mais informatizado.

Neste ponto, o fortalecimento da estrutura de confiança, incluindo segurança da informação, segurança digital e privacidade, é um pré-requisito para o desenvolvimento da Sociedade da Informação (ou sociedade de dados). Tais esforços devem ser apoiados por uma maior cooperação internacional. Nessa cultura global de segurança cibernética, é importante aprimorar a segurança e garantir a proteção de dados e a privacidade, ao mesmo tempo em que se amplia o acesso e o comércio de dados.[318]

Assim sendo, qualquer falha em proteger dados de clientes de serviços financeiros da maneira que os mesmos esperam poderia ser devastador. E claro, os novos *players* apresentam uma tela mais abrangente de vulnerabilidade para

---

[315] CIO. **Internet das coisas em 2020:** mais vital do que nunca. Disponível em: < https://cio.com.br/tendencias/internet-das-coisas-em-2020-mais-vital-do-que-nunca/>. Acesso em: 13 set. 2020.

[316] FONTES, Edison Luiz Gonçalves. **Segurança da Informação:** gestão e governança. 1.ed. São Paulo, 2020. Livro eletrônico, p.21.

[317] ALCARVA, Paulo. **Banca 4.0. Revolução Digital:** *fintechs, blockchain*, criptomoedas, *robo-advisers* e *crowdfunding*. Coimbra: Conjuntura Actual Editora, 2018, p.189.

[318] Documentos da Cúpula Mundial sobre a Sociedade da Informação [livro eletrônico]: Genebra 2003 e Túnis 2005 / International Telecommunication Union; [traduzido por Marcelo Amorim Guimarães]. São Paulo: Comitê Gestor da Internet no Brasil, 2014, p.27. Disponível em: < https://www.cgi.br/media/docs/publicacoes/1/CadernosCGIbr_DocumentosCMSI.pdf>. Acesso em: 30 ago. 2020.

hackers. Ou seja, quanto mais sistemas existem, mais dados há para *hackear*, e maior é a vulnerabilidade.[319]

Confirmando esse entendimento, percebe-se que o uso de dispositivos digitais para contratação e relacionamento é fator inseparável na realidade digital. Ou seja, é aplicar controles de segurança da informação e rotinas para mitigar riscos operacionais e reunir recursos para melhor defender interesses, caso haja algum incidente ou prejuízo envolvendo as atividades de seus clientes que forem praticadas por meio digital. Isso porque conforme avançam as ferramentas tecnológicas, crescem também os ciberataques e surgem novos modelos de fraudes e golpes financeiros. Isso significa que todos os agentes de mercado, todo o ecossistema, de algum modo, será impactado e deverá implementar um ciclo para aprendizado e uma política específica para resposta a incidentes relacionados à violação de dados pessoais e vazamentos. Envolve-se, assim, uma alteração comportamental, para estabelecer uma cultura de segurança e prevenção, com o treinamento de funcionários, transparência nos processos de coleta de dados e eficiência na abordagem com os consumidores.

A seguir, a análise dos pontos mais importantes a respeito da Segurança Digital, Cibersegurança e Privacidade.

4.1 SEGURANÇA DIGITAL

Primeiramente, cabe destacar que a *internet* surgiu em meados dos anos 60, criada por militares durante a guerra fria, porém, não será falado aqui de seu contexto histórico, e sim, do contexto atual que ela se encontra, pois vivemos na era da *cyber* espionagem, na qual nenhum governo respeita a privacidade de seus cidadãos, e assim criando certa desconfiança entre eles. Além disso, é importante mencionar que no mundo globalizado, a cada ano aumenta o número de vazamento de dados e desvios de dinheiro de grandes instituições, pela grande insegurança e falta de capacidade de seus administradores de banco de dados e redes. Como consequência disso, surge os prejuízos causados por esses ataques de *crackers*, que na maioria das vezes, utilizam técnicas que são desde de simples, até as mais

[319] CHISHTI, Susanne; BARBERIS, Janos. **A Revolução *Fintech*:** o manual das *startups* financeiras. Tradução: Samantha Batista. Rio de janeiro: Alta Books, 2017, p.32.

avançadas para efetuar invasões em grande escala, afetando principalmente o mercado financeiro e causando milhões em prejuízos. Dessa forma, percebe-se que tudo gira em torno da privacidade, segurança e os maldosos *hackers* que espreitam nas sombras da *internet* apenas aguardando mais uma vítima indefesa.[320]

Nesse sentido, a maneira como as instituições lidam com os dados e privacidade do consumidor pode se tornar um ponto de diferenciação e até mesmo uma fonte de vantagem competitiva para os negócios. Assim, a proliferação de violações e a demanda dos consumidores por privacidade e controle de seus próprios dados levaram os governos a adotar novos regulamentos, como o Regulamento Geral de Proteção de Dados (GDPR) na Europa, o Ato de Privacidade do Consumidor da Califórnia (CCPA) naquele estado dos EUA e a Lei Geral de Proteção de dados (LGPD) no Brasil, que será analisada mais à frente.

Antes de seguir adiante, vale ressaltar que o período de isolamento social por conta da pandemia do novo coronavírus levou à adoção de ferramentas para o *home office* e, consequentemente, a um consumo maior de dados. A Akamai, plataforma de armazenamento em nuvem responsável por 30% do tráfego *online* mundial, registrou em abril de 2020 um aumento de 112% no uso de rede no Brasil em relação ao mesmo período do ano passado. Segundo a empresa, a alta foi causada porque mais pessoas passaram a usar a *internet* para trabalhar, estudar, fazer compras e se divertir. Contudo, com mais pessoas adotando o modelo de *home office*, cresce também a atividade de cibercriminosos em busca de informações.

Nota-se, portanto, que se de um lado a pandemia trouxe aumento da digitalização, de outro aumentou – e muito – o número de fraudes no sistema bancário brasileiro. Segundo a Pesquisa de Tecnologia Bancária – FEBRABAN 2020, as transações bancárias realizadas pelo *mobile banking* tiveram um aumento de 19% em 2020, com incremento de 41% nas transações com movimentação financeira. Estima-se que 67% das transações bancárias de pessoas físicas passaram a ser realizadas por meio do *mobile banking* só em abril. O principal ponto

[320] MARTINS, Gabriel da Silva. **Segurança digital:** o guia para segurança na internet. 1º ed. São Paulo Brutal Security, 2015**.** Livro eletrônico, não paginado.

aqui é que com o aumento do uso dos canais digitais pelos brasileiros durante a quarentena elevou a escala das fraudes.[321]

A título de curiosidade conforme dados da Polícia Federal nos Estados Unidos (FBI), somente no ano passado os crimes cibernéticos[322] denunciados somaram US$ 3,5 bilhões de prejuízo (cerca de R$ 15 bilhões). Inclusive, o órgão mantém um departamento dedicado para contatar as instituições financeiras e tentar reaver o dinheiro das vítimas. No relatório, especialistas alertam que os criminosos estão ficando tão sofisticados que está mais difícil para as vítimas identificarem as bandeiras vermelhas e diferenciarem o real de falso.[323]

Diante disso, cada vez mais a segurança digital torna-se importante. Têm sido muito comum casos de sequestro de servidores de empresas, em que todos os dados ficam indisponíveis até o pagamento de resgate.[324]

A partir daí, percebe-se, que o termo segurança digital se refere à proteção das informações no ambiente virtual. Para isso, são usadas ferramentas para preservação da identidade e garantia de confidencialidade, integridade, disponibilidade e autenticidade de documentos e dados pessoais de usuários.

Conforme se vê, a segurança digital é a proteção de sua identidade digital – o equivalente na rede ou *Internet* a sua identidade física, inclui as ferramentas para proteger a sua identidade, bens e tecnologia no mundo *on-line* e celular. Estas ferramentas incluem *softwares*, antivírus, serviços de *Internet*, biométricos e dispositivos pessoais de segurança, tais como um *token* USB baseado em cartão inteligente, o cartão SIM no telefone celular, o *chip* seguro no cartão de pagamento sem contato ou e-passaporte são dispositivos de segurança digital, porque eles dão a liberdade de se comunicar, viajar, comprar, acessar o banco e trabalhar usando sua identidade digital em uma maneira que seja conveniente, agradável e segura.

---

[321] FEBRABAN. **Clientes pessoas físicas fizeram 74% das transações bancárias pelos canais digitais em abril.** Disponível em: < https://portal.febraban.org.br/noticia/3474/pt-br/>. Acesso em: 27 jul. 2020.

[322] Os crimes cibernéticos são aqueles crimes praticados através da Internet, ou seja, através da rede mundial de pessoas interligadas por computadores, ou outros sistemas de dados.

[323] Revista CIAB - FEBRABAN. 2020. **Inovação e segurança devem ser inseparáveis no segmento financeiro.** Disponível em: <https://noomis.febraban.org.br/especialista/patricia-peck-pinheiro/inovacao-e-seguranca-devem-ser-inseparaveis-no-segmento-financeiro>. Acesso em: 26 jun. 2020.

[324] PELLINI, Rudá. **O futuro do dinheiro: banco digital, *fintechs, criptomoedas* e *blockchain*:** entenda de uma vez por todos esses conceitos e saiba como a tecnologia dará liberdade e segurança para você gerar riqueza. São Paulo: Editora Gente, 2019, p.142.

Dito isso, verifica-se, que a segurança digital é, sem dúvida, um dos assuntos mais debatidos atualmente, seja sobre o uso das redes sociais ou do *mobile banking*. Pensar nesse tema é essencial para instituições e usuários, tendo em vista que dados são fontes de informações relevantes, se estudados da melhor forma. De maneira geral, a segurança digital tem como objetivo resguardar informações confidenciais, por isso é importante se preocupar com ela.

De acordo com o Relatório de Ameaças de Dados Thales de 2020 - Edição Global com pesquisa e análise da IDC, as organizações alcançaram um ponto crítico na nuvem global, fazendo com que lutassem com os desafios de segurança da transformação digital (DX). Hoje, metade (50%) de todos os dados corporativos são armazenados na nuvem e quase metade (48%) desses dados são considerados confidenciais. Com o uso de várias nuvens se tornando o novo normal para as instituições, todos os entrevistados, da pesquisa, disseram que pelo menos alguns dos dados confidenciais armazenados na nuvem não são criptografados e 49% globalmente indicaram que experimentaram uma violação. Além das complexidades DX e de várias nuvens, o estudo global mostra que a computação quântica disparou como uma grande preocupação, com 72% das organizações alegando que afetará suas operações criptográficas e de segurança nos próximos cinco anos.[325]

No mesmo cenário, há de se salientar, ainda, o relatório State of the Internet / Security Financial Services Report 2020, volume 6, Issue 1, da Akamai Technologies, inc (NASDAQ: AKAM), que examina os serviços financeiros e identifica inúmeras tendências emergentes, observou-se que em maio de 2019 e continuando até o final do ano, houve uma mudança dramática de criminosos que começaram a mirar nas APIs. De acordo com dados da Akamai, até 75% de todos os ataques de abuso de credencial contra o setor de serviços financeiros visavam APIs diretamente. De acordo com as conclusões do relatório, de dezembro de 2017 a novembro de 2019, 85.422.079.109 ataques de abuso de credenciais em toda a base de clientes. Quase 20%, ou 16.557.875.875, eram a nomes de *host* claramente identificados como pontos de extremidade de API. Dentre eles, 473.513.955 atacaram as organizações do setor de serviços financeiros. Usando o mesmo período de 24 meses, também se observou mais detalhadamente os aplicativos da

---

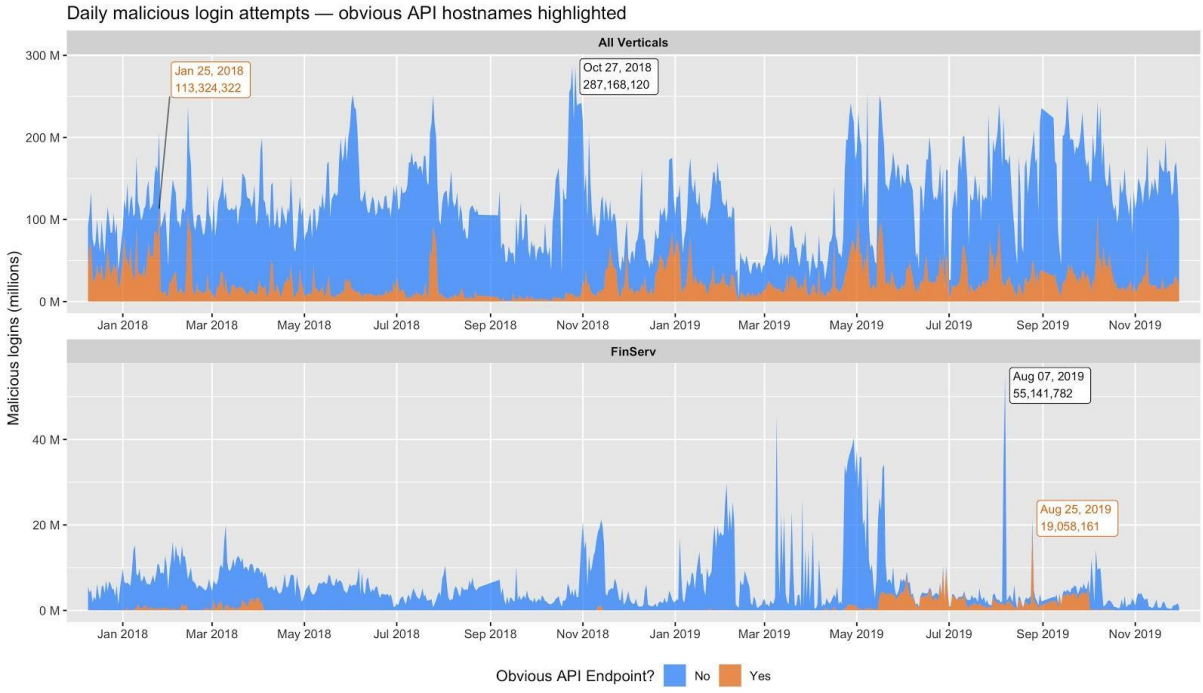
[325] THALESGROUP. **Relatório de Ameaças de Dados Thales de 2020.** Disponível em: < https://www.thalesgroup.com/en/group/journalist/press-release/global-cloud-tipping-point-2020-thales-data-threat-report-global>. Acesso em: 27 jul. 2020.

web e os ataques DoS (ataques de negação de serviço distribuído) contra o setor de serviços financeiros. Durante esse tempo, foram 662.556.776 ataques a aplicativos da *web* contra o setor de serviços financeiros.

Observa-se assim, que é preciso aplicar mecanismos de controle conforme as particularidades e necessidades de cada instituição. E isso vai além do segmento financeiro, alcança também todos aqueles com quem os bancos operam e fazem negócios, dos correspondentes bancários aos fornecedores de nuvem, aos parceiros de aplicativos, entre outros. Seja por contratos ou por APIs, todas as conexões que geram fluxos de dados precisam estar sob um guarda-chuva de gestão de riscos operacionais digitais.

Nesse sentido, cabe destacar o (gráfico 4) abaixo que mostra *logins* maliciosos diários, com os pontos finais de API óbvios em destaque. O topo gráfico mostra todas as verticais, enquanto o gráfico inferior está focado exclusivamente em serviços financeiros. Observa-se que a taxa de logins maliciosos contra APIs no setor de serviços financeiros aumentou significativamente começando em maio de 2019.

Gráfico 4 – Taxa de logins maliciosos contra APIs no setor financeiro



Fonte: Akamai[326]

[326] AKAMAI. **State of the Internet / Security Financial Services Report 2020.** v.6, p. 08. Disponível em: < https://www.akamai.com/br/pt/multimedia/documents/state-of-the-internet/soti-security-financial-services-hostile-takeover-attempts-report-2020.pdf>. Acesso em:13 set

Por fim, estamos em uma sociedade cada vez mais tecnológica, em meio a dezenas de ameaças e vulnerabilidades. Todo patrimônio está nos dados, por isso a necessidade de haver camadas de proteção com ações que incluem investimentos em políticas, tecnologia, processos e em melhores práticas, além de campanhas de conscientização e educação em segurança digital. Ainda assim, com um planejamento específico que garanta a segurança e a legitimidade para tratar os dados de acordo com as atividades desenvolvidas, por meio do consentimento específico para as finalidades informadas, poderemos desenvolver ainda mais o mercado, aumentar a competitividade, a inclusão e fomentar mais inovação.

4.2 CIBERSEGURANÇA OU SEGURANÇA CIBERNÉTICA

Conforme exposto anteriormente, ameaças virtuais surgem o tempo todo, fazendo com que o cenário da segurança cibernética esteja em constante evolução – o que significa que temos de estar vigilantes e prover aos clientes e usuários soluções que protejam seus dados.

É importante frisar que com a pandemia de COVID-19, as fusões e aquisições de segurança cibernética neste ano estão no mesmo ritmo de 2019, embora pareça haver menos apetite para gastar muito. Os dez maiores negócios em 2019 totalizaram mais de US $ 30 bilhões, enquanto os dez maiores em 2020 totalizaram menos de US$ 13 bilhões. O maior negócio em 2020 tem menos da metade do tamanho do maior em 2019. As empresas de *private equity* continuam a ter uma grande presença nas maiores aquisições.[327]

Vale lembrar que a pandemia acelerou o uso dos recursos tecnológicos e muitas áreas que não tinham serviços consolidados passaram a oferecer caminhos digitas para seus usuários. Isso promoveu uma convergência do mundo real e digital e, também, chamou a atenção de cibercriminosos. Sempre atentos, eles adaptaram seus ataques com práticas usadas em crimes financeiros cibernéticos e tradicionais.

Conforme observado em uma análise recente da Check Point Software Technologies no meio do ano, “o primeiro impacto da pandemia foi a proliferação de

---

[327] SWINHOE, Dan. **11 biggest cybersecurity M&A deals in 2020.** CSO. Disponível em: < https://www.csoonline.com/article/3574730/10-biggest-cybersecurity-manda-deals-in-2020.html>. Acesso em: 15 out. 2020.

ataques de *malware*[328] que usaram técnicas de engenharia social com iscas temáticas COVID-19 para o estágio de entrega.” Nomes de domínio foram criados e estacionados com nomes relacionados à pandemia. Conforme os trabalhadores começaram a usar plataformas de videoconferência, os ataques passaram a atacar o *Zoom*, *Teams* e outras plataformas de videoconferência. Uma tendência preocupante é que 80% dos ataques observados no primeiro semestre de 2020 usaram vulnerabilidades relatadas e registradas em 2017 e antes, de acordo com o relatório da Check Point, e mais de 20% dos ataques usaram vulnerabilidades com pelo menos sete anos. Isso mostra que temos um problema em manter nosso *software* atualizado.[329]

Contudo, uma conclusão rápida que se pode ter é que as ações emergenciais necessárias para o combate à COVID-19 de certa maneira desafiam a segurança dos dados e aumentam os riscos de vazamento de informações. Houve um aumento expressivo de uso de ambientes de nuvem (*cloud*) com sobrecarga das redes e infraestruturas que podem colapsar, muitos que estão utilizando destes ambientes e que não receberam orientação para uso seguro ou, ainda, os ambientes não estão preparados para sigilo e proteção. Nunca houve tanto fluxo de dados pessoais e dados pessoais sensíveis sendo compartilhados[330] devido ao momento de calamidade pelo qual estamos passando.

A partir daí, cabe destacar que Cibersegurança ou Segurança Cibernética é a prática que protege computadores e servidores, dispositivos móveis, sistemas eletrônicos, redes e dados contra ataques maliciosos. Também é chamada de segurança da tecnologia da informação ou segurança de informações eletrônicas. O termo é aplicável a uma variedade de contextos, desde negócios até computação móvel.

Outro ponto importante é que a segurança cibernética é uma indústria maciça que emergiu junto com o comércio eletrônico. À medida que mais e mais fundos se movem digitalmente, os criminosos informáticos encontram formas fáceis de cometer

---

[328] Malware *do* inglês *Malicious software* (*software* malicioso) ou código malicioso. Termo genérico que se refere a todos os tipos de programa que executam ações maliciosas em um computador. Exemplos de códigos maliciosos são os vírus, *worms*, *bots*, cavalos de troia, *rootkits* etc.

[329] BRADLEY, Susan. **4 tops vulnerabilities ransomware attackers exploited in 2020.** CSO. Disponível em: < https://www.csoonline.com/article/3572336/4-top-vulnerabilities-ransomware-attackers-exploited-in-2020.html>. Acesso em: 15 out. 2020.

[330] Compartilhamento é a disponibilização de arquivos ou recurso fisicamente ligados a um terminal de uma rede para outros terminais. Compartilham-se *winchesters*, arquivos, diretórios, impressoras, *scanners* e outros periféricos.

crimes e de fraudar pessoas, sem sequer necessitar envolver-se em atos violentos.[331]

Neste ponto, com o aumento exponencial das ameaças cibernéticas[332] nos últimos anos, tanto em volume, quanto em sofisticação, reguladores e autorreguladores têm voltado maior atenção para esse assunto com o objetivo de orientar as instituições em seus respectivos mercados e verificar se suas estruturas estão preparadas para identificar e mitigar riscos cibernéticos, assim como para se recuperar de possíveis incidentes. Além disso, os avanços tecnológicos criam facilidades e possibilitam o uso de novas ferramentas para a atuação das instituições, permitindo agilidade na construção e disponibilização de serviços, ampliação dos meios de comunicação, entre outros avanços. Por outro lado, o aumento do uso de tais ferramentas potencializa os riscos de ataques cibernéticos, ameaçando a confidencialidade, a integridade e a disponibilidade dos dados ou dos sistemas dessas instituições.[333]

Vale ressaltar que os setores financeiro e de TI estão mais avançados em segurança cibernética, por serem alvos mais frequentes, investem cada vez mais nesse tipo de segurança.

É importante destacar, ainda, que as *fintechs* e outras organizações do setor financeiro, possuem dados preciosos e desejados por criminosos cibernéticos. Por isso, investem pesado na segurança da informação. Isso é uma realidade: *ransomware*[334]*,* violações de dados e ataques de negação de serviço distribuídos são altamente direcionados a instituições financeiras. Os impactos das perdas vão

---

[331] RUBINI, Agustin. **A Fintech em um Flash**. Tradução: Fernanda Belokurows. Babelcube Inc., 2017. Livro eletrônico, não paginado.

[332] Ameaças cibernéticas são os perigos específicos que criam o potencial para o risco cibernético, ou seja, existem no contexto de risco cibernético empresarial como caminhos potenciais para a perda de confidencialidade, integridade e disponibilidade de ativos digitais. Por extensão, o impacto do risco das ameaças cibernéticas inclui fraude, crime financeiro, perda de dados ou perda de disponibilidade do sistema. Além disso, as ameaças cibernéticas não são o mesmo que os riscos cibernéticos, que se referem ao potencial de perdas de negócios de todos os tipos - financeiros, de reputação, operacionais, de produtividade e de regulamentação - no domínio digital. O risco cibernético é uma forma de risco empresarial, que pode causar perdas no domínio físico, como danos a equipamentos operacionais.

[333]ANBIMA. **Guia de cibersegurança.** 2.ed. 6 dez. 2017. Disponível em: < https://www.anbima.com.br/data/files/F5/62/AB/91/FBC206101703E9F5A8A80AC2/Guia-de-Ciberseguranca-ANBIMA.pdf>. Acesso em: 15 out. 2020.

[334] R*ansomware* é um *malware* que pode bloquear um dispositivo ou criptografar seus conteúdos para extorquir dinheiro de seu proprietário. Em troca, os operadores de códigos maliciosos prometem – claro, sem qualquer garantia – restaurar o acesso às máquinas afetadas ou aos dados.

desde a interrupção dos negócios, danos na reputação corporativa e violação de informações dos clientes. À medida que as organizações se tornam cada vez mais dependentes de tecnologia, o problema passa a ser a vulnerabilidade na própria infraestrutura digital. No caso das financeiras, as ameaças cibernéticas estão em permanente evolução em complexidade e intensidade e podem resultar em interrupção comercial significativa ou danos à propriedade.

De acordo com a segunda edição da Pesquisa *Fintech Deep Dive 2019*, da PwC, conduzida em parceria com a Associação Brasileira de *Fintechs* (ABFintechs), a cibersegurança é dominada por menos de um quarto das *fintechs* participantes atualmente. E que apenas 20% dizem querer dominá-la no futuro. Esse cenário é ainda mais preocupante quando se leva em conta o interesse crescente das instituições pela Internet das Coisas e os novos riscos que ela pode trazer para esse ambiente. Por ser capaz de conectar entre si diferentes dispositivos, a IoT deverá permitir uma experiência mais personalizada para o consumidor e uma avaliação de riscos mais precisa, mas a coleta, o gerenciamento e o compartilhamento de um volume crescente de dados pessoais abrem novos e múltiplos flancos para ataques e vazamentos.

Em uma pesquisa (publicada em julho de 2020), feita pela *Price waterhouse Coopers* (PwC), prestadora de serviços profissionais nas áreas de auditoria e consultoria, revelou que:

> A cibersegurança é a mais alta prioridade de investimento dos CEOs do segmento este ano e eles veem as ameaças cibernéticas como o segundo maior risco ao crescimento. É preciso investir mais. Também é preciso fortalecer a vigilância e a proteção de dados à medida que os modelos de serviço se tornam mais abertos.[335]

No mesmo sentido, surgem novos modelos de fraudes e golpes financeiros, por meio dos *bots*[336]. São contas que servem para multiplicar as informações distribuídas na rede, passando-se por contas de pessoas reais. Basicamente consistem em aplicações autônomas que navegam na *internet* enquanto

---

[335] PRICE WATERHOUSE COOPERS (PWC). **Tendências do setor de bancos e mercado de capitais em 2020:** lançando as bases para o crescimento. Disponível em: < https://www.pwc.com.br/pt/estudos/setores-atividade/financeiro/2020/tendencias-do-setor-de-bancos-e-mercado-de-capitais-em-2020-lancando-as-bases-para-o-crescimento.html>. Acesso em: 13 set. 2020.

[336] Bot é um programa que, além de incluir funcionalidades de *worms*, sendo capaz de se propagar automaticamente por meio da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em um computador, dispõe de mecanismos de comunicação com o invasor, permitindo que o programa seja controlado remotamente. O invasor, ao se comunicar com o *bot*, pode orientá-lo a desferir ataques contra outros computadores, furtar dados, enviar *spam* etc.

desempenham algum tipo de tarefa pré-determinada. Esses perfis interagem com aplicativos da mesma maneira que um usuário legítimo faria, dificultando sua detecção e prevenção, e promovem atividades maliciosas e concorrência desleal, como *spam*, coleta de dados pessoais, *login* de força bruta, e fraudes em transações e em anúncios digitais.

Segundo Relatório de Bad Bot Report 2020, da Imperva, empresa de *software* e serviços de segurança cibernética, em 2019 o tráfego de *bots* classificados como ruins[337] chegou a 24,1%, e o setor de serviços financeiros foi o mais atingido (47,7%).

Assim sendo, é válido destacar que o Banco Central do Brasil (BACEN) não mede esforços para garantir que o Sistema Financeiro Nacional se mantenha sólido e estável e proteja os consumidores. A vista disso, regulamentou a questão da cibersegurança para as instituições financeiras, através da Resolução nº 4.658 de 26/04/2018 e da Resolução nº 4.752 de 26/09/2019.

Segundo a Resolução nº 4.658/18, as instituições financeiras que operam digitalmente, precisam implantar uma política de segurança cibernética. Para tanto, torna-se necessário a definição de requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem (*cloud computing*) a serem observados pelas instituições financeiras e demais instituições. Não basta ter a tecnologia, é preciso educar na prevenção de riscos, visto que muitos dos incidentes de vazamentos envolvem falhas comportamentais.

Por isso, nos termos da Resolução (art. 3º), deve-se contemplar as seguintes medidas: (i) os procedimentos e os controles adotados para reduzir a vulnerabilidade da instituição a incidentes; (ii) os controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis; (iii) o registro, a análise da causa e do impacto, bem como o controle dos

---

[337] Os *bots* ruins interagem com os aplicativos da mesma forma que um usuário legítimo, tornando-os mais difíceis de detectar e prevenir. Eles permitem abusos em alta velocidade, uso indevido e ataques a *sites*, aplicativos móveis e APIs. Também, permitem que operadores de *bots*, invasores, concorrentes desagradáveis e fraudadores executem uma ampla gama de atividades maliciosas. Essas atividades incluem *web scraping*, mineração de dados competitivos, coleta de dados pessoais e financeiros, *login* de força bruta, fraude de anúncio digital, *spam*, fraude de transação e muito mais.

efeitos de incidentes relevantes para as atividades da instituição; e (iv) os mecanismos para disseminação da cultura de segurança cibernética na instituição.[338]

Já a Resolução 4.752 altera algumas disposições específicas da Resolução 4.658/18, de forma que: (i) a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem, bem como (ii) toda e qualquer alteração contratual que implique na modificação das informações previamente informadas ao Banco Central do Brasil (BACEN), devem ser comunicadas em até 10 (dez) dias após a contratação dos serviços ou alteração contratual. Anteriormente, referidas comunicações deveriam ser feitas previamente e com, no mínimo, 60 (sessenta) dias de antecedência da contratação ou alteração contratual. Agora, no caso, da contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior, a R. 4.752 institui que, em caso da não existência de convênio para troca de informações entre BACEN e autoridades supervisoras dos países onde os serviços poderão ser prestados, a instituição contratante deverá solicitar ao BACEN autorização para (i) a contratação do referido serviço; e (ii) as alterações contratuais que impliquem modificação das informações já prestadas ao BACEN.[339]

Ou seja: a obrigatoriedade da implementação de politicas de segurança cibernética, com estabelecimento de conteúdo mínimo da referida politica de segurança; bem como, estabelecer um plano de ação e resposta a incidentes de segurança da informação e de designação do diretor responsável pela segurança cibernética da instituição financeira. Além disso, estabelecimento de exigências mínimas para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, com requisitos para contratação desses serviço quando prestados no exterior, com dever de comunicação prévia, pelas instituições, ao BACEN a respeito da contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem; estabelecimento de regras especificas para o tratamento dos incidentes relacionados ao ambiente cibernético, incluindo o desenvolvimento de ações para o compartilhamento de informações

---

[338] FRAZÃO, Ana; TEPENDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** 2.ed. São Paulo: Thomson Reuters Brasil, 2020, p.417-418.

[339] BANCO CENTRAL DO BRASIL. **Resolução nº 4.752,** de 26 de setembro de 2019. Disponível em: < https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50846/Res_4752_v1_O.pdf>. Acesso em: 15 out. 2020.

sobre os referidos incidentes; e a possibilidade do BACEN vetar ou impor restrições para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem quando constar a inobservância do disposto na resolução.[340]

Tendo em vista as regras de cibersegurança apresentadas acima, é importante mencionar, também, a Circular nº 3.909 de 16/08/2018, que trouxe a obrigatoriedade de implementação de uma 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.[341] Para tanto, a norma apresenta regras e diretrizes voltadas ao tratamento preventivo e reativo de incidentes de segurança, exigências mínimas para a contratação de serviços que envolvam dados e atribuições de responsabilidade dentro da instituição de pagamento.

Cabe destacar, também, mais um dispositivo para contribuir nesse trabalho de blindagem digital das instituições financeiras, a Circular BACEN 3.979/2020, publicada em 30 de janeiro de 2020. O documento dispõe sobre:

> A constituição e a atualização da base de dados de risco operacional e a remessa ao Banco Central do Brasil (BACEN) de informações relativas a eventos de risco operacional. A norma equipara risco cibernético ao risco operacional agindo de forma preventiva para construção de um sistema financeiro mais robusto, visando, de forma geral, a proteção dos dados dos clientes sob sua custódia. Logo, as instituições devem manter uma base de dados de risco operacional e mandar informes regulares ao BACEN. As informações que constarem da base de dados de risco operacional devem ser encaminhadas ao BACEN com periodicidade semestral, relativas a 30 de junho e 31 de dezembro de cada ano e abranger um período de dez anos (no entanto, para as informações encaminhadas de 2021 a 2025, a abrangência de dados vai de 5 a 9 anos). Além do envio das informações semestralmente, deve-se encaminhar informações de forma individualizada, em relação a cada evento, quando o valor da perda bruta acumulada, for igual ou superior a R$ 1.000,00 ou o valor do risco não coberto por provisão, for igual ou superior a R$10.000.000,00. Os demais riscos, devem ser enviados nos relatórios semestrais. Os processos relacionados a constituição do gerenciamento da base de dados de risco operacional devem ser avaliados periodicamente pela auditoria interna da instituição, pelo menos no que diz respeito a sua abrangência, consistência, integridade e confiabilidade. Essas informações devem ser mantidas à disposição do

---

[340] PALHARES, Felipe. et al. **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020, p.140.

[341] BANCO CENTRAL DO BRASIL. **Circular nº 3.909,** de 16 de agosto de 2018. Disponível em: < https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50645/Circ_3909_v1_O.pdf>. Acesso em: 15 out. 2020.

> BACEN por no mínimo dez anos. A circular publicada entrou em vigor no dia 1º de dezembro de 2020.[342]

Daí a importância das regras claras por meio de regulamentações específicas, pois tende a ser um grande desafio de ordem prática harmonizar as relações com as novas legislações de proteção de dados, especialmente quando no campo de execução pelo ente privado. Isso porque há um paradigma natural entre segurança e privacidade. E quanto maior a necessidade de prevenção e de combate ao crime, maior a necessidade de análise detalhada de informações pessoais com uso de diversas bases cruzadas. Devemos lembrar que a visão de gestão de riscos deve ser holística, e que o setor financeiro está abarcado por um rol de resoluções que iniciam lá na 4.557, alcançam a recente Circular 3.978/2020 de combate à lavagem de dinheiro e que chegam até mesmo na implementação das medidas exigidas pela nova legislação de proteção de dados pessoais Lei 13.709/2018 (LGPD).

É importante mencionar, ainda, o relatório Global Risks Report 2020, em sua 15º edição, publicado pelo Fórum Econômico Mundial com o apoio da Marsh & McLennan, e Zurich Insurance Group, que oferece uma ampla perspectiva sobre as principais ameaças que podem afetar a prosperidade mundial, verificou que os ataques cibernéticos são considerados o segundo risco mais preocupante que o universo dos negócios enfrentará na próxima década em todo o mundo. De acordo com a opinião dos mais de 750 especialistas e tomadores de decisão que foram consultados para a elaboração do relatório, 76,1% espera que os ataques cibernéticos aumentem em infraestrutura em 2020, e 75% aguarda um aumento nos ataques em busca de dinheiro ou dados. Por sua vez, percebe-se que a Inteligência Artificial, a tecnologia móvel de 5º geração (5G) e a computação quântica estão criando não apenas oportunidades, mas também novas ameaças.[343]

No mesmo sentido, Frank Dickson, vice-presidente do programa, Produtos de Segurança Cibernética, IDC afirma que:

> Quantidades sem precedentes de dados confidenciais estão sendo armazenados em ambientes com várias nuvens por organizações em todo o mundo. Ter a segurança certa na nuvem nunca foi tão

---

[342] BANCO CENTRAL DO BRASIL. **Circular nº 3.979,** de 30 de janeiro de 2020. Disponível em: < https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50913/Circ_3979_v1_O.pdf>. Acesso em: 15 out. 2020.

[343] WORLD ECONOMIC FORUM. **The Global Risks Report 2020**. 15.ed. Disponível em: < http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf>. Acesso em: 15 out. 2020.

> importante. Conforme as redes 5G são implementadas, a IoT continua a se expandir e a computação quântica está cada vez mais perto de se tornar uma realidade, as organizações devem adotar uma mentalidade de proteção de dados mais moderna. O primeiro passo para proteger os dados confidenciais é saber onde encontrá-los. Depois de classificados, esses dados devem ser criptografados e protegidos com uma forte estratégia de gerenciamento de chaves em várias nuvens.[344]

Ainda, assim, é importante mencionar que no dia 06 de fevereiro de 2020, foi publicado o Decreto nº 10.222/2020 que regulamenta a chamada “E-Ciber (Estratégia Nacional de Segurança Cibernética)”. O referido decreto instituiu as ações estratégicas e os objetivos relacionados à segurança da informação, em consonância com as políticas públicas e os programas do Governo federal, sendo construída em módulos, para contemplar a segurança cibernética, a defesa cibernética, a segurança das infraestruturas críticas, a segurança da informação sigilosa e a proteção contra vazamento de dados e terá validade no quadriênio 2020-2023. Os objetivos estratégicos são: (a)Tornar o Brasil mais próspero e confiável no ambiente digital; (b) Aumentar a resiliência brasileira às ameaças cibernéticas; e (c) Fortalecer a atuação brasileira em segurança cibernética no cenário internacional. Além disso, há também uma introdução genérica que aborda avanços da tecnologia, revolução digital e a necessidade de proteção do espaço cibernético.

A seguir, para evitar incidentes, algumas medidas vêm sendo adotadas, no sentido de desenvolver e estabelecer controles internos no combate aos ciberataques, conforme (quadro 3) abaixo:

---

[344] THALESGROUP. **Relatório de Ameaças de Dados Thales de 2020.** Disponível em: < https://www.thalesgroup.com/en/group/journalist/press-release/global-cloud-tipping-point-2020-thales-data-threat-report-global>. Acesso em: 27 jul. 2020.

Quadro 3 – Medidas no combate aos ciberataques

Função	Descrição
Definição de papéis e responsabilidades	Indicação do executivo e área responsável pela implementação do programa de segurança cibernética, assim como pela tratativa de incidentes.
Definição de perfis de acesso aos sistemas, rede, base de dados e servidores	Matriz de perfis de acesso, segregando claramente responsabilidades e funções, de forma a evitar acessos indevidos e possibilitar o monitoramento dos acessos.
Regras para a definição de senha	Regras mínimas sobre quantidade e tipos de caracteres utilizados nas senhas e periodicidade de troca.
Monitoramento do uso de internet	Regras para a utilização da internet, bloqueio de sites que podem gerar riscos adicionais e monitoramento do uso dos colaboradores.
Regras para download	Definir regras de download, evitando que ocorram downloads de arquivos de fonte duvidosa, assim como itens desnecessários.
Regras para upload	Restringir a permissão de upload em sites de internet somente a usuários autorizados por alçada competente, com procedimentos de revisão periódica.
Controles para utilização de e-mails, mídias e periféricos	Regras para a permissão do uso e monitoramento de tais ferramentas, de forma a evitar a entrada de itens lesivos e/ou a saída de informações confidenciais/sensíveis. Monitoramento e concessão de envio de e-mails externos, bem como a proibição do uso de serviços de e-mails externos (ex.: gmail, hotmail, yahoo etc.).
Trilhas de auditoria e guarda dos logs	Arquivar trilhas de auditoria e logs, permitindo a verificação de comandos suspeitos e acessos indevidos. Definir também o tempo de guarda dos logs.
Regras de backup	Prever periodicidade para a realização dos backups, forma de armazenamento e controle de acesso, garantindo que todas as informações tenham fonte de dados secundária e segura.
Controle de entrada e saída de equipamentos	Controlar a movimentação dos equipamentos para garantir que não sejam alterados.
Controle de prestadores de serviço	Regras para controle do acesso físico e lógico dos prestadores de serviço, além de cláusulas de confidencialidade na contratação desses terceiros.
Softwares de segurança	Utilização de softwares de segurança como firewalls, antivírus e outros.
Atualização dos sistemas, infraestruturas e softwares	Manter os sistemas, infraestruturas e softwares sempre atualizados.
Classificação da informação	Regras para a classificação das informações, impedindo o acesso ou divulgação indevida ou exigindo a sua criptografia.
Ciclo de vida da informação	Processos seguros para o devido manuseio, armazenamento, transporte e descarte das informações.
Disseminação da cultura de segurança	Mecanismos adotados para divulgar o programa contra ataques cibernéticos, tais como realização de treinamentos, criação de canais de comunicação interna ou simulações.

Fonte: CIO[345]

Com base nessas informações, pode-se concluir que vivemos novos tempos, onde a transformação digital não é apenas tecnológica. Não basta ter a tecnologia, é preciso educar na prevenção de riscos, visto que muitos dos incidentes de vazamentos envolvem falhas comportamentais, e por isso, as instituições financeiras precisam implementar mecanismos de disseminação de cultura de segurança com medição de resultados apuráveis. Ou seja, todos aqueles que lidam com informações sensíveis devem liderar o processo de transformação de cultura, que deve ser disseminada para os prestadores de serviço e terceirizados, usuários e

[345] CIO. **Anbima lança guia de cibersegurança para instituições financeiras.** Disponível em: < https://cio.com.br/noticias/anbima-lanca-guia-de-ciberseguranca-para-instituicoes-financeiras/>. Acesso em: 13 set. 2020.

clientes. A campanha deve funcionar de dentro e para fora da instituição, com um amplo alcance e relevância.

Esclarecida a dinâmica acerca da segurança da informação, segurança digital, e cibersegurança, cabe agora, enfrentar, ainda, a questão da privacidade. Para a devida compreensão, deve-se fazer uma análise sobre o assunto, questionando-se alguns pontos importantes, como se verá a seguir.

4.3 PRIVACIDADE

Antes de nos atentarmos à privacidade, é o momento de compreender algumas noções básicas sobre à proteção de dados. No entanto, é importante ressaltar que o assunto será aprofundado mais á frente, mediante análise da Lei Geral de Proteção de Dados (LGPD).

Primeiramente, a proteção de dados situa-se entre os direitos da personalidade, pois, também, interfere na dimensão relacional e social do ser humano.[346] Logo, a proteção de dados se firmou, como um pilar para consolidação de um ambiente democrático, livre, e que respeite a privacidade, a liberdade e a igualdade dos indivíduos, ou seja, o bem jurídico protegido pelo direito à proteção de dados se mostra mais amplo, abarcando também a integridade física e moral, a privacidade e a personalidade da pessoa, as liberdades em geral e a igualdade, como componentes da própria dignidade da pessoa humana.[347]

Como já mencionado, a era da informação é marcada pela possibilidade de conexão e compartilhamento de dados nunca antes visto. Hoje é possível se conectar com pessoas de qualquer lugar do mundo e trocar informações instantaneamente. Por certo, em uma sociedade cada vez mais orientada e movida por dados (*data-driven society*), com alta velocidade de processamento de dados e infindáveis formas de captura de informações, não se pode deixar perder de vista o direito à proteção desses dados.

Fazendo um paralelo, com a Pandemia Covid-19, que vem assolando o planeta desde o final de 2019, o que vence a luta contra o novo corona vírus é a

---

[346] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. Rio de janeiro: Forense, 2020, p.83.
[347] PALHARES, Felipe. et al. **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020, p.502.

informação. Este é o principal consenso entre diversos especialistas de várias áreas em todo o mundo. Por isso a importância do combate efetivo à propagação de noticias falsas e desinformação, assim como a relevância de todos colaborarem com dados atualizados. A pandemia intensificou o uso de tecnologia, que por sua vez, aumentou o tratamento de dados pessoais. Além disso, nunca foi tão necessário tratar dados sensíveis e compartilhar estas informações. A utilização de dados para a contenção da crise tem sido, portanto, essencial e uma das ferramentas mais poderosas na atuação global para impedir o avanço ainda maior da pandemia e de seus efeitos.[348]

Com isso, o recolhimento de informações privadas pelos sistemas automatizados, sem que sequer saiba o cidadão que seus dados estão sendo compilados; a troca de informações por órgãos públicos ou por instituições, ampliando significativamente o volume de dados; a capacidade de armazenamento de milhões e milhões de informações; a contínua diminuição dos custos de geração, transmissão, arquivamento e tratamento de dados; e, finalmente, por mais simples que possam parecer individualmente alguns dados, os resultados cada vez mais complexos dos tratamentos informatizados, com efetivo risco de violação à proteção dos mesmos.

Contudo, o usuário tem o direito de não querer passar seus dados, bem como o de não querer que a instituição use sua informação; assim como a instituição tem o direito de não querer tê-lo como cliente. Se o usuário não concorda com os termos e políticas, não consegue seguir adiante. E, mesmo concordando com tudo, se deixar de ser usuário do serviço, seus dados continuam com a instituição, em geral, para sempre, para qualquer propósito.[349]

Por essa razão, a proteção de dados se provou como um dos temas mais recorrentes no meio de tecnologia. Desde 2018, diversos países sancionaram legislações de proteção de dados, blocos econômicos definiram diretrizes e agências nacionais de proteção de dados foram criadas. Todos esses eventos foram permeados por escândalos sobre vazamento de dados e uso não autorizado de dados, inclusive para fins eleitorais. De fato, 2018 foi o ano da proteção de dados,

---

[348] PALHARES, Felipe. et al. **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020, p.491-512.
[349] PINHEIRO, Patrícia Peck. **Direito Digital**. 5 ed. São Paulo: Editora Saraiva, 2013. Livro eletrônico, não paginado

seja sob a ótica das discussões sobre proteção e governança de dados, seja por conta das diversas violações ou vazamentos de dados de instituições financeiras.[350]

A vista disso, a proteção de dados é resultado da sociedade da informação. Com o surgimento de computadores e, em seguida, bancos de dados, o controle sobre a informação – e, em especial, dados – passa a ser visto como uma forma de poder. A preocupação com a proteção de dados deriva da percepção da amplitude e potencialidade de controle e manipulação sobre a sociedade e o mercado que este tipo de dado oferece. A proteção deste tipo de dado faz-se importante pela forma como são divulgados e tratados, a manter seus titulares em uma condição de vulnerabilidade.[351]

Dessa forma, percebe-se que os brasileiros estão desconfiados quanto aos conteúdos que circulam na *web* e inseguros em relação à proteção dos seus dados. Ainda, assim, sobre a proteção dos dados, tema que está mais em pauta após a entrada em vigor da Lei Geral de Proteção de Dados (LGPD) em setembro de 2020, as opiniões ficam divididas: 38% dizem que suas informações pessoais estão mais seguras hoje do que há cinco anos, enquanto outros 38% pensam o oposto. Para 21%, o nível de segurança continua o mesmo.[352] Dito isso, deve ser garantido aos indivíduos o direito de domínio sobre os seus dados para que tenham a livre escolha de compartilhar com quem lhe interessar, escolher conteúdos que são do seu interesse, debater temas, promover pesquisas. Assegurando-lhes a liberdade. Certamente esse é um grande desafio de transformação aos atores que promovem e fomentam a atual sociedade da informação: utilizar a tecnologia como ferramenta de garantia à proteção de dados.[353]

Entendido algumas noções básicas sobre a proteção de dados, é momento de compreender melhor a privacidade, fazendo uma importante exposição dos

---

[350] PALHARES, Felipe. et al. **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020, p.109.

[351] VERGILI, Gabriela Machado. **Análise comparativa entre direito à privacidade e direito à proteção de dados pessoais e relação com o regime de dados públicos previsto na Lei Geral de Proteção de Dados.** Disponível em: < https://dataprivacy.com.br/analise-comparativa-entre-direito-a-privacidade-e-direito-a-protecao-de-dados-pessoais-e-relacao-com-o-regime-de-dados-publicos-previsto-na-lei-geral-de-protecao-de-dados/>. Acesso em: 19 out. 2020.

[352] Revista CIAB - FEBRABAN. 2020. **Brasileiros se preocupam com *fake news* e são dependentes da internet, mostra estudo.** Disponível em: < https://noomis.febraban.org.br/videos/brasileiros-se-preocupam-com-fake-news-e-sao-dependentes-da-internet-mostra-estudo?pesquisa=prote%C3%A7%C3%A3o%20de%20dados>. Acesso em: 19 out. 2020.

[353] TUMELERO, Thays. **Por que a privacidade importa tanto?** Disponível em: < https://www.nsctotal.com.br/noticias/por-que-a-privacidade-importa-tanto>. Acesso em: 19 out. 2020.

pontos mais relevantes sobre o assunto. Não se pretende, aqui, (re)elaborar um novo conceito de privacidade, mas, tão somente, resgatar a importância desse direito basilar à própria democracia, como se verá a seguir.

Primeiramente, privacidade significa coisas distintas para pessoas diferentes. Em geral, privacidade é o direito de ser deixado em paz e o direito de estar livre de instruções pessoais fora de propósito. Em muitos países, já faz tempo que a privacidade representa uma questão legal, ética e social.[354]

Contudo, não há um consenso entre os doutrinadores quanto á definição de privacidade, o que pode dificultar o entendimento conceitual desse princípio. A Constituição Federal não fala em privacidade, mas sim o seu artigo 5º, X, dispõe sobre a intimidade, vida privada, honra e imagem das pessoas.[355]

Por isso, via de regra, a privacidade (*privacy*) pode ser definida como o direito de estar só ou, talvez mais preciso, o direito de ser deixado só ("*right to be let alone*").

Patrícia Peck Pinheiro, esclarece em sua obra que:

> O direito à privacidade constitui um limite natural ao direito à informação. No entanto, não há lesão a direito se houver consentimento, mesmo que implícito, na hipótese em que a pessoa demonstra de algum modo interesse em divulgar aspectos da própria vida. Assim como há limites naturais ao direito à privacidade quando atinge interesses coletivos. Neste caso, a predominância do interesse coletivo sobre o particular requer verificação caso a caso. Ademais, todo indivíduo deve ter direito a proteção de sua privacidade. Isso é indiscutível. Além disso, a privacidade dos usuários, além de uma garantia, deve, também, ser protegida, porque as informações dos usuários viraram moeda e são usadas como pagamento dos serviços que se dizem gratuitos, mas que retêm as informações dos indivíduos para sempre, utilizando-a para qualquer fim.[356]

Importante salientar, ainda, que a interpretação de privacidade vem mudando substancialmente, devido às mudanças trazidas pelos avanços tecnológicos e a maior vulnerabilidade a que o titular dos dados pessoais está exposto.

A título de exemplo, em 2001, no julgamento do REsp 306.507/SP, Relatora a Ministra Eliana Calmon, reconheceu-se que o "contribuinte ou o titular da conta bancária tem direito à privacidade em relação aos seus dados pessoais". No REsp

---

[354] SHARDA, Ramesh; DELEN, Dursun; TURBAN, Efraim. ***Business intelligence* e análise de dados para gestão do negócio.** Tradução: Ronald Saraiva de Menezes. 4.ed. Porto Alegre: Bookman, 2019, p.532.

[355] TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei geral de proteção de dados pessoais:** comentado artigo por artigo. 2.ed. ver., atual e ampl. Salvador: Editora JusPodivm, 2020, p.32.

[356] PINHEIRO, Patrícia Peck. **Direito Digital**. 5 ed. São Paulo: Editora Saraiva, 2013. Livro eletrônico, não paginado

1.168.547/RJ, Relator o Ministro Luís Felipe Salomão, julgado em 2010, assentou-se a existência de um novo conceito de privacidade, bem como a necessidade de consentimento do interessado para divulgação de informação pessoal a seu respeito, pois, com o desenvolvimento da tecnologia, a tutela da privacidade passa a ter ponto de referência o consentimento do interessado para "dispor com exclusividade sobre as próprias informações, nelas incluindo o direito à imagem".[357]

Por conta disso, privacidade como autodeterminação informativa/existencial e reconhecimento da construção dinâmica da identidade pessoal conjugam-se, assim, como novas formas de manifestação de projeção jurídica da pessoa humana contra as ameaças de estigmatização e discriminação oriundas do desenvolvimento tecnológico.[358]

Ou seja: a privacidade hoje, longe de se restringir à intimidade e ao direito de ser deixado só, ampliou seus domínios para abranger o controle sobre as informações que digam respeito ao sujeito, a autodeterminação informativa, o direito à não discriminação, a liberdade, a igualdade, o direito ao acesso e acompanhamento dos dados pessoais quando se tornam objeto de disponibilidade de outros, dentre outros.[359]

Historicamente, a preocupação com aspectos relacionados à privacidade tem sido recorrente e o tema muito estudado por doutrinadores. Privacidade é um conceito aberto, altamente subjetivo e atualmente a expressão tem sido utilizada para, de forma genérica, inferir uma série de outros conceitos que podem se confundir com parte ou com o todo, o que tem feito com que a legislação aborde o tema de forma fragmentada.[360]

Em razão disso, percebe-se que privacidade é uma das palavras mais multifacetadas que se pode trazer ao debate, com seus vários sentidos atribuídos em vários tempos e por várias culturas. Sua compreensão remete a um conceito

---

[357] FRAZÃO, Ana; TEPENDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** 2.ed. São Paulo: Thomson Reuters Brasil, 2020, p.87.
[358] FRAZÃO, Ana; TEPENDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** 2.ed. São Paulo: Thomson Reuters Brasil, 2020, p.447.
[359] FRAZÃO, Ana; TEPENDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** 2.ed. São Paulo: Thomson Reuters Brasil, 2020, p.107.
[360] PALHARES, Felipe. et al. **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020, p.104.

fluido, melhor compreendido quando dividido em três dimensões distintas, porém complementares (decisional, informacional e espacial). Em cada uma dessas dimensões se pode identificar os problemas a elas relativos e, a partir daí, localizar o direito violado.[361] Assim, conversas sobre privacidade devem ser baseadas na ética e na confiança. A conversa deve passar de "Estamos em conformidade?" para "Estamos fazendo a coisa certa?"

A título de curiosidade, o termo privacidade teve origem em 1890, onde dois juristas americanos, Samuel D. Warren e Louis D. Brandeis, publicaram na *Harvard Law Warren*, um estudo considerado um marco na história do direito moderno, ao sustentarem que novos inventos e métodos comerciais reclamavam o surgimento de um novo direito fundamental do cidadão, construído a partir de direitos clássicos de proteção à pessoa e à propriedade, e que eles denominaram direito à privacidade (the *right to privacy*).

O texto, que inicia com a afirmação de que do direito à vida logo se passou ao direito de aproveitar a vida (*right to enjoy life*), ou o direito de ser deixado em paz (t*he right to be let alone*), salienta que o direito à propriedade teve seu alcance ampliado para a noção de propriedade intangível. Os autores afirmaram, também, que as mudanças políticas, sociais e econômicas, bem como o avanço tecnológico, requereram o reconhecimento e a criação de novos direitos, construídos a partir de direitos clássicos de proteção à pessoa e à propriedade e que eles denominaram direito à privacidade, correspondente nas palavras do juiz americano Cooley, ao direito de ser deixado em paz, de estar só.[362] Além disso, os autores questionam se haveria, no *common law*, um fundamento para a proteção à privacidade dos indivíduos, e qual seria sua natureza e extensão.[363]

---

[361] PEIXOTO, Erick Lucena Campos; JÚNIOR, Marcos Ehrhardt. Os desafios da compreensão do direito à privacidade no sistema jurídico brasileiro em face das novas tecnologias**. REVISTA JURÍDICA LUSO-BRASILEIRA (RJLB)**, ANO 6 (2020), n.º 2, ISSN: 2183-539X, p.389-418. Disponível em: < https://www.cidp.pt/revistas/rjlb/2020/2/2020_02_0389_0418.pdf>. Acesso em: 19 out. 2020.

[362] MACEDO, Fernanda dos Santos; BUBLITZ, Michelle Dias; RUARO, Regina Linden. A *privacy* norte-americana e a relação com o direito brasileiro. **Revista Jurídica Cesumar.** v. 13 n. 1, p. 161-178, jan./jun.2013 - ISSN 1677-64402. Disponível em: < https://periodicos.unicesumar.edu.br/index.php/revjuridica/article/view/2666/1898>. Acesso em: 19 out. 2020.

[363] FRAZÃO, Ana; TEPENDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** 2.ed. São Paulo: Thomson Reuters Brasil, 2020, p.54.

No contexto brasileiro, a privacidade já era tutelada no ordenamento jurídico de forma indireta e majoritária em legislação esparsa ou setorial, de acordo com os seguintes marcos normativos:

> 1. A Constituição Federal de 1988 em seu artigo 5º, cujo status é de clausula pétrea, faz referência a direitos invioláveis do cidadão e cita diferentes vertentes da privacidade, dentre elas se destacam a intimidade, a inviolabilidade do domicilio e de correspondência.
> 2. O Código de Defesa do Consumidor (CDC), de 1990 dá ao consumidor o direito de ter acesso às suas informações pessoais e às suas respectivas fontes. Além disso, também prevê que cadastros não podem conter informações negativas por período superior a 5 anos e que, caso houver, o consumidor pode exigir imediata correção de incongruência em seus dados.
> 3. A lei nº 9.507 de 1997 (Lei do habeas Data) regula o direito de acesso a informações e disciplina o rito processual do habeas data. O habeas data permite que a pessoa tenha direito a assegurar o conhecimento de suas informações em registros ou banco de dados de entidades governamentais ou de caráter público.
> 4. O Código Civil de 2002 traz à tona a vida privada e a divulgação de informações sensíveis que, por meio de solicitação do indivíduo, pode ser proibida. Outro ponto relevante que o Código Civil trouxe para a privacidade é o pseudônimo, que é o artificio adotado para a proteção do nome de um indivíduo.
> 5. A Lei 12.414 de 2011 (Lei do cadastro positivo) disciplina a formação e consulta de bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. A lei limita o conteúdo dos bancos de dados a informações de adimplemento que sejam necessárias para avaliar a situação econômica de um indivíduo.
> 6. A Lei nº 12.527 de 2011 (Lei de Acesso à Informação), regula o acesso (i) às informações fornecidas por órgãos públicos que possam ser de interesse particular ou coletivo, (ii) a registros administrativos e a informações sobre atos de governo, e (iii) à gestão da documentação governamental e as providências para franquear sua consulta a quantos dela necessitem. A LAI prevê que o tratamento de informações pessoais deve ser feito de forma transparente e que respeite a intimidade e a vida privada das pessoas. Ademais, estabelece regras para o acesso e divulgação dessas informações.
> 7. A Lei nº 12.965 de 2014 (Marco Civil da Internet), estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Tal lei tem como princípio a proteção da privacidade, mas não garante a privacidade. Suas disposições estão mais focadas em regras de consentimento, segurança e contextualização da informação que eventualmente podem tangenciar o tema. Não é uma normativa geral sobre proteção de dados pessoais.[364]

O cenário acima descrito, demonstra que no Direito brasileiro, a Privacidade é tão importante que possui menção em determinados regulamentos. O mais importante é a figura do Habeas Data (Art. 5º, LXXII, CF e a Lei 9.507/1997), remédio para proteção da esfera íntima dos indivíduos e, contra usos abusivos de registros de dados pessoais coletados por meios ilícitos e meios de evitar a

[364] PALHARES, Felipe. et al. **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020, p.106-109.

introdução de dados sensíveis nestes arquivos. Visa também desfazer a conservação de dados falsos ou com fins diversos dos previstos em lei. Como se vê, o direito à privacidade tem proteção constitucional e infraconstitucional, e, é considerado Direito de Personalidade, ou seja, um direito que faz parte do próprio ser humano e que não deve ser definido sob a ótica do segredo. Atualmente, são quase inexistentes as informações que permanecem em absoluto sigilo. Na verdade, imaginar que o fato de uma informação não se mostrar como segredo não retira dela a proteção à privacidade.[365] Logo, é inegável a importância adquirida pelo direito à privacidade nos últimos anos. É retrato da nossa sociedade contemporânea, dominada pelos meios de comunicação de massa e as diversas redes sociais.

Segundo dados do relatório sobre a responsabilidade de dados corporativos, publicado pelo grupo KPMG, nos Estados Unidos, 87% das pessoas acreditam que a privacidade de dados é um direito humano. O relatório também mostra que 56% dos cidadãos querem ter mais controle sobre os seus dados pessoais.[366]

Assim, ao se atribuir a característica de “privado” a uma certa coisa, a um determinado assunto, quer se dizer que há uma restrição onde alguém tem um nível de acesso mais profundo que outra pessoa. Há uma relação desigual aqui: uma pessoa tem mais acesso que outra, tendo o poder de restringir, de controlar esse acesso. Essa é a chave para o entendimento da privacidade, já que carrega o significado de proteção contra o acesso indesejado à coisa por terceiros. Na maioria das vezes, quando se diz que um indivíduo sofreu uma violação da privacidade, na verdade, o que se está querendo dizer é que ocorreram várias violações em vários direitos da privacidade, e até em dimensões diferentes desta. Uma pequena postagem em uma rede social pode facilmente ferir o direito à honra, à imagem, à proteção de dados pessoais, à intimidade etc., os chamados dados sensíveis, cuja proteção é uma das principais preocupações na chamada sociedade da informação.

De acordo com Daniel J. Solove, em seu artigo intitulado Privacy Self-Management and the Consent Dilemma, v. 126 Harvard Law Review 1880 (2013), há seis pontos importantes, sobre privacidade, que merecem destaque:

---

[365] DA SILVA, Luciana Vasco. Direito de privacidade no direito brasileiro e norte americano. **Revista Eletrônica do Curso de Direito - PUC Minas Serro,** n.12, p.68-82, ago. / dez. 2015 – ISSN 2176-977X. Disponível em: < http://periodicos.pucminas.br/index.php/DireitoSerro/article/view/9051>. Acesso em: 19 out. 2020.

[366] KPMG. **The new imperative for corporate data responsibility.** Disponível em: < https://advisory.kpmg.us/content/dam/advisory/en/pdfs/2020/consumer-data-report-kpmg.pdf>. Acesso em: 19 out. 2020.

> 1. A abordagem regulatória atual para proteger a privacidade envolve o que chamo de "autogestão da privacidade" – a lei fornece às pessoas um conjunto de direitos que lhes permite decidir como pesar os custos e benefícios da coleta, uso ou divulgação de suas informações. O consentimento das pessoas legitima praticamente qualquer forma de coleta, uso e divulgação de dados pessoais. Infelizmente, a autogestão da privacidade está sendo solicitada a trabalhar além de suas capacidades. O autogerenciamento da privacidade não oferece controle significativo sobre os dados pessoais.
> 2. A pesquisa em ciências sociais e empíricas minou as principais suposições sobre como as pessoas tomam decisões em relação a seus dados, suposições que sustentam e legitimam o modelo de autogestão da privacidade.
> 3. As pessoas não conseguem autogerir adequadamente sua privacidade devido a uma série de problemas estruturais. Há muitas entidades que coletam e usam dados pessoais para tornar viável para as pessoas gerenciarem sua privacidade separadamente com cada entidade. Além disso, muitos danos à privacidade são o resultado de uma agregação de pedaços de dados durante um período de tempo por diferentes entidades. É virtualmente impossível para as pessoas pesar os custos e benefícios de revelar informações ou permitir seu uso ou transferência sem uma compreensão dos potenciais usos posteriores.
> 4. O autogerenciamento da privacidade trata da privacidade em uma série de transações isoladas guiadas por determinados indivíduos. Os custos e benefícios da privacidade, no entanto, são avaliados de forma mais apropriada de forma cumulativa e holística – não apenas no nível individual.
> 5. Para avançar, a lei e a política de privacidade devem enfrentar um dilema complexo e confuso com o consentimento. O consentimento para a coleta, uso e divulgação de dados pessoais muitas vezes não é significativo, e a solução mais aparente – medidas paternalistas – nega ainda mais diretamente às pessoas a liberdade de fazer escolhas consensuais sobre seus dados.
> 6. O caminho a seguir envolve (1) o desenvolvimento de uma abordagem coerente para o consentimento, que dê conta das descobertas das ciências sociais sobre como as pessoas tomam decisões sobre dados pessoais; (2) reconhecer que as pessoas podem se envolver na autogestão da privacidade apenas seletivamente; (3) ajustar o tempo da lei de privacidade para focar nos usos posteriores; e (4) desenvolver regras de privacidade mais substantivas.[367] (Tradução livre)

De fato, a privacidade enfrenta um desafio atual, que é se reinventar numa sociedade da informação, numa nova revolução tecnológica construída nas bases da anterior. Toda estrutura de fluxo de informação construída nas décadas anteriores serve de suporte para esta nova fase do desenvolvimento tecnológico. *Big Data*, Internet das Coisas e vigilância/segurança são termos cada dia mais comuns e levam às grandes preocupações com a privacidade.

Por certo, a função de privacidade na maioria das empresas de serviços financeiros não é nova. As regulamentações existentes trouxeram alguma visibilidade para a função, com violações de dados que chamam a atenção nas

[367] SOLOVE. Daniel J. **Privacy Self-Management and the Consent Dilemma.** LinkedIn. Disponível em: < https://www.linkedin.com/pulse/20130521143630-2259773-my-new-article-privacy-self-management-and-the-consent-dilemma>. Acesso em: 19 out. 2020.

manchetes lançando uma luz ainda mais brilhante sobre o risco de privacidade. Mas a visibilidade é apenas um ponto de partida. Dada a natureza centrada no cliente do risco de privacidade, pode-se argumentar que a responsabilidade pela privacidade deve mudar para a primeira linha de defesa de uma instituição, aumentando sua estatura. Além disso, pode ser a hora de a função de privacidade refletir o aumento pós-crise de conformidade ou o aumento mais recente da segurança da informação. O risco de privacidade pode ganhar sua própria proeminência ao construir um modelo operacional sustentável em toda a primeira e segunda linhas de defesa da organização.

Cabe ressaltar, ainda, que cada vez mais informações são coletadas das pessoas, formando imensos bancos de dados organizados ou não, mas com os quais é possível determinar padrões de comportamento, de consumo, idade, gostos, entre diversas outras informações, que são utilizadas em um comercio de informações e num *marketing* tão segmentado e específico quanto se pode ser, afinal, um *marketing* feito no lugar correto, na hora correta, para a pessoa já interessada no seu produto tem muito mais chance de ser eficaz e resultar numa venda do que aquele feito para um grupo aleatório de pessoas, a titulo de exemplo, com idade entre dezoito e vinte e cinco anos, inclusive sendo forma de agregar valor ao produto. E por isso e outros motivos devemos falar sobre privacidade do indivíduo conectado, e especialmente do usuário de objetos conectados (ou inteligentes).[368]

Neste ponto, a informação pessoal está, quase como ato reflexo, ligada à privacidade por uma equação simples e básica que associa um maior grau de privacidade à menor difusão de informações pessoais e vice-versa. Esta equação nem de longe encerra toda a complexa problemática em torno dessa relação, porém pode servir como ponto de partida para ilustrar como a proteção das informações pessoais passou a encontrar guarida em nosso ordenamento jurídico: como um desdobramento da tutela do direito à privacidade.[369]

---

[368] TEIXEIRA, Tarcísio; LOPES, Alan Moreira; TAKADA, Thalles. **Manual jurídico da inovação e das startups.** 2.ed. Salvador: Editora JusPodivm, 2020, p.54.

[369] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law (EJJL**). Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: < https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315/658>. Acesso em: 19 out. 2020.

Dessa forma, movimentos ousados são necessários para acelerar a jornada para a privacidade – construída em uma estrutura de controle que reflete a nova realidade de risco na era da informação e focada em fornecer valor sustentável para os negócios.

Segundo a pesquisa Gartner, empresa de pesquisa e consultoria, prevê que até 2021, mais de 60% das grandes organizações terão um programa de gerenciamento de privacidade totalmente integrado ao negócio. Para muitas organizações, a responsabilidade pela privacidade não é clara ou equivocada, ou ambos. A resposta: os líderes de toda a organização têm um papel a desempenhar na tradução de requisitos e na priorização de ações de mitigação de riscos a privacidade.[370]

Com isso, percebe-se que qualquer cidadão tem o direito humano fundamental à privacidade e à proteção de seus dados garantido por lei. Assim, como a privacidade, essa proteção passa a ser essencial porque os dados potencialmente precisarão ser tratados, mas é necessário que sejam tratados de forma legitima, justa e transparente, para garantia e segurança que, mesmos em momentos e situações emergenciais, que exigem o atendimento de direitos da sociedade, direitos e garantias individuais e da coletividade serão resguardados. Logo, a proteção de dados e privacidade não pode ser relegada ao se invocar o interesse público, sendo necessário encontrar um equilíbrio para que as medidas cheguem ao seu fim sem restringir desproporcionalmente direitos fundamentais.[371] Ademais, em meio a pandemia da Covid-19, parece que finalmente estamos despertando para a importância da privacidade e proteção de dados. Algumas políticas púbicas têm chamado a atenção das pessoas para a discussão sobre a possível violação de suas vidas privadas. Dessa forma, a finalidade do uso de alguns dados se justifica desde que com a devida transparência e proporcionalidade. Além disso, a Privacidade é um Direito e a Proteção de Dados é o meio de garantir segurança jurídica a esse Direito.

Nesse sentido, a privacidade e a proteção de dados têm se destacado como novas frentes de evolução jurídica uma vez que tutelam direitos e aspectos que, até

---

[370] GARTNER. **The Call for Legal and Compliance to Minimize Data Privacy Risk.** Disponível em: < https://www.gartner.com/smarterwithgartner/call-legal-compliance-minimize-data-privacy-risk/>. Acesso em: 19 out. 2020.

[371] PALHARES, Felipe. et al. **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020, p.502-503.

a ampla adoção da *internet*, não despertavam tanta preocupação do público e dos operadores de Direito.[372]

Esclarecida a dinâmica sobre privacidade, na sequência, analisar-se-á a Lei Geral de Proteção de Dados, a fim de compreender melhor a sua importância e relevância, para o setor financeiro, como se verá a seguir.

4.3.1 Lei Geral de Proteção de Dados – LGPD

Na segunda metade do século XX a indústria tradicional passou a valorizar a informação e a tecnologia em maior escala, o que modificou o espaço geográfico global, e posteriormente culminou no advento da Terceira Revolução Industrial, também conhecida como a Era da Informação. Nessa nova etapa da sociedade industrial e da evolução histórica dos direitos humanos, a dignidade da pessoa humana perpassa pela proteção dos dados pessoais[373], em especial pelos dados sensíveis, o que propiciou a criação de novos regimes jurídicos que passaram a tutelar de modo mais rigoroso e pedagógico a coleta, armazenamento, tratamento, processamento, proteção e o sigilo dos dados.[374]

Por conta disso, o setor financeiro acostumado a lidar com sigilo e dados de clientes e usuários é objeto de profunda evolução tecnológica e a tempo investe significativamente em recursos e tecnologia. Não apenas à novas tecnologias aplicadas à forma de atendimento de clientes, mas à gestão da informação financeira destes que se torna matéria prima para novos avanços e aprimoramento dos serviços financeiros. Ao longo das últimas décadas, as informações esparsas e mantidas em papel foram substituídas por bases de dados eletrônicos e incluídas

---

[372] PALHARES, Felipe. et al. **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020, p.123.

[373] Conjunto de regras que visam impedir o tratamento inadequado, injusto ou antiético de dados pessoais. Está relacionado à chamada “privacidade informacional”. Enquanto a proteção à privacidade, em sentido mais amplo, está mais voltada à preservação da intimidade, a proteção de dados pessoais se concentra em resguardar, contra abusos e mau usos, os dados ou informações que dizem respeito a cada um de nós. Ao fazê-lo, a proteção de dados visa resguardar direitos de alta significância. Nesse sentido, o regime de proteção de dados pessoais é, em grande parte, baseado na “autodeterminação informativa” (*informationelle Selbstbestimmung*), ou seja, a regulação jurídica da privacidade informacional está fortemente amparada no conceito de que o indivíduo (no caso, o titular dos dados) deve poder controlar livremente as formas de coleta, uso e revelação de seus dados pessoais pela sociedade. Essa é a única maneira pela qual é garantida ao individuo a preservação da capacidade de livre desenvolvimento de sua personalidade, entre outros direitos fundamentais.

[374] TEIXEIRA, Tarcísio. **Empresas e a implementação da Lei Geral de Proteção de Dados.** 1.ed. Salvador: Editora JusPodivm, 2021, p.51-52.

em aplicativos, de modo a permitir a perenidade da informação, a facilidade de acesso e o cruzamento de dados, trazendo para essa indústria um novo horizonte e imprimindo um novo dinamismo. No entanto, esse tipo de atividade deve andar em paralelo com o direito à privacidade e à proteção de dados pessoais dos usuários desses serviços. O crescimento exponencial no armazenamento de dados pessoais em sistemas informatizados traz, automaticamente, uma maior exposição de tais dados a um incidente de segurança, além de tornar mais fácil a eventual utilização não autorizada de tais informações.[375]

Como se pode notar, o fornecimento de dados pessoais para aquisição de produtos e serviços se tornou uma tarefa comum no mundo conectado. Os bancos de dados que contêm dados pessoais, tão comuns em nossos dias, proporcionam uma nova definição dos poderes e direitos a respeito das informações pessoais e, consequentemente, sobre a própria pessoa. Aumenta o número de sujeitos que podem ter acesso a um conjunto sempre mais detalhado e preciso de informações sobre terceiros, o que faz com que o estatuto jurídico desses dados se torne um dos pontos centrais que vão definir a própria autonomia, identidade e liberdade do cidadão contemporâneo. Logo, a análise sistemática de base de dados que reúne informações de clientes pode trazer benefícios incalculáveis a toda a coletividade e alterar a forma como o serviço é prestado.

Ademais, é importante lembrar que a informação sempre foi sinônimo de poder, e aquele que detém o privilégio do acesso irrestrito aos dados, pode, em algum momento, desviar o seu uso, se não forem criadas medidas de controle para coibir abusos.[376]

Cabe lembrar, ainda, que a proteção dos dados pessoais compõe uma das partes essenciais da tutela da dignidade da pessoa humana, mostrando-se essencial para a garantia das liberdades fundamentais, da igualdade, da solidariedade e da integridade psicofísica. O desenvolvimento de mecanismos destinados a regular o tratamento dos dados auxilia a evitar discriminação que não encontrem fundamento constitucional, como aquelas que possam dificultar o acesso ao crédito ou a empregos por determinados grupos. Além disso, afasta práticas que possam reduzir

---

[375] PALHARES, Felipe. et al. **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020, p.128-129.
[376] PALHARES, Felipe. et al. **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020, p.508.

a liberdade e autonomia dos indivíduos, como decisões a partir de análises de dados não informadas ao titular e sob critérios não transparentes. A tutela dos dados relativos à pessoa natural mostra-se hoje vital para que ela se realize integralmente e se relacione na sociedade, representando garantia de maior segurança às informações dos cidadãos e impedindo práticas autoritárias e de vigilância por parte de instituições públicas e privadas.[377]

Por esse e outros motivos, o tema “proteção de dados pessoais” recebe destaque na sociedade e com a aprovação da Lei Geral de Proteção de Dados Pessoais (LGPD), o Brasil inaugura o que se pode denominar de “sistema protetivo dos dados pessoais”. Essa lei deve ser entendida como tal, pois estabelece princípios que devem nortear a coleta, o compartilhamento e o tratamento dos dados pessoais, direitos básicos dos titulares dos dados pessoais, obrigações impostas aos controladores e responsáveis pelo tratamento desses dados.[378]

Além do mais, a lei foi criada com o fim de proteger e tutelar o direito à privacidade e garantir a inviolabilidade da intimidade, da honra e da imagem da pessoa natural e, com isso, o desenvolvimento econômico e tecnológico e a inovação. Assim, a LGPD se aplica a todo tipo de tratamento de dados pessoais, seja por meio biométrico, digital, eletrônico ou físico, por pessoa natural ou por pessoa jurídica de direito público ou privado. Faz-se a ressalva de que a lei não se aplica a tratamento de dados que sejam realizados por pessoa natural para fins particulares e não econômicos, ou fins jornalísticos, artísticos, acadêmicos, de segurança pública, de defesa nacional, de segurança do estado e de atividades de investigação e repressão de infrações penais, entre outras. Apesar disso, ainda assim é recomendado o cuidado com a proteção dos dados para que, independentemente de a lei não cobrir esses casos, continuem mesmo assim sendo preservados os direitos de intimidade e privacidade de terceiros.[379] Por fim, aos dados originados e destinados a outros países, que apenas passam pelo território nacional não será aplicável a lei brasileira, desde que o país de proveniência

---

[377] FRAZÃO, Ana; TEPENDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** 2.ed. São Paulo: Thomson Reuters Brasil, 2020, p.282.

[378] TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei geral de proteção de dados pessoais:** comentado artigo por artigo. 2.ed. ver., atual e ampl. Salvador: Editora JusPodivm, 2020, p.11-12.

[379] TEIXEIRA, Tarcísio; LOPES, Alan Moreira; TAKADA, Thalles. **Manual jurídico da inovação e das startups.** 2.ed. Salvador: Editora JusPodivm, 2020, p.281-282.

proporcione grau de proteção de dados semelhante ao dessa Lei, o que será avaliado pela autoridade nacional.[380]

Em paralelo, é impossível deixar de mencionar a Medida Provisória 954, de 17 de abril de 2020, que dispõe a respeito do compartilhamento de dados por empresas de telecomunicações com a Fundação Instituto Brasileiro de Geografia e Estatística (IBGE), em seu artigo 2º, determina que empresas de telecomunicação prestadoras de serviços telefônico fixo comutado e de serviço móvel pessoal disponibilizem ao IBGE a relação de nomes, número de telefone e endereços de seus consumidores – pessoas físicas ou jurídicas. É evidente, no escopo da LGPD, a proteção aos dados se estende apenas às pessoas físicas, mas é cristalino que a MP não fere somente os princípios basilares da legislação de proteção de dados pessoais, mas também as garantias fundamentais da dignidade da pessoa humana (artigo 1º, III, da CF), da inviolabilidade, da intimidade, da vida privada, da honra e da imagem das pessoas (art. 5º, X, CF), além do sigilo dos dados (artigo 5º, XII, CF). Foi nesse sentido que entendeu o Plenário do Superior Tribunal Federal, em maio de 2020, e assim, suspendeu, por maioria (10x1), a eficácia da Medida Provisória 954/2020. Por certo, isso foi um marco histórico, com relação ao reconhecimento da proteção de dados pessoais, como direito fundamental.[381]

Cumpre esclarecer, ainda, que a LGPD estabelece um dever de adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais contra acesso não autorizado e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. As instituições serão obrigadas a adotar medidas de proteção a partir da criação de qualquer nova tecnologia ou produto (*privacy by design*)[382].

---

[380] TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei geral de proteção de dados pessoais:** comentado artigo por artigo. 2.ed. ver., atual e ampl. Salvador: Editora JusPodivm, 2020, p.41.

[381] PALHARES, Felipe. et al. **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020, p.387.

[382] Desenvolvido na década de 1990 por Ann Cavoukian, ex-comissária de Informação e Privacidade da Província de Ontário, no Canadá, o conceito de *privacy by design* foi determinante para a transformação de como se enxerga a proteção de dados. O conceito antecipa a ideia de que o futuro da proteção de dados depende idealmente de uma mudança organizacional, transformando o modo de operação padrão de entidades que lidam com produtos ou serviços ancorados no tratamento de dados ou que possam impactar a privacidade de seus usuários e de terceiros. Assim, o termo *privacy by design* refere-se à metodologia que visa proteger a privacidade do usuário desde a concepção de quaisquer sistemas de tecnologia da informação ou de práticas de negócio que sejam concernentes ao ser humano. Logo, a proteção de privacidade seria o ponto de partida para o desenvolvimento de qualquer projeto, sendo incorporada à própria arquitetura técnica dos produtos ou serviços.

Neste caso, vazamentos de dados e incidentes de segurança devem ser notificados à autoridade de proteção de dados e, em alguns casos, aos titulares afetados.[383] Além disso, o *compliance*, as boas práticas de governança, o gerenciamento de riscos, o plano emergencial para incidente de vazamento de dados e de forma especial o mapeamento de dados, são indispensáveis para a garantia da segurança e a proteção das informações, e são algumas das mais variadas técnicas de adequação à LGPD.[384]

Observa-se, assim, que o legislador fala em medidas de segurança desde a concepção do produto ou do serviço, os chamados *privacy by design* (privacidade desde a concepção, ou seja, melhores práticas de privacidade desde a concepção) e o *privacy by default* (privacidade por padrão), os quais já existem a muito tempo, mas que são trazidas pela lei para direcionar o agente de tratamento quando for criar um produto ou oferecer o serviço. Ambos são indispensáveis aos sistemas de tratamento de dados, já que os mesmos deverão ser estruturados visando proporcionar a segurança adequada desde a sua estruturação, chamada de *security by design* (segurança desde o planejamento do projeto).[385]

Assim, muitas instituições já adotaram tecnologias de segurança para as informações coletadas de seus usuários, sendo que com a vigência da LGPD deverão providenciar que essa segurança seja capaz de proteger os dados pessoais de qualquer pessoa, mesmo após o término de seu tratamento. Agora, caso ocorra algum incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiro não autorizado acessá-los.

É curioso notar, ainda, que 55% dos brasileiros disseram estar extremamente ou muito confiantes de que a lei trará avanços requeridos para proteger seus dados mantidos por organizações públicas e privadas, conforme levantamento conduzido pela Unisys Security Index (USI) 2020, que acompanha as preocupações com a segurança do consumidor.

---

[383] PALHARES, Felipe. et al. **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020, p.138.
[384] TEIXEIRA, Tarcísio. **Empresas e a implementação da Lei Geral de Proteção de Dados.** 1.ed. Salvador: Editora JusPodivm, 2021, p.53.
[385] TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei geral de proteção de dados pessoais:** comentado artigo por artigo. 2.ed. ver., atual e ampl. Salvador: Editora JusPodivm, 2020, p.134-139.

Cabe destacar, também, que a LGPD não detém a exclusividade no tratamento do tema da proteção de dados pessoais, sendo o mesmo igualmente inserido em outros diplomas legais. O que singulariza a regulação presente na lei é a sua abrangência, com a anuência de princípios, direitos, responsabilidades e demais aplicações decorrentes do tratamento de dados pessoais. Fora a LGPD, a proteção de dados encontra guarida constitucional e está também inserida no Código de Defesa do Consumidor (Lei 8.078/1990), no Código Civil (Lei 10.406/2002), na Lei de Acesso à Informação (Lei 12.527/2011) e no Marco Civil da Internet (Lei nº 12.965/2014),[386] para serem aplicadas em conjunto com a LGPD:

> 1. A Constituição contém uma cláusula geral de privacidade (art. 5º, X e XII), que tutela a vida privada, a honra, a imagem e a inviolabilidade de dados das pessoas naturais, além de assegurar o direito à indenização pelos danos materiais e à compensação pelos danos morais decorrentes da violação desses direitos. Da mesma forma, estão entre os fundamentos da Lei Geral de Proteção de Dados a inviolabilidade da intimidade, da honra e da imagem (art. 2º, IV, da LGPD) e os direitos do titular têm sua base principal nos direitos fundamentais de liberdade, de intimidade e de privacidade (arts. 1º e 17 da LGPD);
> 2. O Código de Defesa do Consumidor exige a informação adequada e clara sobre os serviços (art. 6º, III), tendo em vista que a informação é relevante para conduzir a tomada de decisões, razão pela qual o seu controle e as regras de acesso têm relevância jurídica. Desse modo, na prestação de serviços de tratamento de dados pessoais, o consumidor deve ser devidamente informado sobre tudo o que será feito com os seus dados, o que compreende a autorização, o conhecimento, a retificação, a boa-fé, a interrupção e a exclusão. Ainda no CDC, existem regras sobre a redação dos documentos de oferta e apresentação dos produtos e serviços em língua portuguesa, com informações corretas, claras, precisas e ostensivas, elaboração de contratos em termos claros e com caracteres ostensivos e legíveis, com tamanho mínimo de fonte em corpo 12 (arts. 31, *caput*, e 54, § 3º, do CDC). Nos contratos de adesão, nas ofertas em massa de produtos e serviços e, especialmente, na *internet*, como não se sabe previamente se o contratado será – ou não – enquadrado como consumidor, os fornecedores de produtos e serviços que envolvem a captação e o tratamento de dados deverão observar as normas da LGPD e do CDC, para evitar o descumprimento das normas adequadas a cada caso (como, por exemplo, a Política de Privacidade dos sites na internet). Além disso, quando for solicitado, o controlador deve fornecer, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, desde que igualmente respeitados os segredos comercial e industrial (art. 20, § 1º, da LGPD);
> 3. O Código Civil também protege o direito da personalidade nos seus arts. 11/21 do Código Civil, o que tem como fundamentos a intransmissibilidade e a irrenunciabilidade pelos titulares, logo, a menos que exista autorização expressa em lei, os titulares não podem, de modo voluntário, renunciar ou transferir os seus direitos de personalidade (que são aqueles relacionados a aspectos constitutivos da identidade, como o nome, o corpo, a imagem, entre outros). De forma específica, o art. 12 do

[386] FRAZÃO, Ana; TEPENDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** 2.ed. São Paulo: Thomson Reuters Brasil, 2020, p.416.

> Código Civil protege o titular dos dados pessoais contra atividades de tratamento que violem qualquer direito de personalidade, ao conferir a ele os direitos de "(...) exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei". A LGPD tem entre seus objetivos e fundamentos o livre desenvolvimento da personalidade da pessoa natural (arts. 1º e 2º, VII) e protege a personalidade no direito de revisão das decisões automatizadas (art. 20).
> 4. A Lei de Acesso à Informação regula o acesso restrito aos dados pessoais (art. 31, § 1º, I). Assim, os dados e informações pessoais relativos à intimidade, à vida privada, à honra e à imagem dos seus titulares devem ser classificados como de acesso restrito (independentemente de classificação de sigilo), permitido apenas aos próprios titulares e a agentes públicos legalmente autorizados, pelo prazo máximo de 100 anos a partir de sua produção. O acesso à informação pública é a regra na LAI, que, ao mesmo tempo, protege dados e informações pessoais armazenados em bancos de dados de entes públicos;
> 5. O Marco Civil da Internet, que tem como principais fundamentos a neutralidade de rede, a privacidade online e a fiscalização dos acessos, também possui uma ampla regulação protetiva dos dados pessoais que circulam na rede. Entre elas, destaca-se a proibição do compartilhamento dos dados pessoais (art. 7º, VII). Como regra, o compartilhamento dos dados pessoais é proibido, ou seja, os provedores de internet não podem fornecer tais dados a terceiros (inclusive registros de conexão e de acesso a aplicações de internet), exceto nas situações previstas em lei ou quando houver o consentimento expresso, livre e informado do titular (e, como visto, de forma destacada em uma cláusula específica). Essa proteção dos dados e proibição de compartilhamento leva em consideração um dos principais fundamentos do Marco Civil da Internet, que é a privacidade online. Além dos direitos constitucionais da inviolabilidade da intimidade e da vida privada (art. 5º, X, da Constituição), da inviolabilidade das comunicações (art. 5º, XII, da Constituição) e da inviolabilidade da vida privada (art. 5º, XI e XXI, da Constituição), protegem a privacidade no meio virtual os arts. 7º, 10 e 11 do Marco Civil da Internet. Por isso, em regra, as comunicações realizadas pela internet e os dados pessoais armazenados só podem ser compartilhadas com terceiros mediante o consentimento dos titulares ou por meio de decisão judicial (art. 10, § 2º, do MCI). Excepcionalmente, podem ser fornecidos determinados dados pessoais cadastrais listados de modo exaustivo pela lei (qualificação pessoal, filiação e endereço), para autoridades administrativas no desempenho de suas atribuições legais (por exemplo, para Delegado de Polícia com o objetivo de instruir inquérito policial). Por sua vez, a Lei Geral de Proteção de Dados tem entre os seus fundamentos a inviolabilidade da intimidade, da honra e da imagem (art. 2º, IV, da LGPD) e os direitos do titular têm sua base principal nos direitos fundamentais de liberdade, de intimidade e de privacidade (arts. 1º e 17 da LGPD).[387]

No que tange ao setor financeiro, às regras de tratamento de dados pessoais, tem como principais marcos regulatórios: Lei de Sigilo Bancário (Lei Complementar nº 105/2001); Resolução 2.025/1993 (contas de depósitos); Circular 3.461/2009 (combate à lavagem de dinheiro); Resolução 4.539/2016 (relacionamento com

[387]CARDOSO, Oscar Valente. Lei Geral de Proteção de Dados e o diálogo das fontes- 10) Síntese Geral. **Revista Jus Navigandi**, Teresina, ano 25, set. 2020. Disponível em: < https://jus.com.br/artigos/85659/lei-geral-de-protecao-de-dados-e-dialogo-das-fontes-10-sintese-geral >. Acesso em: 15 out. 2020.

clientes e usuários de produtos e serviços financeiros); Resolução 4.557/2017 (gerenciamento contínuo de riscos); Resolução 4.658/2018 (segurança cibernética e *cloud computing*), e a Circular nº 3.909/2018 (trouxe a obrigação de implementação de uma política de segurança cibernética por parte das instituições de pagamento).

Por fim, ainda, temos a Lei do Cadastro Positivo (Lei Complementar nº 166/2019) que passou a permitir a inclusão automática de indivíduos na base de dados do cadastro positivo, ampliando a relevância dessa base de dados para o Sistema Financeiro Nacional e o *Open Banking* (Circular nº 4.015 de 04/05/2020 do BACEN, em conjunto com CMN, Resolução Conjunta nº 1/2020), que tem como fundamento central a facilitação do compartilhamento e acesso aos dados pessoais. Dessa forma, se verifica uma evolução bastante significativa nas normas que visam regulamentar o uso e proteger informações e dados pessoais contra divulgação não autorizada, de usuários de serviços financeiros, no Brasil.[388]

Pois bem, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018 ou "LGPD") entrou em vigor no dia 18 de setembro de 2020, após longas e tortuosas articulações entre o Congresso Nacional e o Governo, com o envolvimento de diversos atores e setores da sociedade civil. No entanto, suas sanções (multas e penalidades por descumprimento) somente serão aplicadas a partir de agosto de 2021.

Dessa forma, com a aprovação e a entrada em vigor da LGPD, o tratamento de dados pessoais passa a receber uma abordagem mais detalhada pela legislação, ofertando a Lei mecanismos que ressaltam a relevância da segurança e do sigilo dos dados pessoais coletados, armazenados e utilizados especialmente por empresas do setor financeiro. Ainda, a LGPD designa limites mais rígidos ao tratamento de dados, exigindo, por exemplo, a adoção de seguranças técnicas e administrativas para protege-los de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito.[389]

---

[388] PALHARES, Felipe. et al. **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020, p.129.
[389] FRAZÃO, Ana; TEPENDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** 2.ed. São Paulo: Thomson Reuters Brasil, 2020, p.419.

Sendo assim, para compreender de forma simples e objetiva a Lei Geral de proteção de Dados é importante entender que com a entrada em vigor da Lei organizações públicas e privadas de todos os setores estão sujeitos à LGPD, e isso inclui instituições financeiras, instituições de pagamento, corretoras, *fintechs* e demais organizações do setor financeiro. A LGPD regulamenta não só a coleta e tratamento de dados nas relações dessas organizações com clientes e parceiros de negócio, como também, no âmbito de suas relações com os empregados. Assim, novos desafios terão que ser enfrentados para cumprir com os requisitos previstos na lei, na concepção e na oferta de produtos e serviços ao consumidor, incluindo, por exemplo, a análise e concessão de crédito.[390]

Ainda, assim, por ser uma regulamentação complexa, que interfere em práticas, processos e comportamentos, a adequação à LGPD exige um planejamento direcionado e orientado por profissionais que entendem como funcionam as questões técnicas e jurídicas envolvidas. É uma verdadeira jornada de modificações em prol de proteção e privacidade no tratamento dos dados pessoais, em ações que interferem em diversas áreas das instituições, desde a gestão até a rotina dos colaboradores. É importante que se tenha como base quatro pilares: transparência, controle, consentimento e segurança. Além disso, um ponto importante para o setor financeiro é a questão de tratamento de dados relacionado à criação de *score* de crédito, principalmente se as bases não foram construídas atendendo à LGPD. Por isso, se faz necessário atualizar a redação da ficha cadastral da oferta do crédito (aviso prévio sobre tratamento), bem como inserir aviso na própria CCB (Cédula de Crédito Bancário)[391], chamados de "*privacy notices*". Portanto, deve-se seguir um plano de ação emergencial para adequação, conforme se verá a seguir:

> 1. Publicar a Política de Privacidade e Proteção de Dados atualizada nos canais digitais;
> 2. Indicar (nomear) o Encarregado (DPO) e divulgar publicamente o contato (art. 41, parágrafo 1º.);

---

[390] PALHARES, Felipe. et al. **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020, p.133.

[391] Título de crédito emitido de forma escrita por pessoa física ou jurídica, em favor de uma instituição financeira. Foi criada através da MP 1.925/99 e incluída na Lei nº 10.931/04. Representa uma promessa de pagamento, em dinheiro, que é decorrente de uma operação de crédito. Assim, toda vez que alguém contrata um empréstimo (independente da modalidade) com uma instituição financeira deve assinar a CCB, declarando ciência do crédito e do pagamento. O documento tem, portanto, a mesma validade de um contrato.

3. Ajustar clausulado de contratos (controlador – operador) com os terceirizados que tratam dados pessoais. Como toda nova lei, há necessidade de revisão de procedimentos e atualização documental considerando desde políticas até cláusulas contratuais. Isso passa pelo mapeamento e fluxo dos dados pessoais – por onde entram (formas de captura), onde ficam armazenados, quais os controles aplicados, se há compartilhamento com terceiros (inclusive dentro do próprio grupo), se há internacionalização (como pode ocorrer no uso de serviços de *cloud*) até como é feita a sua eliminação (que deverá atender a padrões de descarte segura;
4. Atualizar a Política do RH (para cumprir princípio de transparência e ciência e informar sobre compartilhamento, especialmente entrada de dados no banco de talentos e política de benefícios, atenção especial com tratamento de dados de dependentes e menores de idade);
5. Fazer o aviso de privacidade principalmente nos ambientes de grande tratamento de dados pessoais como crédito e cobrança, cuidado com base de dados de *telemarketing* e *marketing* digital e nos ambientes de entrada de pessoas como para visitantes (entrada, recepção). Visto que os dados pessoais devem ser tratados para as finalidades expressamente e explicitamente informadas. Logo, a abordagem comercial precisa estar bem alinhada, com verificação inclusive da legitimidade da origem da base de dados, para evitar uma denúncia no tocante ao uso indevido ou ilícito, que é um dos tipos de violações previstos;
6. Iniciar gestão de consentimentos;
7. Realizar campanha educativa LGPD;
8. Verificar se é caso de protocolar Código Melhores Práticas (por meio da associação do seu setor conforme arts. 50 e 51), junto à Autoridade Nacional de Proteção de Dados (ANPD);
9. Identificação do inventário de dados pessoais e a elaboração da matriz de tratamento de dados associando as categorias, com as finalidades e com as bases legais que justificam o tratamento desses dados.[392]

Nessa linha, é possível listar, ainda, cinco procedimentos indispensáveis:

1. Revisar a estratégia de enriquecimento de bases de dados e geração de *leads* com origem de fontes de terceiros e fontes públicas para adequar para LGPD e evitar riscos de origem (legitimidade) e destino (compatibilização da finalidade de uso);
2. Instituir medidas de cibersegurança com programas de capacitação e conscientização em segurança da informação com avaliação periódica de pessoal, além do comprometimento da alta administração para a melhoria contínua dos procedimentos de segurança cibernética, e especialmente de resposta a incidentes para atender ao dever de *report* do art. 48, LGPD;
3. Implementar solução para atender requisições de titulares no exercício do direito ao apagamento de dados e de portabilidade do art. 18, LGPD;
4. Adequar a estratégia de dados pessoais para proteção de segredo de negócios.
5. Elaborar o relatório de impacto de privacidade para tratamento de dados pessoais sensíveis devido ao uso de biometria e reconhecimento facial na autenticação e combate à fraude (com base no artigo 11, letra g).[393]

---

[392] Revista CIAB - FEBRABAN. 2020. **LGPD em vigor: como a nova lei afeta as instituições financeiras.** Disponível em: < https://noomis.febraban.org.br/especialista/patricia-peck-pinheiro/lgpd-em-vigor-como-a-nova-lei-afeta-as-instituicoes-financeiras?pesquisa=nova-lei-do-cadastro-positivo>. Acesso em: 19 out. 2020.

[393]Revista CIAB - FEBRABAN. 2020. **Como as financeiras devem se preparar para 2020: o ano da LGPD.** Disponível em: < https://noomis.febraban.org.br/especialista/patricia-peck-pinheiro/como-as-

A seguir, alguns conceitos legais que nortearão a interpretação e aplicação da LGPD. Entre os conceitos trazidos no texto legal, no artigo 5º da lei, destaque deve ser dado às definições de dado pessoal, de dado pessoal sensível, dado anonimizado, banco de dados, tratamento e consentimento. Mas a LGPD não se restringe a apenas esses conceitos, trazendo outros. Sendo eles:

I. **Dado pessoal:** Informação relacionada a pessoa natural identificada ou identificável. Isso abre um leque de possibilidades para a tutela da lei. Tem-se a falsa impressão de que apenas dados pessoais diretos, como nome e documentos pessoais poderiam identificar uma pessoa. Entretanto, alguns outros dados são capazes de identificar uma pessoa a depender das circunstâncias, são os chamados dados pessoais indiretos, como, por exemplo, a geolocalização, que a principio não é um dado pessoal, mas que em determinado momento pode levar à identificação de um único individuo tornando-se nesse caso um dado pessoal.

II. **Dado pessoal sensível:** Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. São assim denominados por terem um tratamento diferenciado na lei, com uma tutela mais rígida, já que envolvem informações de foro mais íntimo.

III. **Dado anonimizado:** Dado relativo à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Frise-se que dados anônimos não são dados pessoais e, portanto, não são tutelados pela lei. São aqueles que a sua reidentificação é impossível por qualquer parte e por quaisquer meios razoavelmente possíveis. De outra sorte, esses dados são aqueles que através de técnicas, como a criptografia, não possam ser levados a identificar uma pessoa. Insta frisar que se o dado, mesmo criptografado, por exemplo, for identificado através de meios razoáveis e disponíveis à época do tratamento, possibilitando-se a sua reidentificação, ele estará sobre a tutela da lei, é o que se chama de pseudonimização do dado.

IV. **Banco de dados:** Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico. Com a vigência da lei, muitos bancos de dados terão que ser revistos, pois grande parte deles concentra uma quantidade infindável de dados pessoais, e que, segundo a lei, assim que atinjam sua finalidade deverão ser eliminados, o que na prática poderá ser bem complexo. É de se prever que quanto maior o banco de dados e mais completa a sua gama de informações, maior impacto terá caso algum incidente venha a ocorrer.

V. **Titular:** Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Também merece destaque, que não há previsão legal para as pessoas já falecidas, na medida em que se tutela a proteção de dados pessoais de pessoa viva.

VI. **Controlador:** Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

VII. **Operador:** Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
Observação: tanto o controlador, como o operador são espécies do gênero agente de tratamento e apareceram na lei da mesma forma que o previsto na GDPR, que lá receberam a nomenclatura de *controller* (controlador) e

---

financeiras-devem-se-preparar-para-2020-o-ano-da-lgpd?pesquisa=nova-lei-do-cadastro-positivo>. Acesso em: 19 out. 2020.

processor (operador). A importância da distinção dessas duas figuras se dá principalmente quando se fala no tratamento de dados por empresas, já que muitas vezes uma empresa contrata “dando as ordens”, enquanto a outra executa essas ordens. A lei se aplica a ambas as figuras, tanto ao controlador quanto ao operador, o que acarreta em responsabilidades para ambos. Podemos citar como exemplo de operador aquele que apenas armazena os dados a pedido do controlador, os chamados *cloud servisse provider* (em português, fornecedor de serviços em nuvem), em que seus serviços poderão estar localizados em diferentes países. Essa distinção também se torna importante quando o controlador é um ente público e o operador um ente privado, o que poderá acarretar em diferentes tipos de responsabilização de cada ente, de acordo com sua conduta.

VIII. **Encarregado (DPO):** Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

IX. **Agentes de tratamento:** O controlador e o operador.

X. **Tratamento:** Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Em suma, resume toda e qualquer operação com dados pessoais, não se limitando aos exemplos pontuados pela lei, qualquer atividade que for realizada com dados pessoais será alcançada pelas determinações legais.

XI. **Anonimização:** Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. A anonimização deve levar em conta as técnicas razoáveis e disponíveis adotadas no momento do tratamento, ou seja, por mais que surjam técnicas melhores posteriormente, será considerada aquela à época do tratamento, posto que a tecnologia avança exponencialmente com o tempo, não sendo possível prever o que será razoável futuramente.

XII. **Consentimento:** Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. O consentimento do titular de dados é a forma mais conhecida do tratamento legal de dados e deve ser livre e o mais consciente possível, ou seja, o titular deve ter pleno conhecimento de quais dados estão sendo captados e exatamente para qual fim ele será utilizado, o qual perfaz a inequivocabilidade do consentimento. O consentimento é trazido por muitos como a hipótese principal para o tratamento de dados. Vale pontuar que o consentimento do titular para tratamento de seus dados pessoais sensíveis além de ser livre, inequívoco e informado, também deverá ser especifico e de forma destacada, diferindo-se do consentimento de dados pessoais que não são sensíveis.

XIII. **Bloqueio:** Suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

XIV. **Eliminação:** Exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

XV. **Transferência internacional de dados:** Transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

XVI. **Uso compartilhado de dados:** Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados. Assim, o uso compartilhado de dados é inerente à sociedade informacional, na medida em que ele sustenta grande parte das

atividades de uma empresa e também dos órgãos públicos, sendo essencial para o funcionamento das mesmas, sendo que o conceito abrange a comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado. O compartilhamento poderá se dar entre o ente público e privado ou entre entes públicos e privados entre si.

XVII. **Relatório de impacto à proteção de dados pessoais:** Documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. Logo, é uma obrigação que todo o controlador deverá cumprir. Esse relatório é a prestação de contas. Não basta o controlador cumprir a lei, ele deverá gerar a todo tempo evidências de que está cumprindo a lei. Neste relatório o controlador deverá demonstrar todo o tratamento da dados feitos, bem como os riscos a ele inerentes e medidas, salvaguardas e mitigações de risco.

XVIII. **Órgão de pesquisa**: Órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico. Vale destacar que os órgãos de pesquisa definidos nesse artigo são aqueles que não possuem fins lucrativos e possuem sede ou foro no Brasil. Essa conceituação restringe quais órgãos poderão tratar dados utilizando-se da base legal prevista no inciso IV do artigo 7º da lei.

XIX. **Autoridade nacional:** Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. Isso, demonstra o tamanho de sua importância, somado ao fato de que grande parte do previsto em lei depende dessa autoridade para sua efetividade. Os vetos dos artigos que criavam a Autoridade Nacional de Proteção de Dados (ANPD) se baseou na inconstitucionalidade do processo legislativo, por afronta ao artigo 61, §1º, II, 'e', cumulado com o artigo 37, XIX, da Constituição. Posteriormente, a Lei nº 13.853/2019, aprovada pelo Congresso nacional em 30 de maio de 2019 criou a Autoridade Nacional de Proteção de Dados, de natureza jurídica transitória. Muito se tem questionado sobre a efetiva independência da autoridade, já que ela será indispensável para eficácia da lei, sendo esse um dos motivos pelo qual a Lei 13.853/2019 colou a Autoridade vinculada transitoriamente ao Poder Executivo pelo prazo de 2 anos. Isso pois, se a ANPD estiver permanentemente subordinada ao Poder Executivo Federal implicaria em diferença – substancial – quanto aos modelos internacionais. Sustenta-se que autoridade nacional, mais do que fiscalizar, terá um papel significativo na unificação e concentração de todos os atos relacionados á proteção de dados; até porque no ordenamento jurídico brasileiro existem outras normas de proteção de dados que necessitarão se harmonizarem com a presente lei nº 13.709/2018.[394]

A importância na definição desses conceitos no texto legal está no fato de que servirá de guia para a correta interpretação e aplicação da lei, bem como da fiscalização com relação ao seu fiel cumprimento.

Isto posto, é importante mencionar que, no conceito de dado pessoal, inclui até aquelas informações que não se prestam a identificar a pessoa quando usadas

[394] TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei geral de proteção de dados pessoais:** comentado artigo por artigo. 2.ed. ver., atual e ampl. Salvador: Editora JusPodivm, 2020, p.42-75.

isoladamente (IP, faixa etária, altura, etc.), mas que poderão fazê-lo se conjugadas com outros dados, são, portanto, identificáveis.[395] Além disso, todo o dado pessoal é privativo. Assim, para que se torne público seria necessário que o dado fosse publicamente tratado. E, para que o Poder Público trate um dado, é preciso que o interesse esteja previsto em leis e/ou na Constituição federal, ante a presunção de legalidade dos atos do Poder Público.[396]

Fazendo um paralelo, com a "GDPR" (Regulamentação Geral de proteção de Dados da União Europeia)[397], que revogou a Diretiva Europeia de Proteção de Dados Pessoais (Diretiva 95/46/CE)[398], entrando em vigor no dia 25 de maio de 2018, é possível perceber que, ela, tem como principal objetivo garantir maior controle dos dados pessoais por parte dos usuários e, ainda, com potencial para repercussão global uma vez que se aplica a qualquer entidade que armazene ou processe informações pessoais de cidadãos europeus, esteja essa entidade situada dentro ou fora da União Europeia.[399]

Além disso, a GDPR foi considerada um termômetro para a regulamentação da privacidade de dados. Mesmo na Europa, os formuladores de políticas estão buscando promulgar medidas adicionais de privacidade do consumidor, incluindo a regulamentação de privacidade eletrônica (uma extensão do GDPR), que se concentra na proteção da privacidade de dados transmitidos eletronicamente. Seu *status* como um regulamento (em vez de uma diretiva) significa que pode ser aplicado uniformemente nos estados membros da UE.

---

[395] FRAZÃO, Ana; TEPENDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** 2.ed. São Paulo: Thomson Reuters Brasil, 2020, p.159.

[396] TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei geral de proteção de dados pessoais:** comentado artigo por artigo. 2.ed. ver., atual e ampl. Salvador: Editora JusPodivm, 2020, p.32.

[397] GDPR é um regulamento do direito europeu que unificou as leis de privacidade de dados em toda a Europa e tem como principal objetivo a proteção de todos os cidadãos europeus da violação de dados e de sua privacidade, estabelecendo regras e sanções, que serviram de base para muitos artigos da lei brasileira. Esse regulamento europeu impôs diversas restrições para transferência internacional de dados entre os países europeus e os demais países.

[398] A diretiva 95/46/CE foi aprovada em 24 de outubro de 1995, mas só entrou em vigor três anos depois. Esta diretiva, além de ter sido promulgada em uma época em que a transformação digital ainda era nascente, necessitava que cada país membro da União Europeia editasse normas internas para que as regras fossem aplicáveis. Ela tinha o caráter instrutório e dependia de harmonização interna dos países. Trazia princípios e direito básicos de proteção aos dados pessoais dos cidadãos.

[399] PALHARES, Felipe. et al. **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020, p.110.

Esse novo regulamento de privacidade eletrônica revogará e substituirá a atual Diretiva de Privacidade Eletrônica da UE de 2002. As novas disposições abrangerão as redes de comunicações eletrônicas; dados armazenados ou enviados de equipamentos do usuário final, como telefones, tablets e computadores (incluindo *cookies*, IDs de dispositivos e outros *softwares* de identificação); e métodos empregados para abordar clientes através de redes de comunicação eletrônica para fins de *marketing* direto.[400]

Igualmente à regulamentação europeia (GDPR), a LGPD trouxe novas limitações à transferência internacional de dados pessoais, que somente é permitida nas hipóteses previstas na lei. Tais hipóteses incluem a transferência para países com grau de proteção adequado ou por meio da utilização de cláusulas contratuais padrão, normas corporativas globais, selos e certificados e códigos de condutas a serem aprovados pela ANPD, entre outras hipóteses. A despeito da limitação imposta pela lei para transferência internacional de dados pessoais, o Conselho Monetário Nacional (CMN) impôs, por meio da Resolução nº 4.658/2018 e da Circular nº 3.909/2018, restrições adicionais à contratação de serviços de processamento de dados baseados em nuvem que sejam prestados no exterior, conforme visto nos capítulos anteriores deste trabalho.[401]

Cabe destacar que em termos quantitativos, o GDPR é um corpo normativo mais consolidado em comparação à LGPD. Enquanto ele é composto por 173 (cento e setenta e três) "considerados" e 99 (noventa e nove) artigos; a LGPD possui 65 (sessenta e cinco) artigos distribuídos em 10 Capítulos e não conta com orientações interpretativas. Fazendo uma interseção entre o direito comunitário europeu e o brasileiro, o GDPR seria um código de proteção de dados que conta com 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. E, em vista disso, percebe-se que tais normas foram

---

[400] MIKKELSEN, Daniel; SOLLER, Henning; STRANDELL-JANSSON, Malin. What will Europe's e-privacy regulation mean for your business? **McKinsey&Company.** Disponível em: < https://www.mckinsey.com/business-functions/risk/our-insights/what-will-europes-eprivacy-regulation-mean-for-your-business>. Acesso em: 19 out. 2020.

[401] PALHARES, Felipe. et al. **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020, p.136-137.

talhadas com técnicas legislativas completamente distintas, logo, eventual nível de equivalência deve ser calibrado por uma análise qualitativa.[402]

É importante mencionar, ainda, que outros países também possuem leis relativas à proteção de dados pessoais, como é o caso, por exemplo, dos EUA. O país, diferentemente do bloco europeu, não possui uma legislação unificada, mas sim instrumentos legislativos relativos a diversos setores que visam precipuamente proteger o titular de dados pessoais, como por exemplo: (i) *Privacy Act* (Lei da privacidade): essa lei americana estabelece interessantemente que, para que as informações atinentes a um indivíduo sejam divulgadas, é necessário haver o seu consentimento por escrito, salvo se essa divulgação estiver inserida em uma das doze exceções que a lei traz; (ii) *Privacy Shield* (Escuso ou Blindagem da privacidade): um termo de comprometimento que o país traçou junto à União Europeia para transferência internacional de dados em um nível adequado de proteção; e a (iii) *California Consumer Privacy Act* (Lei de Privacidade do Consumidor da Califórnia - CCPA), contém disposições semelhantes às da GPDR (como o do consentimento informado, por exemplo) e que passou a vigorar no estado em 2020.[403] Ainda, assim, é importante mencionar que à CCPA, dá aos residentes o direito de saber quais dados são coletados sobre eles e de impedir a venda desses dados. Trata-se de uma medida ampla, aplicada a organizações com fins lucrativos que fazem negócios na Califórnia e atendem a um dos seguintes critérios: ganhar mais da metade de suas receitas anuais com a venda de informações pessoais de consumidores; obtendo receitas brutas de mais de $50 milhões; ou manter informações pessoais sobre mais de 100.000 consumidores, residências ou dispositivos.

Como se vê, a LGPD tem como objetivo regular os “dados pessoais”. Esse são definidos como qualquer informação relacionada à pessoa natural identificada ou identificável. Ficam fora do escopo dessa lei, portanto, os dados relacionados a pessoas jurídicas. Qualquer informação que possa ser relacionada a um indivíduo, já identificado ou passível de identificação, pode ser considerada como um dado

---

[402] FRAZÃO, Ana; TEPENDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** 2.ed. São Paulo: Thomson Reuters Brasil, 2020, p.799-813.

[403] TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei geral de proteção de dados pessoais:** comentado artigo por artigo. 2.ed. ver., atual e ampl. Salvador: Editora JusPodivm, 2020, p.24-26.

pessoal. Assim, informações de cadastro, perfil comportamental, econômico e/ou social se enquadram no conceito de dado pessoal. Por outro lado, as informações que não permitem a identificação (imediata ou posterior) de um único indivíduo, podem se enquadrar no conceito de “dado anonimizado”. Como mencionado anteriormente, trata-se, por exemplo, de informação sobre dados estatísticos e cujo processo de anonimização seja irreversível revelam apenas uma informação de caráter coletivo e, por isso, não estão sujeitos ao regime de proteção de dados da LGPD, sendo seu uso livre. De qualquer modo, deve-se buscar um equilíbrio entre o direito à privacidade e o desenvolvimento de produtos e serviços, que ganha enorme propulsão com a digitalização dos serviços bancários, alinhado com a crescente capacidade de processamento de dados pelas *fintechs,* instituições financeiras e outros *players* do mercado financeiro.[404]

Nota-se, portanto, que essa lei, não foi criada para limitar a atuação das empresas gestoras de dados e sim para promover a inovação, bem como a expansão segura dessas atividades, tendo por missão a proteção e promoção dos direitos fundamentais, essenciais para efetiva tutela dos dados privados de seus cidadãos, de suas instituições e corporações privadas. Desta forma, o Brasil passa a integrar o grupo de mais de 120 países que têm uma legislação de proteção de dados semelhante ao modelo europeu (GDPR).

Na sequência, para melhor explicar e visualizar a Lei geral de Proteção de Dados, faz-se necessário apresentar a (figura 7) abaixo, com os principais pontos da lei e as principais transformações que ela traz para o país:

[404] PALHARES, Felipe. et al. **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020, p.134-150.

Figura 7 – Principais transformações trazidas pela LGPD no Brasil

Fonte: SERPRO[405]

Entendido algumas noções básicas da Lei Geral de proteção de Dados (LGPD) passamos agora a analisar, de maneira clara e objetiva, os elementos que compõem a Lei. Dessa forma, busca-se compreender os princípios que a regem, os direitos aos titulares de dados, as bases legais de tratamento desses dados, bem como as sanções e multas propostas. E, ainda, identificar quem é o DPO e qual o seu papel? a Autoridade Nacional de Proteção de Dados (ANPD), e também esclarecer alguns pontos referentes ao *Open Banking* (Sistema Financeiro Aberto) e a "nova" Lei do Cadastro Positivo. É o que se verá, resumidamente, a seguir.

4.3.1.1 Princípios

Os princípios, também conhecidos como *Fair Information Privacy Principles* – FIPPs que, da perspectiva da OCDE e, como consequência, de várias legislações voltadas à proteção de dados pessoais, se propõe a preservar o adequado

[405] SERPRO. **O que muda com a LGPD.** Disponível em: < https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd>. Acesso em: 13 set. 2020.

tratamento de dados pessoais. Por isso, compreender os FIPPs, equivale a compreender os fundamentos de um regime geral de proteção de dados pessoais.[406]

Assim, diferentemente do que acontecia há décadas, as transformações vêm ocorrendo em uma velocidade frenética. O trâmite legislativo, por mais célere que possa vir a ser, não consegue acompanhar os desdobramentos de uma determinada matéria, principalmente quando a mesma envolve tecnologia, como a de proteção de dados, tronando uma lei, desde a sua promulgação, incapaz de prever todos os potenciais conflitos e anseios de uma sociedade. Diante de tal constatação, faz-se indispensável a aplicação de princípios, que norteiam a aplicação da lei, pois os mesmos serão capazes de atingir eventos futuros, como novas tecnologias e distintas realidades.

Os princípios estabelecidos pela LGPD, estão elencados em seu artigo 6[407], trazendo novas diretrizes e limitações sobre como os dados pessoais poderão ser tratados. De forma não exaustiva e bastante resumida, tais princípios estabelecem um dever de transparência sobre como os dados pessoais são tratados dentro das respectivas organizações, estabelecendo ainda que dados desnecessários não devem ser coletados, deve haver uma limitação de finalidade para qual os dados

---

[406] CARVALHO, André Castro; ALVIM, Tiago Cripa et al. **Manual de *Compliance.*** Rio de janeiro: Forense, 2019, p.504-505. ISBN 978-85-309-8315-4.

[407] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.
II -Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III -Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
IV - Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
V - Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
VI - Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
VII - Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
VIII - Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
X - Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

são utilizados, os dados devem ser mantidos em segurança, e a organização que trata dos dados pessoais deve demonstrar o cumprimento dos requisitos previstos na LGPD. Além de adequação aos princípios da LGPD, para que o tratamento de dados seja lícito, a instituição deverá fundamentar o tratamento em uma das 10 (bases) legais previstas na LGPD. Entre outras hipóteses, o tratamento de dados pessoais é autorizado com o consentimento do titular dos dados pessoais, para fins de cumprimento de obrigação legal ou regulatória, quando necessário para execução de contrato, para atender interesses legítimos do controlador dos dados ou terceiros e para fins de proteção ao crédito.

Além disso, os princípios da segurança, da prevenção e da responsabilidade, ou prestação de contas, também são bastante próximos. Isso porque o primeiro visa evitar situações ilícitas, ao passo que o segundo pretende evitar o dano à pessoa por causa do tratamento inadequado dos dados pessoais. Não obstante, o ilícito e o dano são conceitos clássicos da responsabilidade civil. Com efeito, não é espantoso que a concretização desses princípios na lei ocorra, muitas vezes, por um mesmo dispositivo.[408]

Portanto, conclui-se que os princípios da LGPD são, em verdade, princípios do sistema brasileiro de proteção de dados e que a nova lei não supera às anteriores. Ao contrário, ela muito se inspira e, portanto, se integra às predecessoras, de proteção de dados no Brasil. Por sua vez, a violação desses princípios, notadamente o da finalidade, há de ser aferida com referência ao valor da privacidade, a qual, a seu turno, encontra-se naturalmente funcionalizada à dignidade da pessoa humana.

4.3.1.2 Bases legais de tratamento

Antes de seguir, porém, faz-se necessário esclarecer, que não se pretende, aqui, abordar as dez bases legais de tratamento, seja porque isso demandaria muito tempo. Dessa forma, busca-se compreender de forma sucinta e rápida as bases legais de maior destaque da lei.

---

[408] FRAZÃO, Ana; TEPENDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** 2.ed. São Paulo: Thomson Reuters Brasil, 2020, p.76.

De início, cabe mencionar que a Lei geral de Proteção de Dados apresenta, em seu artigo 7[409], um rol com dez hipóteses para o tratamento de dados pessoais. Todavia, esse trabalho não apresenta base legal segura e apta a embasar o tratamento de dados pessoais e dados pessoais sensíveis existentes em processos judiciais, sejam eles físicos ou digitais, pelo Poder Judiciário, de modo que a sua taxatividade deve ser flexibilizada para que se encontre, dentro da própria lei, alicerce legal, como aquele identificado no caput do art. 23[410]. Dessa forma, o caput

---

[409] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
I - Mediante o fornecimento de consentimento pelo titular;
II - Para o cumprimento de obrigação legal ou regulatória pelo controlador;
III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
IV - Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
V - Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
VI - Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
VII - Para a proteção da vida ou da incolumidade física do titular ou de terceiros;
VIII - Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
IX - Quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
X - Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.
§ 1º (Revogado).
§ 2º (Revogado).
§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.
§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.
§ 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.
§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.
§ 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei.

[410] Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do

do artigo 23 da LGPD deve ser considerado uma base legal autônoma àquelas descritas no artigo 7º da LGPD, e apta a embasar o tratamento de dados pessoais e dados sensíveis contidos nos processos judiciais.[411]

Ainda, assim, o tratamento de dados corresponde a "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (art. 5º, inciso X). Além disso, o modelo de tratamento de dados instituídos pela LGPD se ampara nas seguintes características básicas: a ampliação do conceito de dado pessoal; o respeito à base legal; e o legitimo interesse como hipótese autorizativa e a necessidade de realização de um teste de balanceamento de interesses. E, segundo a LGPD, todo e qualquer tratamento de dados deve respeitar a base legal definida no art. 7º.

Atenção: a realização do tratamento de dados deve ocorrer para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; de forma compatível ou adequada com as finalidades informadas ao titular, de acordo com o contexto do tratamento; e ainda no limite do mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados. Utiliza-se do princípio da proporcionalidade, ou seja, o tratamento dos dados é protegido na medida em que o meio é adequado e necessário para o fim almejado.[412]

Ademais, o consentimento[413] é trazido por muitos como a hipótese principal para tratamento de dados, entretanto não há qualquer grau de hierarquia entre as dez hipóteses legais estabelecidas pela LGPD. Pode-se afirmar que o consentimento do titular mesmo diante de novas possibilidades legais de tratamento,

---

interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

411 PALHARES, Felipe. et al. **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020, p.317.

412 FRAZÃO, Ana; TEPENDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** 2.ed. São Paulo: Thomson Reuters Brasil, 2020, p.220.

413 Para os fins da LGPD, considera-se consentimento a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (LGPD, art. 5º, inciso XII). Significa dizer que o consentimento desvinculado da finalidade ou tempo para o qual foi dado não é consentimento e, portanto, não merece proteção.

continua a ter certa preferência sobre os demais, pois geralmente facilita a obrigação do agente de tratamento em demonstrar que o tratamento foi feito dentro de uma hipótese legal, ante o princípio da *accountability*[414] (prestação de contas ou responsabilidade demonstrável). Insta, ainda, ressaltar que o consentimento autoriza tão somente o agente que o obteve, não se estendendo a outras pessoas para quem possa compartilhar os dados, devendo, para esse caso, obter o consentimento especifico do titular.

É importante destacar que, sempre que o consentimento estiver fundado em bases sólidas, isto é, quando estiver baseado em conhecimento efetivo e informado do titular a respeito do processamento dos dados, em especial de seus propósitos, este cumprirá seu papel tradicional. Por outro lado, quando, por conta da complexidade dos fluxos de dados, não for possível assegurar o controle do titular sobre sua privacidade, haverá a expectativa, a partir dos princípios *accountability*, de que o controlador dos dados tomará todas as medidas e disporá de todos os meios que detém para assegurar o processamento ético e justo dos dados pessoais daquele titular. E o faz por meio de duas medidas: (i) libera o titular dos direitos de ônus excessivo e de colocar-se em risco desavisadamente; e (ii) transfere a quem tem interesse e melhores recursos a responsabilidade pelo uso ético e justo dos dados. Tudo isso de forma vigiada.[415]

É nesse contexto que surge o consentimento como instituto jurídico escolhido para que a pessoa não apenas expresse, como também cientifique seu desejo de autorizar o tratamento de seus dados pessoais. Mas isso não basta. Faz parte do processo de consentimento dar, também, a indicação a respeito das circunstancias e para quais finalidades o processamento se dará. Destaque-se que a observância ao princípio da finalidade (*purpose limitation*) é fulcral para efetividade do

---

[414]A exigência de que as empresas e o governo (quando no papel de controlador de dados pessoais) assumam papel central e maiores responsabilidades no processo de tratamento de dados pessoais. Trata-se de mais um meio de legitimação, pelo qual se presume e exige que as instituições que pretendam controlar dados pessoais se responsabilizem, de forma demonstrável (ao regulador), pela utilização e processamento adequados, justos e éticos dos dados pessoais. Logo, não retira do indivíduo o direito de fazer valer seu direito ao controle dos dados que a ele digam respeito. O que o *accountability* propõe é tirar do indivíduo a responsabilidade primária pela proteção de seus dados pessoais e repassá-la à organização que coleta e faz uso dos dados em seu próprio benefício. Pelo conceito de *accountability*, uma organização responsável transparece comprometimento com sua responsabilidade, implementa políticas de privacidade de dados ligadas a critérios externos reconhecidos e estabelece mecanismos de desempenho para garantir tomadas de decisões responsáveis sobre o gerenciamento de dados que estejam de acordo com as politicas da organização.

[415] CARVALHO, André Castro; ALVIM, Tiago Cripa et al. **Manual de *Compliance.*** Rio de janeiro: Forense, 2019, p.512-518. ISBN 978-85-309-8315-4.

consentimento. Como regra geral, cada consentimento deve corresponder a uma finalidade especifica.[416]

Não se deve perder de vista, portanto, que o cumprimento de obrigação legal ou regulatória consiste no controlador poder tratar dados pessoais, mesmo sem o consentimento do titular, quando tiver que cumprir alguma determinação legal ou regulamentação. Pode-se citar, por exemplo, o caso do empregador que necessite informar os dados do seu empregado para fins da seguridade social ou mesmo em casos de fiscalização do Ministério do trabalho. O empregador não precisará de consentimento do seu empregado para tratar os dados pessoais de seus empregados. Nesse caso, porém, quando da contratação de seu funcionário o empregador terá que informá-lo dentro de quais possibilidades seus dados poderão ser tratados, atendendo-se assim o princípio da informação. Por outro lado, o inciso III, do artigo 7º, possibilita que a "Administração Pública trate dados, mas delimita esse tratamento a utilização do mesmo para consecução de políticas públicas previstas em lei ou regulamentos". A realidade é que o Poder Público é um dos grandes agentes de tratamento de dados e isso se deve ao fato de que visa o bem coletivo, demandando-se a coleta de dados pessoais para a consecução de politicas públicas, o que justifica a ausência de consentimento para esse fim.

Além do mais, a hipótese legal esculpida no inciso VII, do artigo 7º, implica na flexibilização do principio da privacidade frente a um principio mais importante que é o da preservação da vida e da incolumidade física do indivíduo. Exemplifica-se, caso um hemofílico sofra um acidente e não tenha esse dado sensível revelado (tratado) poderá perder sua vida. Já a tutela da saúde, prevista no inciso VIII, traz um complemento ao inciso anterior, uma vez que também relativiza o princípio da privacidade e intimidade para a preservação da vida do indivíduo. Em caso de profissionais da saúde, serviços de saúde ou mesmo de entidades sanitárias os dados pessoais poderão ser tratados se forem necessários à preservação da saúde do indivíduo ou mesmo da coletividade. Ainda, o inciso IX traz uma gama de possibilidades para que o controlador trate dados pessoais pelo chamado "legítimo interesse seu ou de terceiros". O legítimo interesse do controlador ou de terceiro

---

[416] CARVALHO, André Castro; ALVIM, Tiago Cripa et al. **Manual de *Compliance.*** Rio de janeiro: Forense, 2019, p.506. ISBN 978-85-309-8315-4.

poderá abarcar múltiplas hipóteses de tratamento de dados, como no caso de ações de *marketing* de uma instituição ou para se evitar uma fraude.

Ainda outra questão pode surgir no enfrentamento do tema, a exemplo do término do tratamento dos dados pessoais, que não se confunde com a tutela do chamado "direito ao esquecimento". Esse concentra-se no tratamento de fatos pretéritos que envolvem o individuo e na possibilidade desses fatos não serem objeto de uma eterna divulgação pública quando não haja qualquer interesse legítimo para tal permanência. A eliminação dos dados pessoais, por manifestação de vontade do titular, independe de qualquer motivação, eis que a revogação do consentimento retira a legitimidade do tratamento dos dados. Além disso, uma vez que o término do tratamento de dados não é seguido da sua eliminação, há de se verificar a repercussão na seara da responsabilidade civil. Observa-se, desde já, a existência de dois posicionamentos, opostos, quanto à natureza da responsabilidade civil, se objetiva ou subjetiva. A leitura sistemática da LGPD parece indicar pistas segundo as quais a responsabilidade seria subjetiva: (1) o próprio histórico de tramitação do projeto de Lei que deu origem à LGPD, que mostra a opção do legislador pela responsabilidade subjetiva; (2) o fato de a LGPD ter todo um capítulo dedicado à "segurança e boas práticas". Trata-se do Capítulo VI; (3) o inciso II do artigo 43, da LGPD.[417] Isso porque, além de outros argumentos, a norma impõe, por meio da previsão de deveres específicos, um padrão de conduta socialmente esperado – o *standard* –, que deve ser seguido pelos agentes de tratamento de dados, sob pena de virem a ser responsabilizados.[418]

Aliás, no que tange a responsabilidade civil, o responsável que, em razão do exercício de atividade de tratamento de dados, causar dano patrimonial, moral, individual ou coletivo, é obrigado a reparar. O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a

---

[417] Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.

[418] FRAZÃO, Ana; TEPENDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** 2.ed. São Paulo: Thomson Reuters Brasil, 2020, p.229-234.

alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.[419]

Observação: o “direito de ser esquecido” aumenta significativamente os riscos do compartilhamento de dados. O consentimento explícito é exigido do titular da conta, por exemplo. No entanto, existe uma contraparte silenciosa para todas as transações financeiras realizadas por esse titular; existe um direito à privacidade para o pagador/beneficiário correspondente? Nesse caso, o processo de consentimento torna-se infinitamente mais complexo – particularmente quanto as partes do banco de transações com instituições diferentes e não há um repositório central de permissões concedidas.[420]

Outra questão, ainda, refere-se à base legal de “proteção ao crédito”, não é certa qual a sua amplitude, isto é, em quais hipóteses a base legal de tratamento para fins de proteção ao crédito poderá ser utilizada, mas esta certamente será de grande valia para as instituições do setor financeiro, especialmente nos casos em que o consentimento não puder ser obtido e outra base legal não puder ser utilizada. Tal amplitude será definida pela Autoridade Nacional de Proteção de Dados (“ANPD”). Sem prejuízo, parece sustentável que a base legal “proteção ao crédito” tenha como escopo permitir a criação de bases de dados com perfis de crédito de consumidores, para fins de auxiliar o processo de concessão de crédito pelas instituições financeiras e demais entidades que de alguma forma concedam crédito no mercado. Além disso, tal base legal também deveria permitir operações de tratamento de dados para fins de realizar a cobrança e negativação de inadimplentes, ainda que em caráter extrajudicial ou anterior à fase litigiosa.

Portanto, a proteção ao crédito também autoriza o tratamento de dados garantindo-se o crescimento da economia como um todo e a preservação da sociedade, precedendo o interesse individual do titular, que está inadimplente ou que é um mau pagador. Essa hipótese engloba ainda o tratamento de dados pessoais para compor o *score* (pontuação) do indivíduo e para preservação antifraude a ser adotada pelo agente de tratamento. Assim sendo, não poderá, por

---

[419] SENADO FEDERAL. **Lei Geral de Proteção de Dados entra em vigor**, publicado em Agência Senado. 2020. Disponível em: https://www12.senado.leg.br/noticias/materias/2020/09/18/lei-geral-de-protecao-de-dados-entra-em-vigor>. Acesso em: 19 out. 2020.

[420] BRODSKY, Laura; OAKES, Liz. Data sharing and open banking. **McKinsey & Company.** Disponível em: < https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking>. Acesso em: 19 out. 2020.

exemplo, o titular solicitar a exclusão de seus dados pessoais dos cadastros de restrição ao crédito ou mesmo se negar a fornecer dados pessoais para pleitear financiamento em uma instituição financeira. É de se lembrar que a proteção ao crédito também é vislumbrada na Lei do Cadastro Positivo (Lei 12.414/2011), que disciplina a formação e consulta a banco de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito, conforme abordaremos mais adiante.

4.3.1.3 Direitos dos titulares de dados (Arts. 17 a 22 da LGPD)[421]

[421] Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.
Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
I - Confirmação da existência de tratamento;
II - Acesso aos dados;
III - Correção de dados incompletos, inexatos ou desatualizados;
IV - Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
V - Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
VI - Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
IX - Revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.
§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.
§ 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.
§ 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.
§ 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:
I - Comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou
II - Indicar as razões de fato ou de direito que impedem a adoção imediata da providência.
§ 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.
§ 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional.
§ 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.
§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor.
Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:
I - Em formato simplificado, imediatamente; ou

Inicialmente, o conceito de titularidade exprime, portanto, não apenas a ideia de poder de controle sobre um bem jurídico, mas, também e consequentemente, o sentido de atribuição do mesmo, com regras claras disponíveis acerca de seus modos de utilização e disposição. Se dados pessoais são hoje um bem jurídico – daí a inequívoca necessidade de tutelá-los –, precisava o legislador determinar a quem pertencem, fosse acerca de seus aspectos extrapatrimoniais –, fosse relativamente a seus aspectos patrimoniais, decorrentes do valor econômico que lhes foi atribuído pela sociedade digital. Resta claro que a intenção do legislador, não foi apenas assegurar o controle dos dados pessoais ao seu titular, o que reflete, de algum modo, a ideia moderna de privacidade, mas tutelá-los por meio de sua efetiva atribuição à pessoa física a quem estão atrelados, criando com isso um vínculo direto e imediato. Logo, a opção legislativa, manifestada no *caput* do art. 17 da LGPD, de tratar a pessoa física a quem os dados se vinculam como seu titular, denota a intenção de refletir que o exercício do direito ali descrito se dará de modo

---

II - Por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.
§ 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.
§ 2º As informações e os dados poderão ser fornecidos, a critério do titular:
I - Por meio eletrônico, seguro e idôneo para esse fim; ou
II - Sob forma impressa.
§ 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.
§ 4º A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos.
Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.
§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.
§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.
§ 3º (Vetado).
Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.
Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

direto e imediato sobre o bem jurídico em questão, inexistindo intervenção de qualquer outra pessoa sobre o vínculo.[422]

Vale esclarecer que a LGPD, embora tenha essa nomenclatura, visa proteger o titular dos dados e não os dados pessoais *per se.* Os dados pessoais, como já mencionado, trazem em si informações significativas sobre o indivíduo, que ao serem utilizados fora de um contexto legal podem acarretar em uma transgressão da liberdade, intimidade e privacidade do seu titular. O que se observa é que o legislador quer deixar claro que a titularidade dos dados é da pessoa natural. Isso pois, mesmo que os dados pessoais de qualquer individuo possam estar espalhados em milhares de bancos de dados pelo mundo, qualquer tratamento deverá obedecer às normas legais, sendo que o seu titular possui direito sobre seus dados inerentes à sua personalidade. Contudo, a ordem prática de todos esses direitos demandará tempo e muito investimento por parte dos controladores, já que engloba não somente o fornecimento dos dados que são tratados, como também quem tratou, a possibilidade de corrigi-los, eliminá-los, bloqueá-los e também a sua portabilidade.[423]

Nesse contexto, as normas de proteção de dados buscam, entre outros objetivos, empoderar os indivíduos que cedem os seus dados pessoais em troca de serviços no mercado digital. Todavia, de nada adianta conceder vários direitos aos indivíduos sem dotá-los de ferramentas efetivas para que esses busquem serviços que respeitem os seus direitos ou que tenham políticas que mais lhe agradem.[424]

Notavelmente, os bancos tradicionalmente consideram a custódia e a proteção dos dados de seus clientes uma responsabilidade, mais uma função de administração do que um ativo a ser comercializado. O compartilhamento de dados em serviços financeiros tende a ser baseado em risco e permissão, com trilhas de auditoria obrigatórias e sujeito a regulamentação e gerenciamento de risco. Se bem feito, no entanto, pode fornecer maior segurança por meio de recursos aprimorados de "saiba seu cliente", validação de identidade e detecção de fraude. Por outro lado, diferentes categorias de dados garantem diferentes níveis de segurança, e o

---

[422] FRAZÃO, Ana; TEPENDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** 2.ed. São Paulo: Thomson Reuters Brasil, 2020, p.145-149.

[423] TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei geral de proteção de dados pessoais:** comentado artigo por artigo. 2.ed. ver., atual e ampl. Salvador: Editora JusPodivm, 2020, p.85-88.

[424] FRAZÃO, Ana; TEPENDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** 2.ed. São Paulo: Thomson Reuters Brasil, 2020, p.343.

consentimento informado requer a compreensão das implicações do compartilhamento antes da aprovação – uma proeza nada pequena quando o clique reflexivo de “Concordo” em um conjunto de termos e condições não lido é padrão.

De acordo com a pesquisa realizada, em abril de 2020, pela *McKinsey & Company*, os consumidores estão se tornando cada vez mais intencionais sobre os tipos de dados que compartilham – e com quem. Eles são muito mais propensos a compartilhar dados pessoais que são uma parte necessária de suas interações com as organizações. Por setor, os consumidores se sentem mais confortáveis em compartilhar dados com provedores de serviços financeiros e de saúde, embora nenhum setor tenha alcançado uma classificação de confiança de 50% para proteção de dados.[425]

Note-se ainda que, além da definição de bases legais, alinhada com os seus princípios, a LGPD impõe às instituições um dever de transparência para com o titular dos dados, independentemente de qual base legal é utilizada para autorizar o tratamento de dados (seja com base no consentimento ou por outra base legal). Assim sendo, as instituições financeiras devem fornecer ao titular dos dados, as suas respectivas políticas de privacidade, com informações claras e completas sobre (i) as categorias de informações coletadas; (ii) como e com que finalidade a coleta de informações é realizada; (iii) identificação da (s) instituição (s) que vai (ão) utilizar, tratar, processar e transferir a informação e qual a responsabilidade dos agentes que realizarão o tratamento; (iv) o que se pode fazer com a informação; (v) por quanto tempo a informação será tratada/armazenada; (vi) como o indivíduo pode entrar em contato com a instituição para pedir correções e exclusões, e também exercer outros direitos a que lhe são atribuídos (como por exemplo, como o consentimento pode ser revogado); e (vii) o nível de proteção assegurado ás informações coletadas.

Além disso, a LGPD traz novos direitos aos titulares de dados, como o direito de obter informações sobre o tratamento de dados, a revisão de decisões automatizadas, realizar o acesso, retificação e eliminação de dados, o direito à revisão de decisões tomadas por meios exclusivamente automatizados é particularmente importante ao setor financeiro, dando origem, por exemplo, a

---

[425] ANANT, Venky; DONCHAK, Lisa; KAPLAN, James; SOLLER, Henning. The consumer-data opportunity and the privacy imperative. **McKinsey&Company.** Disponível em: < https://www.mckinsey.com/business-functions/risk/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative>. Acesso em: 09 set. 2020.

solicitações de revisão de perfis ou do processo de concessão de crédito, realizado de forma automatizada. Também, o direito à portabilidade a outro fornecedor de produtos e serviços. Particularmente com relação a portabilidade, trata-se de direito relevante diante do sistema bancário aberto (*Open Banking*), conforme abordaremos adiante, que tem como um de seus objetivos permitir a portabilidade de informações entre diversos *stakeholders* do mercado financeiro.

Cumpre esclarecer que à portabilidade de dados pessoais, à semelhança do que ocorreu com a telefonia brasileira, poderá facilitar em muito a vida dos cidadãos brasileiros, que poderão portar informações suas coletadas ao longo dos anos de relacionamento com uma instituição para outra qualquer, de sua escolha. As instituições, por outro lado, terão que correr contra o tempo para adequarem tecnologia a fim de possibilitar a portabilidade de seus sistemas para um sistema diverso, sem, contudo, revelar seus segredos. Ainda, será de fundamental importância a atuação da Autoridade Nacional para regulamentar de que forma se dará a portabilidade dos dados pessoais entre as instituições, principalmente no que tange à operacionalidade das operações de forma a preservar os segredos, sem, contudo, impedir que o titular exerça seu direito, até porque não há restrições quanto ao pedido de portabilidade entre instituições de setores diferentes. Além do mais, o titular poderá se dirigir não só à Autoridade Nacional, mas a qualquer órgão de proteção ao consumidor para peticionar em relação aos seus dados contra o controlador. Se for uma relação de consumo, enquanto não se estabelecer a autoridade nacional e suas competências, já, portanto, a previsão de defesa do titular, ora consumidor, para proteção de seus dados pessoais via outras instituições.[426]

Assim, ao permitir que o titular receba de volta os seus dados pessoais fornecidos a um controlador ou que esses sejam transferidos diretamente ao novo serviço desejado, o direito à portabilidade passou a ser considerado como uma nova ferramenta à luz da legislação de proteção de dados. Adiciona-se que o tema da portabilidade de dados não se encerra nos nomes e endereços de e-mail, ganhando novos contornos e extensões, tendo em vista a intensa coleta dos mais variados dados dos indivíduos. Em última análise, preocupações quanto a segurança na

---

[426] TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei geral de proteção de dados pessoais:** comentado artigo por artigo. 2.ed. ver., atual e ampl. Salvador: Editora JusPodivm, 2020, p.88-89.

transmissão dos dados ou quanto à interoperabilidade são inevitáveis. De qualquer forma, já se faz o alerta de qualquer instituto na área de portabilidade de dados deve ser implementado ao lado de políticas de segurança.[427]

Cabe destacar, ainda, que o controlador deverá, em atendimento ao inciso VII, do artigo 18, possuir lista atualizada de quem são as entidades públicas e privadas com os quais compartilha os dados pessoais do titular, por ser seu direito solicitá-la a qualquer tempo. Assim, ainda que nesse caso o tratamento de dados pessoais do titular não exija o seu consentimento, pode ele exigir a informação quanto ao seu compartilhamento. Além disso, o controlador, sempre que solicitado pelo titular dos dados pessoais, deverá confirmar se realiza o tratamento dos mesmos imediatamente em formato simplificado e, na impossibilidade de fornecer imediatamente, terá o prazo de 15 dias para entregar ao titular, seja de forma impressa, seja em formato eletrônico, a declaração clara e completa dos dados pessoais que possui ou da inexistência de registro dos mesmos.

Ressalta-se, inclusive, que nem sempre o resultado colhido por um algoritmo refletirá a realidade do titular de dados, podendo o mesmo sofrer prejuízos caso não lhe seja possibilitada a revisão da decisão. Logo, em decisões automatizadas o titular poderá solicitar as informações necessárias que levaram a tomada de decisão. Não é porque foi um robô que tomou a decisão que o direito à transparência e ao livre acesso será tolhido do usuário, respeitados, evidentemente, os segredos comerciais. De forma que a revisão poderá ser feita tanto por uma pessoa natural como novamente por uma máquina, o que traz certa nebulosidade no *modus operandi* dessa revisão. A título de exemplo temos as seguradoras e as financeiras que de forma automatizada calculam o valor do prêmio a ser pago pelo segurado ou o valor do crédito e da taxa de financiamento de acordo com a análise de dados pessoais coletados para avaliar se o indivíduo é bom ou mau pagador, ou qual a probabilidade do mesmo em utilizar do seguro. Como já visto anteriormente, as máquinas, cada vez mais, têm tomado decisões de forma automatizada, como no caso da inteligência artificial, sendo que as mesmas vão coletando dados continuamente até se criar um determinado padrão e a partir dele tomam-se as decisões. Por isso, a preocupação do legislador com o limite de influência da

[427] FRAZÃO, Ana; TEPENDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** 2.ed. São Paulo: Thomson Reuters Brasil, 2020, p.344-360.

decisão de uma máquina sobre as vidas das pessoas, considerando-se que muitas vezes a análise de dados se dará de forma automatizada, sem a interferência de uma pessoa natural, o que pode levar a premissas errôneas e consequentemente a discriminações e abusos por parte do agente de tratamento.[428]

Há também que se falar que os dados pessoais informados pelo titular em um boletim de ocorrência ou processo judicial, por exemplo, não podem ser utilizados para prejudica-lo, uma vez que os mesmos foram informados ou se tornaram públicos visando exercício regular de um direito, como o de ação ou de defesa. Ressalta-se que não poderá qualquer pessoa física ou jurídica, pública ou privada, utilizar esses dados para prejudicar o titular, que somente os informou para exercer regularmente seu direito. No mais, é importante esclarecer que a lei possibilita ao titular dos dados que sua tutela em juízo seja individual, seja coletiva, quando sentirem que seus direitos estão sob ameaça.

Dessa forma, por mais evidente que possa parecer, esse assunto é de vital importância, pois revela ao indivíduo a titularidade de seus dados pessoais que integram sua personalidade, que deverão estar sob o “manto” da liberdade, privacidade e intimidade.

4.3.1.4 Sanções e multas propostas

A violação das exigências impostas pela LGPD pode sair caro, não só no bolso, como na reputação das instituições, o que para muitas pode ser irrecuperável. Assim, é importante estar em dia com o armazenamento adequado dos dados, e estar pronto para passá-los aos clientes, caso os solicitem, em até 15 dias.

Assim sendo, em caso de descumprimento da lei, as penalidades que podem ser impostas á instituição incluem advertência, obrigação de divulgação do incidente, eliminação ou bloqueio de dados pessoais, multa de até 2% (dois por cento) do faturamento anual da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil, no seu último exercício, excluídos os tributos, limitada, no total, de R$ 50.0000.000,00 (cinquenta milhões de reais) por infração cometida, e suspensão ou proibição das atividades de tratamento ou funcionamento do banco de dados.

---

[428] TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei geral de proteção de dados pessoais:** comentado artigo por artigo. 2.ed. ver., atual e ampl. Salvador: Editora JusPodivm, 2020, p.93-94.

Dessa forma, poderá ser imposto ao controlador o bloqueio ou até mesmo a eliminação do banco de dados do infrator dos dados pessoais relativos à infração, o que a depender do tipo de atividade da instituição poderá leva-la ao encerramento de suas atividades. Os órgãos públicos, não estarão sujeitos às multas estipuladas, entretanto sujeitar-se-ão às demais penalidades, sem prejuízo das demais leis pertinentes (servidor público, acesso à informação e improbidade administrativa).

Porém, uma das particularidades importantes da nossa LGPD é que devido à epidemia do coronavírus e o estado de calamidade pública no Brasil, o prazo para aplicação de multas e sanções (artigos 52 a 54) foi adiado para 1º de agosto de 2021. Enquanto isso, caso ocorram infrações, segue valendo o que determinam outras regulamentações referentes ao setor financeiro, tais como o Código de Defesa do Consumidor, a Lei de Sigilo Bancário, a Lei do Cadastro Positivo, as Resoluções e Circulares do Banco Central do Brasil (BACEN), como a Resolução 4.658/2018 e a Circular 3.909/2018, descritas anteriormente.

Para tanto, as multas que poderão ser aplicadas possuem valores máximos estabelecidos em lei, mas não possuem parâmetros objetivos definidos, o que também dependerá de regulamento próprio, que será editado após consulta pública. Além disso, a autoridade nacional precisará uniformizar critérios e tipos de sanção por infração de maneira a se evitar o *bis in idem* (repetição de uma sanção), bem como que se puna com eficácia o responsável pela infração cometida.

Portanto, as empresas de serviços financeiros, enquanto entidades responsáveis por determinar como os dados pessoais são utilizados, passarão a ter obrigações adicionais relativas ao tratamento desses dados. Entre tais obrigações, destacamos a necessidade de indicar um *Data Protection Officer* (DPO), pessoa encarregada de atuar na comunicação entre a organização e os titulares dos dados e a ANPD, conforme se verá adiante. Ainda, assim, precisam investir bastante na capacitação de seus profissionais, juntamente com soluções tecnológicas e a revisão de seus contratos. Isso, poderá ser feito a partir de três eixos: (i) o da solução de segurança de informação para proteção dos dados pessoais; (ii) da governança e gestão de riscos pelos contratos, documentos, normas, políticas; e (iii) da cultura, com a capacitação e as campanhas de conscientização, das equipes ou mesmo dos usuários clientes.

4.3.1.5 Quem é o DPO e qual o seu papel?

Primeiramente, o DPO tem um papel fundamental na LGPD atuando como canal de comunicação perante os titulares dos dados pessoais e aos órgãos reguladores. Ele deverá supervisionar todas as práticas de tratamento de dados pessoais dentro da organização e verificar se estas estão em conformidade com a Lei Geral de Proteção de Dados.

Embora o legislador nacional tenha copiado do GDPR a figura do *Data Protection Officer* (DPO; em português, Oficial de Proteção de Dados), optou por denominá-lo simplesmente de "encarregado", previsto nos artigos 5º e 41, da lei. Isso pode ser objeto de regulamentação pela ANPD, mas – até o presente momento – a legislação não limitou a sua obrigatoriedade a qualquer tipo de responsável pelo tratamento de dados, atribuindo – de acordo com a lei – a toda e qualquer pessoa física ou jurídica, que trate dados pessoais, a obrigatoriedade de se indicar um encarregado pelo tratamento desses dados.[429]

Assim sendo, a figura do encarregado foi inspirada no Regulamento Geral sobre a Proteção de Dados (GDPR). Na norma europeia estão previstos alguns critérios que tornam obrigatória a nomeação de um DPO. Diferentemente disso, no Brasil, esses critérios deverão ser determinados pela ANPD, que fará essa análise de quais instituições deverão ter necessariamente um DPO/encarregado de todos os tipos de tratamento de dados pessoais realizado por um controlador (agente de tratamento que realiza decisões sobre os dados pessoais), sendo, portanto, um cargo obrigatório para as instituições financeiras.

Pois bem, o DPO, é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), nos termos do art. 5º, inciso VIII, da LGPD. Nesta linha, é o responsável pelo plano de governança em proteção de dados e suas atividades consistem em (i) receber as reclamações e comunicações dos titulares dos dados pessoais e da ANPD; (ii) prestar esclarecimentos e tomar providências cabíveis; (iii) orientar a instituição internamente, os funcionários e contratados da entidade a respeito das práticas a

[429] TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei geral de proteção de dados pessoais:** comentado artigo por artigo. 2.ed. ver., atual e ampl. Salvador: Editora JusPodivm, 2020, p.123.

serem tomadas em relação à proteção de dados pessoais; (iv) realizar *Privacy Impact Assessments* (PIA) para averiguar o risco no uso de dados pessoais e a conformidade regulatória da instituição; (v) manter registros de todas as práticas de tratamento de dados pessoais conduzidas pela instituição, incluindo o propósito de todas as atividades desenvolvidas (*Data Mapping*); (vi) auxiliar no desenvolvimento de produtos, serviços e práticas por meio da adoção de metodologias como *privacy by design* e *data protection by design;* (vii) cumprir as demais atribuições que venham a ser determinadas pelo controlador ou estabelecidas em normas complementares, sobre a definição e as atribuições do DPO, conforme o art. 41, § 2º da LGPD.

Além disso, para o cargo de encarregado, é importante que haja a observância ao princípio de *accountability* (prestação de contas), responsabilização e prestação de contas, previsto no artigo 6º, inciso X da LGPD, correspondendo à obrigatoriedade de demonstração de medidas eficazes e cumprimento das normas de proteção de dados, como geração de evidências em forma de relatórios de impacto, geração de indicadores de incidentes, treinamento dos colaboradores, e outros sobre a conformidade com a LGPD, já que a lei é inteiramente baseada no respeito aos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Cabe ainda ao encarregado garantir a implementação das políticas internas criadas e a adaptação das mesmas aos novos produtos e necessidades que forem surgindo com o decorrer do tempo. A conformidade com a legislação de proteção de dados não é estática, e a instituição deve estar atenta para já prever a adequação de novos produtos, áreas ou negócios.

Há que se esclarecer, ainda, que a responsabilização do encarregado por eventuais desconformidades da instituição não deverá ocorrer. Salvo em casos pontuais em que fique demonstrado o dolo na sua atuação. Nos demais, a responsabilização caberá ao controlador e ao operador dos dados pessoais.

4.3.1.6 Autoridade Nacional de Proteção de Dados (ANPD)

Como já mencionado, após adiamentos e alterações com projeto de lei e medidas provisórias, a LGPD entrou em vigor no dia 18 de setembro de 2020. Logo depois de o Senado aprovar o Projeto de Lei de Conversão (PLV) 34/20, o

presidente da república assinou o decreto que cria a Autoridade Nacional de Proteção de Dados (ANPD). Assim, vale destacar que a ANPD, por definição, é o órgão da administração pública responsável por zelar e implementar a lei de proteção de dados em todo o território nacional, garantindo o cumprimento e o melhor proveito da regulamentação, seja por meio de normas complementares, pareceres técnicos e procedimentos de inspeção. Portanto, a ANPD, tem o objetivo de proteger os direitos fundamentais de liberdade e privacidade, orientar, promover e fiscalizar o cumprimento da LGPD, além de aplicar sanções administrativas em casos de violação no tratamento de dados.

Ademais, a Lei 14.010, de 2020 adiou de 1º de janeiro de 2021 para 1º de agosto de 2021 a vigência das sanções que a Autoridade Nacional de Proteção de Dados (ANPD), ainda pendente de instalação, pode aplicar nos órgãos, entidades e instituições que lidam com o tratamento de dados. O governo federal já aprovou a estrutura regimental e o quadro de cargos da ANPD, mas a nomeação do Conselho Diretor e do diretor-presidente terão de passar pela aprovação do Senado.

Conforme demonstrado, o órgão foi criado pela Lei Geral de Proteção de Dados Pessoais (LGPD – Lei 13.709, de 2018), para zelar pela proteção dos dados pessoais, assegurar a observância de segredos comerciais e industriais e punir eventuais descumprimentos à legislação.

Cumpre esclarecer, ainda, que a Autoridade Nacional de Proteção de Dados, após muito debate, foi criada como sendo uma autoridade de natureza jurídica transitória, ou seja, em um primeiro momento ela será um órgão da administração pública federal, submetida a um regime autárquico especial e vinculada à Presidência da República. O principal questionamento que foi trazido à tona durante o trâmite da MP nº 869/2018, que originou a lei nº 13.853/2019, foi sobre a indispensável autonomia da autoridade, sendo mister sua desvinculação com outros órgãos a fim de garantir a adequada segurança jurídica de suas decisões.[430] E curiosamente volta às questões que eram entrave quando o órgão foi criado, há quase dois anos, de falta de autonomia e independência da Autoridade. Justamente por isso o ideal seria ter um órgão independente, com meios de alcançar eficiência e sustentabilidade.

---

[430] TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei geral de proteção de dados pessoais:** comentado artigo por artigo. 2.ed. ver., atual e ampl. Salvador: Editora JusPodivm, 2020, p.150-151.

Nota-se que mesmo inoperante no momento, a ANPD, será responsável por editar normas e fiscalizar procedimentos relativos à proteção de dados pessoais. Ainda, assim, terá papel decisivo na interpretação e balizamento dos dispositivos da LGPD que servirão como norte para seus destinatários.[431] Ou seja, dada a sua especialidade, a ela caberá definir qualitativamente os parâmetros do interesse legitimo, comungando-se o conhecimento técnico das formas de tratamento com a sua respectiva juridicidade. Isso porque, simultaneamente aos impactos técnicos do tratamento, a Autoridade deverá se pautar por questões jurídicas, as quais a obrigam valorar o bem inserido no ordenamento, de forma a desenvolver solução ágil e segura para decisões sobre o tema.[432]

Por isso, a atuação da ANPD faz muita falta, pois é uma Autoridade com um papel muito relevante na estruturação de todo o sistema de proteção de dados pessoais. Como a LGPD é considerada uma lei horizontal e traz artigos mais amplos sujeitos a complementação, ter uma Autoridade é importante não apenas para ações de fiscalização, mas também de regulamentação e complementariedade de alguns tópicos. Afinal, o objetivo de uma regulamentação de proteção de dados pessoais é harmonizar as relações, aumentar o grau de transparência para fomentar a Livre Economia Digital. E ainda, estimular a inovação, a partir de regras claras e controles mínimos de segurança, para inclusive não sofrermos barreiras comerciais com outros países. São dispositivos para facilitar a atração de investimentos e contribuir com o crescimento econômico.

Desse modo, infelizmente, não há como escapar do clichê de necessidade de uma regulamentação especifica pela ANPD sobre assuntos que necessitam de uma atenção especial sem que se trave o avanço tecnológico e a inovação, de forma a não prejudicar o mercado, mas a definir formas de se continuar desenvolvendo tecnologias e, ao mesmo tempo, respeitando os direitos fundamentais dos titulares.[433]

Contudo, enquanto aguardamos por novas definições, surgem muitas dúvidas em relação à aplicação da lei. Como em relação ao dever de *report,* conforme o art.

---

[431] PALHARES, Felipe. et al. **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020, p.111.
[432] FRAZÃO, Ana; TEPENDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** 2.ed. São Paulo: Thomson Reuters Brasil, 2020, p.468.
[433] PALHARES, Felipe. et al. **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020, p.94.

48: "O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares". Para quem deve ser feito, então? Por ora, a indicação é que seja feita para outra Autoridade. No caso das instituições financeiras, seria o próprio BACEN, por ser o seu regulador. O importante é registrar e armazenar as provas e comunicar o mais breve possível sobre o acontecimento. Além disso, a ANPD e o BACEN, segundo a Lei Geral de Proteção de Dados Pessoais, devem manter consonância, harmonia em suas ações e regulações.

Nota-se, portanto, que mesmo com a recomendação de ser um órgão dotado de autonomia e que tenha um corpo técnico seleto, considerando a matéria especializada que deverá tratar, há muitas incertezas que pairam sobre como será de fato a personalidade e o “tom” da autoridade de proteção de dados à moda brasileira. Mas uma coisa é certa: é dela que devemos cobrar a disseminação da cultura sobre a nova legislação, a criação das melhores práticas setorizadas, a centralização de interpretações, a realização de campanhas educativas para a população e a responsabilidade para que o tratamento de dados realizados pelo poder Público esteja em conformidade com a lei e, caso entenda necessário, estipular outros requisitos ou adequações para que esse tratamento esteja dentro dos parâmetros legais. Daí a importância de a autoridade nacional ser um órgão independente, autônomo e altamente especializado, visto que a lei afeta todos os setores do país, tanto público quanto privado e considerando a sua importância na fiscalização do próprio poder Público deverá poder atuar sem qualquer vínculo ou receio.

Por fim, com o atraso em sua efetiva implementação provoca um cenário em que aumenta o grau de violações de direitos fundamentais, seja por agentes privados, seja por órgãos ou entidades públicas. Pode também significar a perda de oportunidade de criar melhor ambiente de negócio aos agentes privados que precisam de segurança jurídica, institucional e regulatória para a concretização de investimentos.

4.3.1.7 *Open Banking* (Sistema Financeiro Aberto) e a “nova” Lei do Cadastro Positivo

Justifica-se aqui um parêntese, para discorrer-se, ainda que brevemente, acerca de dois assuntos de grande relevância envolvendo dados pessoais para o setor financeiro, o *Open Banking* (Sistema Financeiro Aberto) e a “nova” Lei do Cadastro Positivo. Ambos, aos poucos, estão revolucionando o Sistema Financeiro Nacional, ampliando as possibilidades de acesso aos dados pessoais, mas com cautela e sustentabilidade, atendendo princípios de segurança e privacidade de dados cada vez mais cobrados e exigidos pela sociedade.

Primeiramente, o Open Banking pode ser definido como um modelo colaborativo no qual os dados bancários são compartilhados por meio de interface de programação de aplicativo (API), um conduíte inteligente que permite o fluxo de dados entre sistemas de maneira controlada, mas contínua, entre duas ou mais partes não afiliadas para fornecer recursos aprimorados ao mercado. As APIs têm sido usadas há décadas, principalmente nos Estados Unidos, para habilitar *software* de gerenciamento financeiro pessoal, apresentar detalhes de faturamento em *sites* de bancos e conectar desenvolvedores a redes de pagamentos como Visa e Mastercard. No entanto, as APIs estão recebendo atenção renovada como um meio de aprimorar a entrega de serviços financeiros. Até agora, entretanto, essas conexões têm sido usadas principalmente para compartilhar informações, em vez de transferir saldos monetários.

Há, ainda, a definição de “Open Banking” dada pela Resolução Conjunta nº 1 em seu art. 2º, I: “compartilhamento padronizado de dados e serviços por meio de abertura e integração de sistemas”.

Dessa forma, o sistema financeiro aberto é uma iniciativa que pressupõe a “abertura” dos dados pertencentes aos clientes de instituições financeiras e outras instituições reguladas pelo Banco Central do Brasil (BACEN). Mediante consentimento[434] fornecido pelo cliente ou titular dos dados, as instituições financeiras e/ou outras instituições reguladas pelo BACEN devem compartilhar os dados cadastrais e dados de transações financeiras com outras organizações

[434] Deve ser solicitado de maneira clara, objetiva e adequada. Deve, ainda, especificar a finalidade do compartilhamento e o prazo de validade de acordo com a finalidade solicitada (máximo 12 meses). Ademais deve indicar quais dados serão compartilhados, mediante identificação do cliente.

participantes do sistema Open Banking, por meio de sistemas interoperáveis. Recentemente, o Banco Central do Brasil publicou a Circular nº 4.015 e, em conjunto com o CMN, a resolução nº 1, ambas de 4 de maio de 2020 (“Resolução Conjunta”), que regulamentam como será implementado o Open Banking no Brasil. A Circular nº 4.015, ainda, regulamenta e padroniza quais dados estão sujeitos aos sistemas e quais devem ser disponibilizados para compartilhamento. A Resolução Conjunta estabelece que os dados pessoais de clientes somente poderão ser compartilhados com terceiros mediante o consentimento do cliente, como a manifestação livre, informada, prévia e inequívoca de vontade, feita por meio eletrônico, pela qual o cliente concorda com o compartilhamento de dados ou serviços para finalidades determinadas. Assim diferentemente do que dispõe a LGPD, autorizando o tratamento (e, portanto, o compartilhamento) de dados pessoais em outras bases legais com o consentimento do titular, a portabilidade ou compartilhamento de dados dentro do sistema *Open Banking* dependerá sempre do consentimento do titular dos dados. Ainda, de acordo com a Resolução, o consentimento, os registros de acesso e revogação do consentimento devem ser armazenados pelo prazo mínimo de 5 (cinco) anos (art. 49 da Resolução Conjunta). Além do consentimento, antes de concluir o compartilhamento de dados, as instituições deverão observar as etapas de autenticação (do titular ou da instituição solicitante dos dados, conforme aplicável) e confirmar a operação. De modo similar a LGPD e a resolução CMN 4.658/2018, a Resolução Conjunta também determina a obrigatoriedade das instituições participantes de nomear um Diretor Responsável pelo compartilhamento (art. 32 da Resolução), responsável por produzir semestralmente relatório de compartilhamento (nas datas-bases de 30 de junho e 31 de dezembro). Tal relatório deve ser submetido ao conselho de administração ou, na sua inexistência, à diretoria da instituição até noventa dias após a respectiva data-base. Por fim, a Resolução Conjunta permitirá o compartilhamento de dados entre instituições financeiras e seus parceiros de negócio não regulados (artigo 36 da resolução), desde que obtido o consentimento do titular, adotadas medidas organizacionais e condições contratuais específicas, conforme estabelecido na Resolução.[435]

Percebe-se, que ao estar de acordo com as novas normas do Open Banking, a instituição também, tem que estar pronta para atender a LGPD. Como a resolução

[435] PALHARES, Felipe. et al. **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020, p.145-150.

do Bacen estabelece que o compartilhamento é legitimado pelo consentimento, deve haver a harmonização com a LGPD, aplicando-se os demais direitos do titular previstos em lei. Assim, a instituição doadora dos dados permanece na posição de controladora e responsável pela proteção dos dados pessoais dos seus clientes sob as diretrizes da LGPD. Por isso, é muito importante manter a rastreabilidade para comprovar tanto a conformidade à lei quanto para eventual comprovação de origem de determinado incidente, e cumprir os requisitos necessários ao compartilhamento, que deve passar por um fluxo de: consentimento, autenticação e confirmação, como representado pela seguinte (figura 8):

Figura 8 – Requisitos necessários ao compartilhamento de dados

Fonte: Patrícia Peck Pinheiro[436]

Observações:

1- Com a utilização de API e o compartilhamento de informações, a instituição receptora também assume a posição de controladora e deverá observar a necessidade de enquadramento entre as hipóteses legais da LGPD para justificar tratamento dos dados pessoais após o recebimento via API. Além

[436] Revista CIAB - FEBRABAN. 2020. **Open banking:** cibersegurança e gestão de dados no Sistema Financeiro Aberto. Disponível em: < https://noomis.febraban.org.br/especialista/patricia-peck-pinheiro/open-banking-cibersegurança-e-gestao-de-dados-no-sistema-financeiro-aberto?pesquisa=sigilo-bancario>. Acesso em: 19 out. 2020.

disso, como a Resolução do Bacen estabelece que o compartilhamento será legitimado pelo consentimento, o compartilhamento de dados pessoais também deverá estar harmonizado com a LGPD, aplicando-se os demais direitos do titular previstos em lei. Exemplo: revisão de decisões automatizadas, exclusão de dados, correção ou limitação de tratamento etc.

2- Sob as diretrizes da LGPD, será necessário observar a responsabilidade pelas decisões relativas ao tratamento de dados pessoais, inclusive assumindo, junto com a outra instituição controladora, obrigações mútuas perante os titulares e o dever de colaboração mútuo e garantia da adoção de medidas técnicas e organizacionais aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequada ou ilícita.

3- Há, porém, dados que não serão objeto de compartilhamento, tais como: dados pessoais sensíveis pela legislação (conforme a LGPD), notas ou pontuações de crédito, credenciais e informações de autenticação dos clientes, assim como o que envolver segredo comercial. O ideal é que as instituições participantes compartilhem os dados e informações considerados estritamente necessários à execução da finalidade autorizada por meio do consentimento do cliente, pois o excesso de informações, além de expor o cliente, pode causar prejuízos a ele.

4- As empresas de serviços financeiros participantes do Open Banking devem prestar informações claras e objetivas, com contrato de Termo de Uso e Política de Privacidade[437] atualizados que já prevejam requisitos para o

[437] O lançamento de algum produto ou serviço que tenha como ambiente de negociação a rede mundial de computadores não pode prescindir de um documento chamado “Termo de Uso”, que pode ou não ser acompanhado das regras observadas pela instituição sobre privacidade, normalmente denominado de “Política de Privacidade”. O “Termo de Uso ou Termo de Aceite ou Termo de Serviço, ou Termo de Acesso ou Termo e Condições” diz respeito às regras combinadas com o usuário para utilização do produto oferecido, seja para limitar certas aplicações, seja para impor deveres e alertar sobre direitos. A “Política de Privacidade” diz respeito ao direito à privacidade. É preciso esclarecer o usuário sobre o que será feito com os dados que serão coletados e qual o nível de segurança e privacidade oferecidos. Muito embora os termos de uso e política de privacidade sejam desconsiderados pelo usuário que assina sem jamais prestar atenção no texto, é importante fazer o esclarecimento para evitar problemas no futuro. Alguns mecanismos, já à disposição no mercado, podem ajudar a conscientizar o usuário da importância da leitura e compreensão do termos, como, por exemplo: (i) exigir que o usuário faça a rolagem de todo o texto para fazer a assinatura ao final; (ii) exigir cadastro do usuário prévio e envio do termo de uso para o *e-mail* fornecido como condição para ter acesso ao produto; (iii) exigir o clique no botão que declare expressa concordância com os termos de uso e política de privacidade e (iv) apresentar um texto com letras grandes o suficiente

> compartilhamento das informações. Ainda, a necessidade de gestão de risco que abrangem soluções técnicas, a partir de uma referência de padrões de criptografia, fator de autenticação e nível de segurança em APIs; e soluções documentais, ligadas aos contratos de terceirização dos serviços, com o estabelecimento de cláusulas e até realização de auditorias. Tudo isso precisa estar alinhado com as novas funções, como a do responsável pela segurança cibernética (devido a res. 4.658) e a do encarregado também conhecido por DPO (devido à LGPD), para, assim, evitar problemas com a falta de investimento nas áreas corretas ou então com a necessidade de refazer o projeto que não contemplou essas delimitações.

Nota-se, portanto, que Open Banking se baseia em uma premissa básica – a de que os dados de transações, histórico financeiro e informações gerais de um indivíduo são de propriedade dele e não da instituição financeira. Com isso, o cliente tem o poder de escolha em relação ao que deseja fazer com esses dados, podendo, por exemplo, compartilhá-los com provedores de serviços financeiros de sua escolha. Esse terceiro, provedor de serviços financeiros, poderia então utilizar os dados desse cliente para ofertar novos produtos e serviços financeiros inovadores e adaptados às necessidades do mesmo. Contudo, apesar de parecer simples e bastante óbvio, o tema tem se tornado centro de discussões entre *fintechs*, bancos, reguladoras e clientes de serviços financeiros mundo afora, devido ao fato de que, para que tudo isso aconteça, é necessário desenvolver padrões que permitam o compartilhamento de dados bancários de forma fácil e segura entre as instituições participantes do mercado financeiro. Essa conexão e troca de informações se daria através de interfaces de programação de aplicações (APIs), conforme visto anteriormente. As “APIs abertas” permitiriam que terceiros, desde que autorizados pelos clientes, acessassem informações importantes sobre produtos bancários, sendo elas taxas de juros, termos, condições de operações e também dados de contas de clientes, como histórico de transações e saldos de contas. A utilização desses dados, por sua vez, aumenta a dúvida quanto aspectos relativos à troca de informações, de forma segura, com terceiros.[438]

---

para chamar a atenção e destaque para as cláusulas que limitam o exercício de certos direitos ou restringem o uso por parte do cliente.

[438] DINIZ, Bruno. **O Fenômeno *Fintech*:** tudo sobre o movimento que está transformando o mercado financeiro no Brasil e no mundo. Rio de Janeiro: Alta Books, 2019, p.196.

Por isso, a padronização é a chave para um sistema de Open Banking dar certo. Isso porque o tráfego de dados por APIs traz consigo uma série de novos riscos, e demanda uma política de privacidade e segurança bem estabelecida, para mitigar vulnerabilidades e delimitar responsabilidades dos *players* que operam dentro desse fluxo de informações. Destaque para algumas questões: (i) como limitar a responsabilidade, principalmente considerando um ambiente maior de interoperabilidade via APIs. Com especial atenção a situações em que não seja possível alcançar via contratos, principalmente devido a possíveis intepretações da Súmula 479 do Superior Tribunal de Justiça, emitida em junho de 2012, e que esclarece que “as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias”; (ii) o Art. 1.016 do Código Civil, que determina: “os administradores respondem solidariamente perante a sociedade e os terceiros prejudicados, por culpa no desempenho de suas funções”. Diante do risco intersistêmico, como limitar a responsabilidade das instituições participantes? Em caso de vazamento, haverá responsabilização solidária? Assim, a ausência de limitação de responsabilidade poderá prejudicar instituições que não incorrem no evento danoso (ex.: adoção de rito sumaríssimo nos Juizados Especiais Cíveis, não há dilação probatória). São questões que precisarão ser previstas e melhoradas e que podem também ser tratadas no âmbito da convenção.

Outro ponto, interessante, gira em torno da relação ao dever de editar “dados confidenciais” em certas circunstâncias, bem como às obrigações de fornecedores terceirizados de excluir/destruir dados após um período. Muitos desses detalhes ainda são um trabalho em andamento e serão refinados conforme os impactos do mercado bancário aberto se manifestem. Os bancos digitais estão compreensivelmente preocupados com esses detalhes, já que qualquer erro de divulgação percebido quase certamente irradiará de volta para sua marca.

Com base nos casos mencionados, com a maior circulação de dados pessoais, consequentemente haverá um aumento na responsabilidade dos custodiantes dessas para assegurar sua segurança no compartilhamento. Assim, existe a necessidade de criação de padrões e requisitos, em consonância direta com o disposto pela LGPD, para diminuir fortemente o risco de compartilhamento

indevido desses dados.[439] Inclusive, não foram poucos os desafios regulatórios enfrentados pelo CMN e o BACEN para que a implementação do Open Banking no Brasil pudesse ter segurança jurídica, especialmente em relação à Lei Geral de Proteção de Dados Pessoais ("LGPD", Lei n. 13.709/18).[440]

Como se vê, o Open Banking trará desafios e oportunidades para diversos setores. Na prática a sua implementação permitirá a gestão de dados financeiros pelos titulares, que terão controle total sobre os seus dados, antes guardados a sete chaves por um único banco. O modelo impactará qualquer segmento que tenha algum tipo de operação financeira, não apenas bancos. Nesse contexto, as *fintechs* terão um papel fundamental para as empresas, considerando sua agilidade, escalabilidade e a capacidade em oferecer experiência positiva, contribuindo para a criação de novas oportunidades de negócios,[441] uma melhor experiência do cliente, novos fluxos de receita e um modelo de serviço sustentável para mercados tradicionalmente mal atendidos. Além disso, a norma visa aumentar a eficiência no mercado de crédito e de pagamentos no Brasil, mediante a promoção de ambiente de negócio mais inclusivo e competitivo, preservando a segurança do sistema financeiro e a proteção dos consumidores.

Por fim, algumas premissas basilares do *Open Banking*: (1) dados têm valor, principalmente na sociedade contemporânea; (2) em linha com a LGPD, o consumidor é titular de seus próprios dados e, por isso, detém o poder de decisão quanto ao que ocorre com eles; (3) dados referentes a operações financeiras de consumidores são privados e sigilosos, nos termos da Lei do Sigilo Bancário; (4) possuir dados sigilosos significa, além de responsabilidade, uma enorme oportunidade de entender o perfil dos consumidores e poder ofertar produtos e serviços com base em padrões identificados; e (5) o setor financeiro sempre foi severamente regulado e restrito, o que determinou a concentração desse mercado por poucas e grandes instituições financeiras que por muito tempo foram as únicas a terem acesso aos dados bancários dos consumidores.

---

[439] EROLES, Pedro. ***Fintechs*, Bancos Digitais e Meios de Pagamento:** aspectos regulatórios das novas tecnologias financeiras. São Paulo: Quartier Latin, 2019, p.45.

[440] MORIBE, Gabriela Tiemi. **Série Open Banking no Brasil:** a proteção de dados pessoais na regulação do Open Banking. Disponível em: https://baptistaluz.com.br/wp-content/uploads/2020/09/BLUZ_Open-banking-lgpd.pdf>. Acesso em: 19 out. 2020.

[441] EROLES, Pedro. ***Fintechs*, Bancos Digitais e Meios de Pagamento:** aspectos regulatórios das novas tecnologias financeiras. São Paulo: Quartier Latin, 2019, p.153-207.

Encerrando essa necessária introdução ao tema, Open Banking, em paralelo, cabe mencionar, também, o cadastro positivo, que visa beneficiar aqueles que possuem histórico de “bom pagador”. Trata-se, assim, de um banco de dados que coleta informações relativas ao histórico financeiro e de pagamentos do consumidor em diferentes tipos de obrigações com instituições financeiras e provedores de serviço. Os dados financeiros processados no cadastro positivo incluem informações sobre a concessão de créditos e outras operações financeiras, incluindo data, valor, número de parcelas, datas de pagamento, parcelas pagas (no todo ou em parte) ou em atraso, entre outras. Originalmente criado no Brasil em 2011, com a Lei do Cadastro Positivo (Lei 12.414/2011), a inclusão de indivíduos nesse banco de dados exigia o consentimento do consumidor. A necessidade de obtenção do consentimento implicou baixa taxa de adesão por parte dos consumidores. Com as alterações recentes, a inclusão de consumidores no cadastro passa a ser automática e tais indivíduos serão notificados por prazo de 30 dias a partir da criação de seu perfil. Ao consolidar as informações em um banco de dados, o consumidor agora pode consultar suas informações e verificar suas obrigações de pagamento de forma centralizada, permitindo um melhor controle de suas finanças pessoais e uso consciente de crédito. Porém, apesar do registro automático, o indivíduo terá o direito de optar por não participar do cadastro, a qualquer momento, por meio eletrônico. Ainda, assim, a nova Lei do cadastro Positivo[442] proíbe expressamente o uso de informações consideradas excessivas (ou seja, aquelas que não estão vinculadas à analise de risco de crédito do consumidor) ou o tratamento de dados sensíveis (ou seja, informações que revelem origem étnica e social, saúde, informações genéticas, orientação sexual e crenças políticas, religiosas e filosóficas) para formar o histórico e/ou o *score* de crédito (*credit score*), nota de pontuação de crédito que indica o comportamento financeiro do consumidor. Além disso, as informações tratadas no cadastro positivo devem ser consideradas confidenciais entre os gestores do banco de dados e a divulgação não autorizada implicará violação do sigilo bancário. Incidentes de segurança ou violação de dados,

[442] A Nova Lei do Cadastro Positivo, inclui automaticamente todos os consumidores, pessoas naturais e jurídicas, (modelo *opt out*), estima-se que algo em torno de 140 milhões de pessoas integrarão o cadastro. O Brasil passa a conviver, a partir de julho de 2019, com a Nova Lei do Cadastro Positivo que pretende, ao permitir a análise de histórico de crédito de milhões de consumidores, reduzir, para os bons pagadores, a taxa de juros. A Lei Complementar nº 166, com início de vigência de julho de 2019, regulamentada pelo Decreto nº 9.936/2019, altera substancialmente a Lei 12.414/11, conhecida como Lei do Cadastro Positivo. Mais da metade da norma foi modificada: é possível falar, assim, na existência de uma Nova Lei do Cadastro Positivo.

envolvendo dados do cadastro positivo devem ser notificados à ANPD, ao Banco Central do Brasil e à Secretaria Nacional do Consumidor vinculadas ao Ministério da Justiça (SENACON), dentro de dois dias úteis do conhecimento. Por fim, além das regras especificas do cadastro positivo, os princípios e obrigações estabelecidas na LGPD também devem ser observados na utilização de dados pessoais advindos dessa base de dados.[443]

Fazendo um paralelo, com a LGPD, faz-se necessário demonstrar o (quadro 4) comparativo dos principais pontos de cada uma das regulamentações, com suas semelhanças e diferenças:

Quadro 4 – Comparativo entre a LGPD e a Lei do Cadastro Positivo

Lei Cadastro Positivo – art. 5º	LGPD – art. 18
Cancelamento/ reabertura do cadastro	Eliminação/ Revogação do consentimento
Opt-in automático, carta notificação quando da inclusão	Confirmação da existência de tratamento
Acesso	Acesso
Impugnação/ Correção	Retificação/ Correção
Conhecimento sobre principais elementos e critérios para análise de risco	Conhecimento sobre principais elementos e critérios para o tratamento de dados pessoais
Não há correspondência	Anonimização, bloqueio ou eliminação de dados desnecessários ou excessivos
Informação prévia sobre a identidade do gestor, o armazenamento e o objetivo do tratamento dos dados pessoais	Informações sobre compartilhamento
Revisão pelo consulente de decisão realizada exclusivamente por meios automatizados*	Revisão de decisão realizada exclusivamente por meios automatizados*
Dados já são compartilhados entre os gestores e financeiras	Portabilidade
Ter os seus dados utilizados somente com a finalidade em que foram coletados	Ter os seus dados utilizados somente com a finalidade em que foram coletados

Fonte:Patricia Peck Pinheiro[444]

A partir do quadro comparativo exposto, destacam-se, ainda, questões supostamente relevantes sobre a norma de proteção de dados e a Lei do Cadastro

[443] PALHARES, Felipe. et al. **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020, p.142-144.
[444] Revista CIAB - FEBRABAN. 2020. **Como as financeiras devem se preparar para 2020:** o ano da LGPD. Disponível em: < https://noomis.febraban.org.br/especialista/patricia-peck-pinheiro/como-as-financeiras-devem-se-preparar-para-2020-o-ano-da-lgpd?pesquisa=nova-lei-do-cadastro-positivo>. Acesso em: 19 out. 2020.

Positivo (LCP), conforme aponta Oscar Valente Cardoso[445], de forma exemplificativa, as seguintes:

1. Banco de dados (arts. 2º, I, e 3º, da LCP): há um conceito legal de banco de dados, consistente no "conjunto de dados relativo à pessoa natural ou jurídica armazenados com a finalidade de subsidiar a concessão de crédito, a realização de venda a prazo ou de outras transações comerciais e empresariais que impliquem risco financeiro". A definição da LGPD é mais restrita quanto aos sujeitos (apenas pessoas naturais) e mais genérica quanto ao objeto, porque não limita o objetivo do agrupamento dos dados: "conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico (art. 5º, IV, da LGPD);
2. Prestação de informações objetivas, claras, verdadeiras e de fácil compreensão (art. 3º, § 2º, da LCP): essa regra complementa as regras do Código de Defesa do Consumidor (arts. 31, *caput*, e 54, § 3º, do CDC) e deve ser utilizada como parâmetro para qualquer contrato bancário que tenha entre seu objeto o tratamento de dados. A característica das informações exigidas na LCP e no CDC serve para evitar dúvidas nos consumidores e conflitos sobre a interpretação dos dispositivos contratuais, além de permitir que o consentimento do titular dos dados seja efetivamente consciente e expresso. Na LGPD, a necessidade de prestação de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento (observados os segredos comercial e industrial) consta na descrição do princípio da transparência (art. 6º, VI, da LGPD). Além disso, quando for solicitado, o controlador deve fornecer, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, desde que igualmente respeitados os segredos comercial e industrial (art. 20, § 1º, da LGPD);
3. Autorização para a abertura de cadastro (art. 4º, I, da LCP): uma das alterações realizadas pela Lei Complementar nº 166/2019 está na abertura do cadastro positivo pelo próprio controlador (gestor), ou seja, não é mais

[445] CARDOSO, Oscar Valente. Lei Geral de Proteção de Dados e o diálogo das fontes: 5) Lei do Cadastro Positivo. **Revista Jus Navigandi**, Teresina, ano 25, ago. 2020. Disponível em: < https://jus.com.br/artigos/84868/lei-geral-de-protecao-de-dados-e-dialogo-das-fontes-5-lei-do-cadastro-positivo>. Acesso em: 15 out. 2020.

condicionado ao requerimento ou ao consentimento prévio do titular de dados (o que era previsto até então, no *caput* do art. 4º). Por ser um cadastro benéfico aos usuários dos serviços bancários, inverteu-se a ordem, com a autorização do gestor (que é a pessoa jurídica que administra o banco de dados) para a abertura do cadastro e permite ao titular requerer a sua exclusão. Na LGPD, o consentimento é apenas um entre os dez incisos do art. 7º que contêm hipóteses autorizativa do tratamento dos dados pessoais, entre as quais também está a proteção do crédito (inciso X do art. 7º da LGPD);

4. Permissão do compartilhamento dos dados do titular entre controladores (art. 4º, III, da LCP): além da abertura do cadastro positivo, os gestores podem compartilhar os dados existentes nos cadastros entre os bancos de dados, se o titular não apresentar oposição, após ser notificado previamente da inclusão, nos termos da regra anterior. Por sua vez, na LGPD o consentimento do titular para o compartilhamento é exigido quando também tiver sido um pressuposto para o tratamento dos dados (art. 7º, I e § 5º, da LGPD);
5. Comunicação inequívoca do titular (art. 4º, § 4º, I a III, da LCP): essa norma é similar à prevista no art. 43, *caput* e § 2º, do CDC, ao exigir a comunicação do titular dos dados sobre a abertura, para que ele mantenha, requeira a retificação ou opte pela exclusão de seus dados do cadastro positivo. De acordo com o CDC, a LCP e a LGPD, a abertura de qualquer espécie de banco de dados deve ser informada de forma clara ao titular dos dados (com fundamento no princípio da autodeterminação informativa e nas regras legais), o que assegura o seu conhecimento e (quando for exigido) o seu consentimento informado e inequívoco (art. 5º, XII, da LGPD);
6. Dispensa do dever de comunicação (art. 4º, § 5º, da LCP): o dever de comunicação do titular dos dados pessoais é dispensado quando ele já estiver (legalmente) incluído em outro cadastro da mesma espécie. Assim, quando já existir um cadastro positivo anterior do titular com outro gestor, admite-se o compartilhamento dos dados entre os controladores, independentemente do consentimento do titular, para a sua inclusão em outro banco de dados de cadastro positivo. Essa medida permite a uniformização da pontuação do titular e o seu tratamento isonômico por instituições

diferentes. Ressalva-se, contudo, que não exclui o direito do titular de ciência do compartilhamento e de novo cadastro de tratamento dos seus dados, com a identificação do controlador;

7. Prazo de resguardo da divulgação dos dados (art. 4º, § 7º, da LCP): em complemento à regra da comunicação, existe um prazo legal de resguardo, de 60 dias a partir da inclusão, para que o cadastro positivo seja disponibilizado a terceiros. Nesse prazo, o titular pode pleitear a exclusão ou a retificação dos seus dados;
8. Direitos do Cadastrado (art. 5º da LCP): a LCP contém um rol de direitos do titular dos dados inserido nos bancos de dados de cadastros positivos, o que compreende a operação de todas as formas de gestão dos dados tratados, de abertura, retificação, oposição, exclusão, conhecimento dos critérios de decisão e revisão. Portanto, a maior parte dos direitos do titular previstos no art. 18 da LGPD já é assegurada pela Lei do Cadastro Positivo (mas de forma específica para esses cadastros);
9. Responsabilidade objetiva e solidária entre o controlador e interessados nas consultas (art. 16 da LCP): de forma similar ao previsto nos arts. 12, 14 e 25, § 1º, Código de Defesa do Consumidor, a responsabilidade do controlador e das entidades consulentes é objetiva e solidária. Em suma, todas as pessoas envolvidas na cadeia de tratamento de dados podem ser responsabilizadas, de forma objetiva e solidária, pelos incidentes ocorridos e os danos causados aos titulares. Existem regras semelhantes para a responsabilização do controlador e do operador no exercício de atividade de tratamento de dados pessoais (art. 42 da LGPD), com hipóteses específicas de excludentes da responsabilidade (art. 43 da LGPD).

Assim sendo, o STJ passou a examinar questões atinentes ao cadastro positivo de crédito, visto que, além do direito de acesso e do direito à correção da informação, já previstos no CDC, incluiu, expressamente, entre os direitos do cadastrado : (i) o direito de obter o cancelamento do cadastro; (ii) o direito de conhecer os principais elementos e critérios considerados para a análise de risco; (iii) o direito de ser informado previamente sobre o armazenamento, a identidade do gestor do banco de dados, o objetivo do tratamento dos dados pessoais e os destinatários dos dados em caso de compartilhamento; (iv) o direito de solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados;

(v) o direito de ter os seus dados pessoais utilizados de acordo com a finalidade para qual foram coletados.[446]

A rigor, especialistas entendem que, no longo prazo, o novo cadastro tende a tornar o acesso ao crédito mais fácil e com juros menores para consumidores e empresas que honram seus compromissos financeiros. O bom pagador terá um *score* (nota de pontuação de crédito que indica o comportamento financeiro do consumidor) mais alto e essa pontuação poderá ser considerada pelas instituições financeiras em eventuais concessões de crédito, conforme o Banco Central. A expectativa é que outros segmentos da economia comecem a fornecer informações de pagamentos dos clientes. As conversas mais adiantadas se dão com o setor de telecomunicações e se estima que os dados passem a ser enviados dentro de três a seis meses. Em seguida, ingressarão as empresas de *utilities* (água, luz e gás) e o varejo (lojas que operam com crediário e cartão de crédito próprio). As negociações já estão em andamento.[447]

Em síntese, o governo elaborou o Projeto de Lei Complementar 441/2017, que deu origem à Lei Complementar 166/2019, que altera a Lei 12.414/11. O Projeto alterou o modelo de inclusão dos consumidores no sistema de cadastro positivo, com o intuito de ampliar a base de dados de “bons pagadores”. Para que as alterações feitas na LCP fossem levadas a cabo, o Poder Executivo editou novo Decreto regulamentador (Decreto nº 9.936, 24 de julho de 2019), estabelecendo diretrizes para a constituição dos gestores de banco de dados, a disponibilização de histórico de crédito, as hipóteses de vazamentos de dados, etc. Ademais, o BACEN, em 29 de julho de 2019, editou a Resolução nº 4.737/19 e a Circular nº 3.955/19 para impor normas de registro dos gestores de banco de dados junto ao BACEN para o recebimento de informações de adimplemento das instituições financeiras, bem como da forma de fornecimento destas informações. Por exemplo, há previsão de que não constitui quebra do dever de sigilo bancário o compartilhamento, por parte de instituições financeiras e demais autorizadas pelo Banco Central do Brasil

---

[446] FRAZÃO, Ana; TEPENDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** 2.ed. São Paulo: Thomson Reuters Brasil, 2020, p.87.

[447] Revista CIAB - FEBRABAN. 2019. **Bancos dão a largada ao novo Cadastro Positivo.** Disponível em: < https://noomis.febraban.org.br/temas/regulacao/bancos-dao-a-largada-ao-novo-cadastro-positivo?pesquisa=nova-lei-do-cadastro-positivo>. Acesso em: 13 set. 2020.

("BACEN"), de dados de adimplemento aos gestores de bancos de dados cadastrados junto ao BACEN.[448]

Tendo em vista as premissas já expostas, é de fundamental importância entender que a LGPD também dialoga com a Lei do Sigilo Bancário (Lei Complementar nº 105/2001), não apenas nas relações dos clientes com as instituições, mas ainda nas relações jurídicas das instituições financeiras entre si e nas suas demais contratações com terceiros, conforme se verá a seguir.

4.3.2 Sigilo bancário de proteção de dados – Lei Complementar nº 105/2001

Conforme demonstrado ao longo do trabalho, o mercado financeiro está aos poucos fazendo as adaptações necessárias para viabilizar o funcionamento do seu ecossistema digital, por meio das adequações exigidas com outras regulamentações como, por exemplo, a resolução 4.658/2018 sobre política de segurança cibernética, que foi atualizada com a resolução 4.752/2019, a circular 4.015/2020 sobre Open Banking, e a própria LGPD. Antes mesmo da resolução do Open Banking, a legislação brasileira já dispunha de previsões de portabilidade de informações entre instituições financeiras, estabelecidas na Lei do Sigilo Bancário, que em seu Art. 1º, § 3º, I e V determina que "não constitui violação ao dever de sigilo a troca de informações entre instituições financeiras, para fins cadastrais, inclusive por intermédio de centrais de risco, e a revelação de informações sigilosas, somente com o consentimento expresso dos interessados".

Pois bem, além da LGPD, que se aplica a todos os setores da economia, há, porém, no setor financeiro brasileiro, a LCP 105/2001 (Lei do Sigilo Bancário), que estabelece uma série de regras sobre o dever de sigilo das instituições financeiras (listadas em seu art. 1º, §§ 1º e 2º),[449] em relação às suas operações ativas e

---

[448] MORIBE, Gabriela Tiemi; SILVA, Gustavo Henrique Luz. **O que ainda não te contaram sobre a "nova" Lei do Cadastro Positivo?** Disponível em: < https://baptistaluz.com.br/wp-content/uploads/2020/01/lei_cadastro_positivo_VF.pdf>. Acesso em: 19 out. 2020.

[449] Art. 1º As instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados.
§ 1º São consideradas instituições financeiras, para os efeitos desta Lei Complementar:
I – Os bancos de qualquer espécie;
II – Distribuidoras de valores mobiliários;
III – Corretoras de câmbio e de valores mobiliários;
IV – Sociedades de crédito, financiamento e investimentos;
V – Sociedades de crédito imobiliário;
VI – Administradoras de cartões de crédito;

passivas e aos serviços prestados por estas. Tais informações incluem dados pessoais dos clientes, como nome, endereço, número de inscrição no Cadastro de Pessoas Físicas do Ministério da Fazenda (CPF/MF), saldo em conta corrente, histórico de movimentação financeira, contratação de produtos e serviços financeiros, entre outros, que conforme a LCP 105, devem ser mantidas em sigilo.

Assim, o artigo 1º da lei Complementar nº 105/01 manteve, genericamente, a obrigação de manter sigilo, explicitando no parágrafo 3º[450] as exceções ao dever de sigilo e no 4º[451] os casos autorizados de quebra.[452]

VII – Sociedades de arrendamento mercantil;
VIII – Administradoras de mercado de balcão organizado;
IX – Cooperativas de crédito;
X – Associações de poupança e empréstimo;
XI – Bolsas de valores e de mercadorias e futuros;
XII – Entidades de liquidação e compensação;
XIII – Outras sociedades que, em razão da natureza de suas operações, assim venham a ser consideradas pelo Conselho Monetário Nacional.
§ 2º As empresas de fomento comercial ou *factoring*, para os efeitos desta Lei Complementar, obedecerão às normas aplicáveis às instituições financeiras previstas no § 1º.

[450] Art. 1º, §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 das instituições responsáveis pela retenção e pelo recolhimento da contribuição prestarão à Secretaria da Receita Federal as informações necessárias à identificação dos contribuintes e os valores globais das respectivas operações, nos termos, nas condições e nos prazos que vierem a ser estabelecidos pelo Ministro de Estado da Fazenda.
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.

[451] Art. 1º, § 4º: a quebra de sigilo poderá ser decretada, quando necessária para apuração de ocorrência de qualquer ilícito, em qualquer fase do inquérito ou do processo judicial, e especialmente nos seguintes crimes:
I – de terrorismo;
II – de tráfico ilícito de substâncias entorpecentes ou drogas afins;
III – de contrabando ou tráfico de armas, munições ou material destinado à sua produção;
IV – de extorsão mediante sequestro;
V – contra o sistema financeiro nacional;
VI – contra a Administração Pública;
VII – contra a ordem tributária e a previdência social;
VIII – lavagem de dinheiro ou ocultação de bens, direitos e valores;
IX – praticado por organização criminosa.

[452] SARAIVA FILHO, Oswaldo Othon de Pontes; GUIMARÃES, Vasco Branco. **Sigilos bancário e fiscal:** homenagem ao Jurista José Carlos Moreira Alves. 2. ed. revista e ampliada. Belo Horizonte: Fórum, 2015, p.95.

Como já mencionado, a LC 105/2001 estabelece que as instituições financeiras devem conservar sigilo em suas operações (ativas e passivas)[453] e serviços prestados, e também, estabelece algumas exceções a essa regra de sigilo, por meio da qual informações financeiras poderiam ser compartilhadas com terceiros com o consentimento do interessado, ou com outras instituições financeiras em certas circunstâncias. Porém, para que o compartilhamento de dados pessoais no âmbito do sistema aberto de dados (*Open Banking*) não implique em violação do sigilo bancário, foi determinado que o compartilhamento de dados de transações financeiras no *Open banking* somente poderá ocorrer com o consentimento qualificado do titular dos dados, conforme visto anteriormente.

Apesar do rigor técnico apontado, observa-se que a expressão "sigilo bancário" foi incorporada pela história através dos usos e costumes. Por essa razão, o seu uso não será afastado, sendo aqui tratado como sinônimo de sigilo financeiro até para fins didáticos. Denota-se que a definição de sigilo bancário é influenciada pela distinção existente entre dever e obrigação. O sigilo bancário, portanto, pode ser conceituado como o dever jurídico que têm as instituições financeiras de não revelar, salvo justa causa, as informações que venham a obter em virtude de sua atividade profissional.[454]

É importante observar que o mandamento constitucional que declara inviolável o sigilo de dados (art. 5º, XII) leva a que se indague se alcança também as informações protegidas pelo sigilo bancário. Colocando de outro modo: se o fundamento jurídico do sigilo bancário pode ser buscado na Constituição Federal, em que dispositivo estaria ele contido? No inc. X do art. 5º – garantia da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas – ou no inc. XII do mesmo artigo – inviolabilidade "da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas"? A teoria do fundamento constitucional do sigilo bancário, tal como formulada em outros países, centra-se na proteção à intimidade e à vida privada. Proteção esta, no caso brasileiro, assegurada pelo inc. X do art. 5º da CF. O que bem esclarece, os tribunais brasileiros, em especial o STF, que têm baseado suas decisões sobre o

---

[453] Como tais operações são documentadas e, hoje, armazenadas em bancos de dados, haveria espaço para subsumir o sigilo bancário ao sigilo de dados de que fala a constituição no seu artigo 5º, inciso XII.

[454] FURLAN, Fabiano Ferreira. **Sigilo bancário.** Prefácio Carlos Alberto Rohrmann. Belo Horizonte: Fórum, 2008, p.19-22.

sigilo bancário principalmente naquele inc. X do rol de direitos e garantias constitucionais, como resulta claro da maioria dos acórdãos encontrados.[455]

Outro ponto, interessante, é que aliado à acepção de direito fundamental, o sigilo bancário ainda é visto como um verdadeiro direito da personalidade. Denota-se, assim, que o sigilo bancário pode incorporar as seguintes características: (a) oponibilidade *erga omnes*; (b) generalidade; (c) extrapatrimonialidade; (d) indisponibilidade; (e) intransmissibilidade; (f) irrenunciabilidade; (g) imprescritibilidade; (h) impenhorabilidade; (i) vitaliciedade; (j) inatos.[456]

Assim, no Brasil o sigilo bancário assumiu a conotação de direito fundamental do ser humano, sendo tratado como inerente ao direito à privacidade e à personalidade, nos termos do estabelecido pela jurisprudência dos Tribunais e pela doutrina, conforme já assinalado.[457]

Antes de seguir adiante, vale ressaltar que, em dezembro de 2019, o STF. Plenário. RE 1055941/SP, Rel. Min. Dias Toffoli, reafirmou o seu entendimento sobre a constitucionalidade do compartilhamento de dados bancários com a Receita Federal e com o Ministério Público para fins penais, independentemente de autorização prévia em processo judicial, e fixou as seguintes teses no Tema nº 990 da Repercussão Geral, Info 962, afirmando que: (i) É constitucional o compartilhamento dos relatórios de inteligência financeira da UIF[458] e da íntegra do

---

[455] HAGSTRÖM, Carlos Alberto. **Comentários à lei do sigilo bancário:** Lei Complementar nº105, de 10 de janeiro de 2001. Porto Alegre: Sergio Antônio Fabris Ed., 2009, p. 182-183.

[456] FURLAN, Fabiano Ferreira. **Sigilo bancário.** Prefácio Carlos Alberto Rohrmann. Belo Horizonte: Fórum, 2008, p.52-54.

[457] FURLAN, Fabiano Ferreira. **Sigilo bancário.** Prefácio Carlos Alberto Rohrmann. Belo Horizonte: Fórum, 2008, p.269.

[458] Unidade de Inteligência Financeira (UIF) é um órgão vinculado administrativamente ao Banco Central, mas com autonomia técnica e operacional, sendo responsável por produzir e gerir informações de inteligência financeira que sirvam para prevenir e combater crimes como lavagem de dinheiro, financiamento de terrorismo, financiamento da proliferação de armas de destruição em massa etc.; sendo também responsável por estabelecer uma interlocução institucional com órgãos e entidades nacionais, estrangeiros e internacionais que tenham conexão com a matéria. Assim, a Unidade de Inteligência é um grande banco de dados que recebe informações dos bancos, das seguradoras, dos cartórios de registro de imóveis, de joalherias. Em seguida, cruza dados e produz relatórios que poderão ser encaminhados à Receita Federal e aos órgãos de persecução penal em caso de indícios de ilícitos tributários ou de infrações penais. A UIF faz atualmente as mesmas funções que eram desempenhadas pelo Conselho de Controle de Atividades Financeiras (COAF). A MP 893/2019 transformou o COAF na Unidade de Inteligência Financeira. Vale ressaltar que a UIF não checa a veracidade das informações nem abre investigações. A UIF não pode quebrar o sigilo bancário e fiscal por conta própria. Pode trabalhar a informação, produzir relatório, identificar a irregularidade e mandar para os demais órgãos, como a Receita e o Parquet. A partir disso, a UIF analisa a comunicação recebida com o objetivo de identificar se existe nela algum indício de lavagem de dinheiro, de financiamento do terrorismo ou de outros crimes. Caso seja identificado algum indício de crime, é elaborado um Relatório de Inteligência Financeira (RIF), com natureza jurídica equivalente à de “peças de informação”, que é encaminhado às autoridades competentes (Receita

procedimento fiscalizatório da Receita Federal do Brasil (RFB), que define o lançamento do tributo, com os órgãos de persecução penal para fins criminais, sem a obrigatoriedade de prévia autorização judicial, devendo ser resguardado o sigilo das informações em procedimentos formalmente instaurados e sujeitos a posterior controle jurisdicional; (ii) O compartilhamento pela UIF e pela RFB, referente ao item anterior, deve ser feito unicamente por meio de comunicações formais, com garantia de sigilo, certificação do destinatário e estabelecimento de instrumentos efetivos de apuração e correção de eventuais desvios.[459]

Para melhor compreensão, faz-se necessário demonstrar o (quadro 5) com os órgãos que podem requisitar informações bancárias diretamente, sem autorização judicial:

Quadro 5 – Órgãos autorizados a requerer informações bancárias diretamente, sem a autorização judicial

SIGILO BANCÁRIO **Os órgãos poderão requerer informações bancárias diretamente das instituições financeiras, sem autorização judicial**	
POLÍCIA	NÃO. É necessária autorização judicial.
MP	NÃO. É necessária autorização judicial (STJ HC 160.646/SP, Dje 19/09/2011). **Exceção:** É lícita a requisição pelo Ministério Público de informações bancárias de contas de titularidade de órgãos e entidades públicas, com o fim de proteger o patrimônio público, não se podendo falar em quebra ilegal de sigilo bancário (STJ. 5ª Turma. HC 308.493-CE, j. em 20/10/2015).
TCU	NÃO. É necessária autorização judicial (STF MS 22934/DF, DJe de 9/5/2012). **Exceção:** O envio de informações ao TCU relativas a operações de crédito originárias de recursos públicos não é coberto pelo sigilo bancário (STF. MS 33340/DF, j. em 26/5/2015).
Receita Federal	SIM, com base no art. 6º da LC 105/2001. O repasse das informações dos bancos para o Fisco não pode ser definido como sendo "quebra de sigilo bancário".
Fisco estadual, distrital, municipal	SIM, desde que regulamentem, no âmbito de suas esferas de competência, o art. 6º da LC 105/2001, de forma análoga ao Decreto Federal 3.724/2001.
CPI	SIM (seja ela federal ou estadual/distrital) (art. 4º, § 1º da LC 105/2001).

Federal, Polícia Federal, Ministério Público Federal). Ademais, não raras vezes a atuação da Receita começa com informações dadas pela UIF.

[459] É possível o compartilhamento, sem autorização judicial, dos relatórios de inteligência financeira da UIF e do procedimento fiscalizatório da Receita Federal com a Polícia e o Ministério Público. **Dizer o Direito.** Disponível em: < https://www.dizerodireito.com.br/2019/12/e-possivel-o-compartilhamento-sem.html>. Acesso em: 19 out. 2020.

	Prevalece que CPI municipal não pode.

Fonte: Dizer o Direito[460]

O que se vê é que a Lei do Sigilo Bancário, em seu artigo 1º, parágrafo 3º, inciso I, como já referido anteriormente, determina que a troca de informações entre instituições financeiras não constituirá violação do dever de sigilo quando efetuada para fins cadastrais – não há previsão específica de outras destinações ou de compartilhamento entre outros tipos de prestadores de serviços.[461]

Cumpre destacar, também, que os dados pessoais coletados e armazenados devem ser mantidos em sigilo, de modo a preservar a privacidade do indivíduo. Não obstante, em adição às regras de segurança impostas pela LGPD e a LC 105/2001, existem normas referentes à preservação e ao tratamento de dados às quais as instituições financeiras e demais entidades autorizadas a operar pelo BACEN estão sujeitas, dentre as quais destacamos, a título de exemplo, as seguintes:

> - Resolução do CMN nº 2.554, de 24/09/1998, conforme alterada, que exige que as instituições financeiras, bem como outras instituições autorizadas pelo BACEN, criem e implementem controles internos relativos: (i) às atividades que desempenham; (ii) aos seus sistemas de informação financeira, operacional e de gestão; e (iii) ao cumprimento de leis e regulamentos a que estão sujeitas.
> - Resolução do CMN nº 4.480, de 25/04/2016, posteriormente revogada e atualizada pela resolução nº 4.753, de 26/09/2019, destinada a regulamentar a abertura e o encerramento de contas bancárias por meios eletrônicos e que dispõe de regras específicas de cibersegurança e proteção de dados.
> - Resolução do CMN nº 4.474, também de 2016, impõe regras especificas aos procedimentos e tecnologias utilizados na digitalização de documentos e na manutenção de documentos digitalizados por instituições financeiras. Essa resolução estabelece, por exemplo, que os documentos digitalizados e os *backups* de documentos digitalizados devem ser armazenados em um local seguro, permitindo acesso rápido para sua revisão e restauração. Além disso, documentos digitalizados e suas cópias de *backup* devem ser armazenadas no Brasil e em um local físico diferente do local de armazenamento do documento digitalizado. Os contratos para digitalização de documentos celebrados entre a instituição financeira e terceiros devem conter linguagem específica que autorize o acesso do BACEN aos contratos celebrados e à documentação e informações sobre os serviços prestados.
> - Resolução do CMN nº 4.658/2018 e a Circular nº 3.909/2018, que dispõem sobre a obrigatoriedade de implementação de uma política de segurança cibernética por parte das instituições financeiras e demais entidades autorizadas a operar pelo BACEN, bem como sobre requisitos para a contratação de serviços de processamento e armazenamento de dados e de comunicação em nuvem (*cloud computing*) pelas referidas

[460] A Receita pode requisitar das instituições financeiras, sem autorização judicial, informações bancárias sobre o contribuinte. Entenda a decisão do STF. **Dizer o Direito.** Disponível em: < https://www.dizerodireito.com.br/2016/02/a-receita-pode-requisitar-das.html>. Acesso em: 19 out. 2020.

[461] EROLES, Pedro. ***Fintechs*, Bancos Digitais e Meios de Pagamento:** aspectos regulatórios das novas tecnologias financeiras. São Paulo: Quartier Latin, 2019, p.44.

> instituições financeiras. Para tanto, a norma apresenta regras e diretrizes voltadas ao tratamento preventivo e reativo de incidentes de segurança, exigências mínimas para a contratação de serviços que envolvam dados e atribuições de responsabilidade dentro da instituição financeira.[462]

É importante observar, ainda, que a Lei do Sigilo exige confidencialidade das instituições financeiras. O quadro regulamentar é complementado por vários regulamentos fornecidos por reguladores, como o Banco Central do Brasil e a Autoridade de Valores Mobiliários. Segundo a Lei, apenas as seguintes situações não violam as obrigações de confidencialidade:

> - Intercâmbio de informações entre instituições financeiras para fins de base de dados;
> - Informações de inadimplentes de crédito exigidas pelas entidades de proteção de crédito;
> - Comunicação de atividades ilícitas a reguladores adequados (e.g. CVM, UIF);
> - Divulgação de informações com o consentimento expresso de todas as pessoas envolvidas e proprietários da informação;
> - A violação da confidencialidade também pode ser necessária como parte de uma investigação judicial, especialmente se for nos seguintes crimes: terrorismo; tráfico de drogas ou armas; extorsão por sequestro; contra o sistema financeiro nacional; contra a administração pública; contra o direito tributário e a segurança social; lavagem de dinheiro; praticado por organizações criminosas.[463]

Curioso observar que a confidencialidade dependerá de um conjunto de elementos a serem considerados igualitariamente e não pode ser um trunfo do autor da comunicação para esconder a prática de ilícitos, manietando o destinatário de qualquer possiblidade de reação. Por outro lado, admitindo-se a sua natureza confidencial, uma divulgação indevida implicará a possibilidade de reparação de eventuais danos patrimoniais e a compensação de danos morais, além das medidas judiciais pertinentes para fazer cessar ameaça ou lesão de direitos.[464]

Ainda assim, o cumprimento do sigilo bancário e a conformidade com a proteção de dados permitem o intercâmbio de dados privados, se forem solicitados por entidades públicas específicas associadas ao setor financeiro ou para suporte de investigação legal. Por certo, a regra geral é que os dados financeiros devem ser mantidos em sigilo.

---

[462] PALHARES, Felipe. et al. **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020, p.138-139.

[463] MONTEIRO, Renato Leite. et al. **Proteção de Dados no Setor Financeiro.** Disponível em: < http://baptistaluz.com.br/wp-content/uploads/2017/12/Brazil-Data-Protection-in-the-Financial-Sector_2017_PORT.pdf>. Acesso em: 19 out. 2020.

[464] FRAZÃO, Ana; TEPENDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** 2.ed. São Paulo: Thomson Reuters Brasil, 2020, p.170.

Note-se ainda que a violação do dever de sigilo constitui ilícito penal sujeitando os responsáveis à pena de reclusão de um a quatro anos e multa. Além disso, tal conduta tem reflexos nas esferas cível e administrativa, sujeitando seus responsáveis a eventual pagamento de indenização para o prejudicado e imposição de penalidades administrativas.

A título de exemplo, em março de 2020, o Instituto Sigilo ajuizou uma ação civil pública com pedido de indenização por perdas e danos morais e materiais contra o Nubank, alegando que o banco estaria acessando dados pessoais de brasileiros por meio de entidades financeiras e comerciais, sem o consentimento expresso dos titulares de dados, para fins publicitários.[465]

Portanto, o sigilo em relação aos dados financeiros deve ser sempre garantido a todos os indivíduos nos moldes determinados pela Constituição Federal e pelas leis infraconstitucionais. A coleta e a utilização de dados financeiros devem ser informadas aos titulares dos dados e estarem baseadas em uma ou mais bases legais de tratamento, sendo que qualquer alteração de finalidade ou destinação desses dados deve ser obrigatoriamente informado ao indivíduo titular dos dados.

---

[465] PALHARES, Felipe. et al. **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020, p.386.

5 DISCUSSÃO

Como já mencionado, a Lei do Sigilo Bancário trata do sigilo como regra geral nas atividades bancárias, em virtude da natureza jurídica dos dados e em respeito à privacidade da vida financeira das pessoas.

Já a Lei Geral de Proteção de Dados objetiva proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

As relações entre à privacidade e o direito ao sigilo têm ocupado posição destacada nos recentes debates jurídicos.

No Brasil, há a peculiaridade desses direitos possuírem *status* constitucionais, dotados de jusfundamentalidade. Assim, vê-se que a proteção dos dados pessoais, como elemento do direito à privacidade, encontra-se assegurada no artigo 5º, inciso X, da Constituição. Nesse sentido, inclusive, tem-se a Proposta de Emenda Constitucional (PEC 17/2019), que expressamente dispõe do direito à proteção de dados pessoais como de direitos fundamentais.[466] Igualmente, o direito de sigilo bancário recebe respaldo no artigo 5º, X, da Carta Fundamental.

Assim, na sequência, uma breve análise dos principais pontos acerca da proteção de dados pessoais, sob a ótica da Lei do Sigilo Bancário, em relação a Lei Geral de Proteção de Dados, conforme destaca Oscar Valente Cardoso[467], de forma exemplificativa, os seguintes:

i. Dever de sigilo (art. 1º, caput, da Lei do Sigilo Bancário): deriva diretamente do direito à privacidade previsto na Constituição, e que é tratado como regra nas atividades das instituições financeiras, com base na natureza jurídica dos dados dos clientes. Assim, a lei inicia com o principal dever imposto a suas destinatárias, de manutenção do sigilo em todas as operações ativas e passivas e nos serviços prestados. Além disso, o § 3º do art. 1º da Lei do Sigilo Bancário descreve as atividades que podem ser realizadas sem a violação do dever de sigilo (que serão analisadas na sequência), enquanto o seu § 4º prevê as hipóteses de quebra do sigilo. Logo, há novamente uma

---

[466] FRAZÃO, Ana; TEPENDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** 2.ed. São Paulo: Thomson Reuters Brasil, 2020, p.196.

[467] CARDOSO, Oscar Valente. Lei Geral de Proteção de Dados e o diálogo das fontes: a vez da Lei do Sigilo Bancário. **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 25, n. 6259, 20 ago. 2020. Disponível em: < https://jus.com.br/artigos/84714/lei-geral-de-protecao-de-dados-e-dialogo-das-fontes-4-lei-do-sigilo-bancario >. Acesso em: 15 out. 2020.

preocupação legislativa anterior com a proteção e o sigilo dos dados pessoais, em decorrência da tutela da vida privada, o que se repete na Lei Geral de Proteção de Dados, que tem entre os seus fundamentos a inviolabilidade da intimidade, da honra e da imagem (art. 2º, IV, da LGPD) e os direitos do titular têm sua base principal nos direitos fundamentais de liberdade, de intimidade e de privacidade (arts. 1º e 17 da LGPD);

ii. Compartilhamento de dados cadastrais entre instituições financeiras e centrais de risco (art. 1º, § 3º, I, da Lei do Sigilo Bancário): conforme a primeira hipótese de ausência de violação de sigilo, as instituições financeiras podem trocar informações entre si, o que compreende, inclusive, o compartilhamento de dados para verificar a veracidade e a autenticidade dos dados cadastrais (e, entre outros objetivos, evitar fraudes de cadastros e documentos), além de comunicarem mutuamente a ocorrência de eventuais riscos nas contratações (de inadimplência, fraude ou por outras razões). Esse compartilhamento deve observar, especialmente, os princípios da finalidade e da necessidade (art. 6º, I e III, da LGPD), razão pela qual os dados compartilhados devem ser apenas os necessários para o objetivo pretendido e devem ser utilizados para a finalidade específica pretendida com o compartilhamento. Acrescenta-se que o titular tem o direito de obter informações sobre o compartilhamento de seus dados e da sua finalidade (art. 9º, V, da LGPD);

iii. Fornecimento de informações em cadastros de emitentes de cheques sem provisão de fundos e de inadimplentes a entidades de proteção de crédito (art. 1º, § 3º, II, da Lei do Sigilo Bancário): na segunda hipótese de ausência de violação de sigilo, as instituições financeiras não precisam consultar previamente o devedor sobre a comunicação do fato (dívidas vencidas e cheques sem provisão de fundos) aos órgãos de proteção de crédito. Contudo, ele deve ser notificado previamente da inscrição, o que lhe dá, por exemplo, o direito de acesso e de correção de dados eventualmente incorretos (art. 18, II e III, da LGPD). Ainda, tal fornecimento e tratamento dos dados enquadra-se na hipótese de proteção do crédito prevista no art. 7º, X, da LGPD, e o titular tem o direito de obter informações sobre o compartilhamento dos dados e da sua finalidade (art. 9º, V, da LGPD);

iv. Fornecimento de informações acerca de contribuições tributárias recolhidas que incidirem sobre operações bancárias e financeiras (art. 1º, § 3º, III, da Lei do Sigilo Bancário): a terceira hipótese de ausência de violação de sigilo trata do fornecimento de dados que eram prestados pelas instituições financeiras à Receita Federal, sobre a retenção e o recolhimento da contribuição provisória sobre movimentação ou transmissão de valores e de créditos e direitos de natureza financeira, com a identificação dos contribuintes e suas operações (art. 11, § 2º, da Lei nº 9.311/96). Assim, o dispositivo permite que, nos tributos incidentes sobre operações financeiras, as instituições repassem à Receita Federal as informações (e os dados) relacionadas ao fato gerador, como os contribuintes e os valores globais das operações que levaram à incidência do tributo, entre outras. Esse tratamento dos dados pelas instituições financeiras e, de forma compartilhada, pela Receita Federal, enquadra-se na hipótese de cumprimento de dever legal prevista no art. 7º, II, da LGPD. Da mesma forma que nos dois casos anteriores, o titular tem o direito de obter informações sobre o compartilhamento de seus dados e da sua finalidade (art. 9º, V, da LGPD);

v. Comunicação da prática de ilícitos penais ou administrativos (art. 1º, § 3º, IV, da Lei do Sigilo Bancário): de acordo com a quarta hipótese de ausência de violação, o sigilo bancário não protege a prática de atos ilícitos, penais ou administrativos, o que compreende também as operações posteriormente realizadas com os recursos oriundos das práticas criminosas (ou seja, a lavagem de dinheiro);

vi. Fornecimento consentido de dados pelos interessados (art. 1º, § 3º, V, da Lei do Sigilo Bancário): na quinta hipótese de ausência de violação de sigilo, em acréscimo às anteriores, a Lei do Sigilo Bancário já prevê a possibilidade do consentimento do titular como um requisito para o tratamento dos dados, ou seja, é lícita a revelação dos dados bancários com o consentimento expresso do titular. Na Lei Geral de Proteção de Dados, o consentimento deve ser livre, expresso (manifestação positiva da vontade do titular), inequívoco, por escrito, revogável (revogabilidade do consentimento), de finalidade específica e limitada (art. 5º, II, da LGPD);

vii. Prestação de informações no cumprimento de dever legal (art. 1º, § 3º, VI, da Lei do Sigilo Bancário): a sexta hipótese de ausência de violação de sigilo é a

mais ampla e prevê que devem ser fornecidas informações pelas instituições financeiras nos termos e condições dos casos previstos nos arts. 2º a 7º e 9º da lei, que compreendem, por exemplo, o acesso aos dados pelo Banco Central do Brasil no desempenho de suas funções de fiscalização, o envio de dados bancários para cumprimento de decisão judicial ou para a instrução de processo administrativo fiscal, entre outras. Do mesmo modo que em casos anteriores, o titular tem o direito de obter informações sobre o compartilhamento de seus dados e da sua finalidade (art. 9º, V, da LGPD);

viii. Dados de pagamentos e operações de créditos (em cumprimento ou adimplidas), para cadastros positivos de crédito (art. 1º, § 3º, VII, da Lei do Sigilo Bancário): por fim, conforme a sétima hipótese de ausência de violação de sigilo, os dados podem ser compartilhados não apenas para os bancos de dados de cadastros de inadimplentes (como visto no art. 1º, § 3º, II), mas também para a apuração de nota ou o cálculo de pontuação em cadastros positivos de crédito, ou seja, em benefício do titular dos dados. Conforme visto no compartilhamento de dados para os cadastros de inadimplentes, nos cadastros positivos o titular também tem o direito de obter informações sobre o compartilhamento dos dados e da sua finalidade (art. 9º, V, da LGPD) e de correção de dados eventualmente incorretos (art. 18, II e III, da LGPD).

A Lei do Sigilo bancário, como se vê, guarda similitudes com a Lei Geral de proteção de Dados. Nessa perspectiva, mister destacar, ainda, o memorando elaborado pelos escritórios Pinheiro Neto Advogados e Mattos Filho a pedido da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (ANBIMA), que tem por objetivo analisar determinados aspectos relacionados à Lei Geral de Proteção de Dados (“LGPD”) e à Lei Complementar 105, de 10 de janeiro de 2001 (“Lei de Sigilo Bancário” ou “LC 105/01”), vis-à-vis as regras de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (“PLDFT”), consoante se verifica em anexo. Ao passo que ambas as normas possuem diversos fundamentos e matrizes sobre as quais se estruturam, além de possíveis semelhanças quanto as atividades que podem ser realizadas sem a violação do dever de sigilo. Daí porque se impõe mister hermenêutico que assegure a correta compreensão de quais são os dados pessoais passíveis de sigilo. Contudo, se faz necessário, a superação de uma interpretação tradicional em direção à harmonização de ambos os direitos, trazida

pelas leis em comento, em diversos momentos, e que está apta a justificar o acesso de terceiros a dados pessoais de clientes.

Nesta direção e baseado na revisão realizada, bem como no estudo da Lei Geral de Proteção de Dados (Lei n° 13.709/2018) e da Lei de Sigilo Bancário (LCP 105/2001) se apresenta uma minuta de Contrato de Termo de Uso e de Política de Privacidade[468] ideal para *fintechs* de serviços financeiros (bancos digitais). Nesse sentido, por se tratar de instrumentos com funções autônomas, o conteúdo das cláusulas deve ser tratado separadamente. A vista disso, será apresentado alguns aspectos contratuais de ambos os instrumentos, demonstrando caso a caso, de acordo com as necessidades específicas e os direitos e obrigações em conformidade com a LGPD, conforme se verá a seguir.

[468] O "Termo de Uso ou Termo de Aceite ou Termo de Serviço, ou Termo de Acesso ou Termo e Condições" diz respeito às regras combinadas com o usuário para utilização do produto ou serviço oferecido, seja para limitar certas aplicações, seja para impor deveres e alertar sobre direitos. Outra questão relevante consiste no fato de que o termo de uso deve ser levado ao registro público. Além disso, o Termo de Uso não permite ao Usuário discutir suas cláusulas, decorrendo daí o seu caráter adesivo. A "Política de Privacidade ou Diretiva de Privacidade" diz respeito ao direito à privacidade. É preciso esclarecer ao usuário sobre o que será feito com os dados que serão coletados e qual o nível de segurança e privacidade oferecidos. Muito embora os termos de uso e política de privacidade sejam desconsiderados pelo usuário que assina sem jamais prestar atenção no texto, é importante fazer o esclarecimento para evitar problemas no futuro. Alguns mecanismos, já à disposição no mercado, podem ajudar a conscientizar o usuário da importância da leitura e compreensão do termos, como, por exemplo: (i) exigir que o usuário faça a rolagem de todo o texto para fazer a assinatura ao final; (ii) exigir cadastro do usuário prévio e envio do termo de uso para o *e-mail* fornecido como condição para ter acesso ao produto; (iii) exigir o clique no botão que declare expressa concordância com os termos de uso e política de privacidade e (iv) apresentar um texto com letras grandes o suficiente para chamar a atenção e destaque para as cláusulas que limitam o exercício de certos direitos ou restringem o uso por parte do usuário. Por fim, tais instrumentos se amoldam à regra da atipicidade contratual porque não têm previsão em lei e depende do pacto estabelecido pelas partes que devem decidir o direito, as obrigações e as responsabilidades que serão inseridos no contrato atípico, também denominado contrato inominado pela doutrina. Em tese, trata-se de um poder legítimo conferido aos particulares para autorregular seus interesses e negócios, onde a prestação é uma conduta humana, uma ação ou omissão das partes, dar, fazer ou não fazer. Portanto, o "Termo de Uso" e a "Política de Privacidade" são contratos eletrônicos que visam limitar a responsabilidade, direcionar a forma de utilização do seu produto por parte dos usuários, assim como esclarecer possíveis dúvidas que seu cliente tenha sobre o funcionamento do seu *software*/produto.

CONTRATO DE TERMO DE USO		
ITEM	**CLÁUSULA**	**JUSTIFICATIVA**
1	**Aceite ao Termo**	Alertar ao usuário (titular dos dados), que, ao utilizar o serviço, concorda expressamente com os termos e serviços apresentados. Ou seja, ao utilizar o serviço, o usuário confirma que leu e compreendeu os Termos aplicáveis a ele e concorda (consenti) em ficar vinculado aos mesmos. As transações realizadas serão por ele aceitas e consideradas válidas como meio eficaz para comprovar a autoria, a autenticidade, a integridade e a confidencialidade. Segue a descrição do aceite da plataforma da instituição: **O USUÁRIO EXPRESSAMENTE RECONHECE QUE A ADESÃO AO PRESENTE TERMO SE COMPLETA MEDIANTE CLIQUE NO BOTÃO ("Aceitar") NA TELA DE CADASTRO DA INSTITUIÇÃO FINANCEIRA.** **Atenção:** o consentimento (art. 7º, I da LGPD) deverá ser manifestamente expresso, livre, específico, informado, inequívoco e explícito, isto é, como um instrumento adequado para o exercício do dever de informar. Deve ser fornecido por escrito ou por outro meio que evidencie a manifestação de vontade do titular (artigo 8º, *caput*, da LGPD). Sob essa ótica, se o consentimento for escrito, a lei delimita que este deverá constar de cláusula destacada das demais cláusulas contratuais (artigo 8º, §1º, da LGPD), de modo que será vedado o tratamento de dados pessoais mediante vício do consentimento (artigo 8º, §3º, da LGPD), cabendo, nesses casos, a responsabilização do controlador. Assim sendo, constata-se que o consentimento deverá se referir a finalidades determinadas, caso contrário, isto é, em caso de autorizações genéricas, recairá a nulidade ao tratamento realizado (artigo 8º, §4º, da LGPD). Ademais, é dispensada a exigência do consentimento para os dados tornados manifestamente públicos pelo titular (art. 7º, §3º, da LGPD). Por certo, essa cláusula, deve ser clara e transparente, informando o titular sobre o uso que será feito de seus dados, para qual finalidade e qual procedimento a instituição adotará (art. 6º, I e VI da LGPD).
2	**Definições**	Conceitos importantes, como termos técnicos ou legais (LGPD, art. 5º), precisam ser explicados de forma clara, objetiva e especifica, para melhor entendimento do usuário (titular), destaque deve ser dado às seguintes definições: V – Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; VI – Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; VII – Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; VIII – Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); IX – Agentes de tratamento: o controlador e o operador; e XIX – Autoridade Nacional de Proteção de Dados (ANPD): órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta lei em todo o território nacional.
3	**Arcabouço Legal**	Os dados pessoais são coletados e tratados pela instituição para o cumprimento de obrigações legais e regulatórias, para o exercício regular de direitos e para proteção do crédito. Dentre os instrumentos legais que têm relação direta com a utilização do serviço, que podem ser consultados pelo titular dos dados para esclarecimento de dúvidas relacionadas ao serviço financeiro prestado, estão: (a) Lei 13.709/2018 (Lei Geral de Proteção de Dados); (b) Lei 12.965/2014 (Lei de Acesso à Internet); (c) LCP 105/2001 (Lei de Sigilo Bancário); (d) Lei 12.414/2011 (Lei do Cadastro Positivo); (e) Decreto nº 7.724/2012); (f) Resolução do CMN nº 4.658/2018 atualizada pela

		resolução 4.752/2019 e a Circular nº 3.909/2018; (g) Resolução nº 4.737/19 e a Circular nº 3.955/19; (h) Circular 4.015/2020 e a Resolução Conjunta nº 01 (*Open Banking)*. **Atenção:** a instituição possui controles internos capazes de avaliar a compatibilidade entre as informações prestadas pelo usuário e as suas operações bancárias, nos termos das determinações constantes das mencionadas leis e demais normas e regulamentações aplicáveis editadas pelo Conselho Monetário Nacional e pelo Banco Central do Brasil (BACEN).
4	**Descrição do serviço**	É recomendável, aqui, informar ao usuário sobre a forma de acesso a esses serviços financeiros: requisitos, documentos, etapas do processo e prazos para a prestação do serviço. Deve ser informado também o que os titulares estão utilizando ou adquirindo, para evitar reclamações relacionadas ao serviço. Além dessas informações, o detalhamento sobre compromissos e padrões de qualidade na prestação do serviço, como: prioridades de atendimento, previsão do tempo de espera e mecanismos de consulta acerca do andamento do serviço solicitado e de eventuais manifestações, além, dos procedimentos para atendimento quando o sistema informatizado se encontrar indisponível, por exemplo, e quaisquer outras informações julgadas de interesse dos usuários. Resumidamente devem estar presentes as seguintes informações: (i) Quem é o responsável pela prestação do serviço; (ii) Descrição do escopo do serviço e sua finalidade; (iii) Forma de utilização do serviço e informações necessárias para o uso adequado do mesmo.
5	**Direitos do usuário**	O usuário (pessoa física), na condição de titular dos dados pessoais, tem direito a obter, em relação aos seus dados tratados pela instituição, a qualquer momento, informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial (art. 9º da LGPD), de maneira que o princípio da transparência e da boa-fé estejam presentes. Acrescido a isso, deverá ser esclarecido ao titular os meios pelos quais poderá exercer seus direitos, nos moldes do artigo 18 da LGPD, merecendo destaque alguns direitos inerentes à proteção de dados: (i) garantir que o titular possa assegurar que seus dados estão sendo tratados de forma segura, verídica e cumprindo a sua finalidade; (ii) a liberdade de revogar o consentimento e requerer o apagamento dos dados, como reflexo da liberdade de escolha, de forma que, assim como o consentimento, a revogação deve ser expressa a qualquer tempo (art. 8º, §5º), bem como a portabilidade de dados pessoais (LGPG, art. 18, inciso V). Particularmente com relação a portabilidade, trata-se de direito relevante diante do sistema bancário aberto (*Open Banking*), que tem como um de seus objetivos permitir a portabilidade de informações entre diversos *stakeholders* do mercado financeiro. Ainda assim, o consentimento das informações coletadas não deve ser utilizado em prejuízo do titular. Com efeito, a LGPD reiteradamente torna imperativo o consentimento, sobretudo ao se tratar de novas modificações (artigo 8º, §6º, da 13.709/2018), de modo é por completo irrazoável que as alterações do serviço se deem sem notificação do titular de dados.
6	**Responsabilidades**	Evidencia de forma clara quais são as responsabilidades de cada parte envolvida no serviço financeiro prestado (art. 9º, VI da LGPD), estabelecendo direitos e deveres para ambas as partes e compreendem suas obrigações ao utilizar e prover o serviço, de forma a esclarecer quais situações configuram violações ao Termo e para quais cabem reparação de danos. **A instituição de serviço financeiro (Controlador)** deve cumprir todas as legislações inerentes ao uso correto dos dados pessoais do usuário de forma a preservar a privacidade dos dados utilizados no serviço, bem como garantir todos os direitos, garantias legais e segurança para proteção desses dados evitando risco ou dano relevante aos titulares. Além disso, deve notificar o usuário, quanto às ordens judiciais de pedido das informações necessárias para investigações ou ameaças potenciais contra pessoas, bens ou sistemas que sustentam o serviço ou de outra forma necessária para cumprir com as obrigações legais, salvo quando o processo estiver em segredo de justiça. **É dever do usuário do serviço,** apresentar informações verdadeiras e se

		responsabilizar pelas possíveis consequências de erros e omissões; obedecer às regras estabelecidas no Termo; manter o sigilo da senha, que deve ser pessoal e intransferível; responsabilizar-se por possíveis aplicativos de terceiros que possam fazer o uso de dados pessoais em seus dispositivos; responsabilizar-se pela segurança do dispositivo pelo qual é realizado o acesso ao serviço; reparar danos diretos e indiretos que sejam causados à instituição e a terceiros pelo mal uso do serviço; dentre outros. **Atenção:** é importante esclarecer que o controlador ou operador que, em razão dos riscos de exercício da atividade de tratamento de dados pessoais, causar danos a outrem, em violação à LGPD, é obrigado a repará-lo, razão pela qual a excludente de responsabilidade não possui fundamento. Entretanto, trata-se de ônus dos agentes de tratamento a prova de que se encaixa em uma excludente de responsabilidade (artigo 43, incisos, da LGPD), com situações específicas que os eximem de responsabilidades: (i) quando, atribuídos a certo tratamento de dados, comprovarem que não realizaram tal tratamento; (ii) que, nas situações em que tenha realmente realizado o tratamento de dados que lhe é atribuído, não houve violação à legislação de proteção de dados; e, (iii) por fim, que o dado proporcionado pelo titular é decorrente de culpa exclusiva deste ou de um terceiro. Ademais, o legislador atribuiu uma seção própria para a responsabilidade e o ressarcimento dos danos, em seu artigo 42, § 1º e incisos. Verifica-se, assim, a solidariedade dos agentes. Em primeiro plano, o inciso I trata da possibilidade de ser exigido ao operador quando este descumprir a LGPD ou, ainda, quando não observar instruções legais do controlador. O inciso II, por outro lado, permite a responsabilidade solidária do controlador, quando diretamente envolvido no tratamento que gerou danos ao titular. Contudo, como a definição de tratamento de dados pessoais é extensa (artigo 5º, inciso X, da LGPD), isto é, apresenta uma pluralidade de atividades, tais como a coleta, modificação, transmissão, processamento e armazenamento, por vezes, é possível que exista mais de um controlador, que praticou uma dessas atividades separadamente. Além disso, o controlador não se responsabiliza por eventuais atrasos, falhas ou indisponibilidades da rede sem fio, da *internet* ou dos serviços prestados pela operadora de telefonia móvel, do usuário, que venham a prejudicar ou impedir a transmissão de informações. Por tudo dito, a LGPD, além de incentivar que o tratamento de dados seja um tratamento seguro, em conformidade com as suas disposições, protegendo os dados do titular em sua integralidade, além de garantir inviolabilidade da intimidade, da honra e da imagem (art. 2º, IV, da LGPD), também busca equilibrar as relações, em sua justa medida, a fim de que não haja excessos na responsabilidade dos agentes de tratamento, porque qualquer cláusula que implique em danos ao titular ou à sua privacidade será considerada como não escrita.
7	**Mudanças no Termo**	Informar aos usuários do serviço como será feita a modificação do Termo, para que eles estejam cientes, se haverá algum custo, ou se existe alguma forma de cancelar o serviço. Além disso, alertar como os usuários terão conhecimento do novo Termo. Logo, qualquer alteração futura (art. 9º, §2º, da LGPD), no Termo de uso (i) deve ser comunicada diretamente ao usuário, por *e-mail*, (ii) ao acessar o serviço; ou (iii) pode-se alertá-lo para que revisem os Termos com frequência, para que tenha conhecimento das novas regras. **Atenção:** caso o usuário não concorde com as alterações, ele poderá solicitar o cancelamento do serviço contratado com a instituição. O não cancelamento, após a publicação da alteração, será entendido como sua concordância.
8	**Informações para contato**	Em caso de eventuais dúvidas com relação ao Termo de Uso é importante que o controlador informe por qual canal essas dúvidas serão sanadas (telefone para contato, endereço de *e-mail*, *chats*, canal de atendimento), detalhando sobre o seu funcionamento, como horário de funcionamento, conforme o caso. O contato do responsável deve ser capaz de atender o estipulado pela LGPD com relação ao acesso à informação (art. 6º, IV, VI e o art. 9º da Lei) garantindo assim a transparência das informações e também a

		gratuidade da consulta a essas informações.
9	**Foro**	Essa cláusula visa o comprometimento das partes envolvidas na prestação do serviço financeiro prestado – usuário e instituição – a reclamar eventuais direitos em determinado órgão jurisdicional, caso uma delas entenda que questões presentes no Termo de Uso do serviço tenham sido violadas. Deve-se informar também que o titular de dados (usuário) tem direito de apresentar reclamação à Autoridade Nacional de Proteção de Dados caso entenda que alguma questão presente no Termo de Uso tenha sido violada (art. 18, § 1º da LGPD).

POLÍTICA DE PRIVACIDADE		
ITEM	**CLÁUSULA**	**JUSTIFICATIVA**
1	**Identificação dos Agentes de tratamento e do Encarregado**	Esta cláusula consiste em identificar os agentes de tratamento (controlador e operador) e o encarregado (DPO), de acordo com o art. 5º, VI, VII e VIII da LGPD. Esses atores desempenham papel essencial no levantamento das informações necessárias para elaboração de uma Política de Privacidade adequada a instituição de serviço financeiro. Dessa forma, LGPD estabelece, em seu Art. 41, que o controlador deverá indicar um encarregado pelo tratamento de dados e divulgar publicamente a identidade e as informações de contato do mesmo (§ 1º), já que ele é o canal de comunicação entre o controlador, o titular dos dados e a ANPD. Ademais, o inciso III e VI do Art. 9º da Lei, prevê de forma clara às informações de contato do controlador, bem como a necessidade de disponibilizar informações sobre as responsabilidades dos agentes que realizarão o tratamento, e como o operador é um desses agentes, é importante que ele forneça, também, as suas informações. A conclusão desta etapa é o Art. 6º, VI, o princípio da transparência que assegura a garantia aos titulares do fornecimento de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento.
2	**Tratamento dos Dados**	Com o objetivo de facilitar o acesso ao titular dos dados, todos os dados pessoais tratados pelo serviço financeiro prestado devem ser especificados nesta cláusula. Esse tratamento (LGPD, art. 5º, inciso X) deve respeitar os princípios estabelecidos no artigo 6º da LGPD, especialmente o princípio da necessidade (inciso III), que estabelece a limitação do tratamento ao mínimo necessário para a realização das finalidades previstas, de forma proporcional e não excessiva. Além disso, o princípio da responsabilização e prestação de contas (inciso X) requer que a instituição que realiza o tratamento de dados pessoais possa demonstrar que está plenamente aderente à LGPD, comprovando a observância e o cumprimento das normas de proteção de dados pessoais estabelecidas, inclusive quanto a sua eficácia. Esse tratamento poderá ser realizado desde que enquadrado em uma das hipóteses elencadas em seu art. 7º. Tais hipóteses podem ser compreendidas como condições necessárias para verificar se o tratamento de dados a ser realizado pelo controlador ou operador é permitido, e que no caso, merece destaque a hipótese de tratamento mediante consentimento do titular (LGPD, art. 7º, inciso I): hipótese em que o titular tem chance real de escolha sobre o tratamento de seus dados. É trazido por muitos como a hipótese principal para o tratamento dos dados e tem certa preferência sobre as demais. Ressalta-se algumas perguntas, que devem ser respondidas positivamente para que a hipótese de tratamento do dado por consentimento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD: (i) É viável a coleta e o armazenamento da opção de consentimento do usuário de modo a poder comprovar posteriormente a sua expressa manifestação de vontade? (ii) Se o consentimento se der de forma escrita, será garantido que a opção pelo consentimento conste de cláusula

		destacada das demais, em que o titular seja instado a escolher livremente pela anuência ou não ao consentimento solicitado? (iii) O consentimento será solicitado para cada uma das finalidades de tratamento, e será informado ao titular que tipo de tratamento será realizado, antes que este opte pelo consentimento? **Atenção: (**a) É vedado o tratamento de dados pessoais mediante vício de consentimento (LGPD, art. 8º, § 3º); (b) O consentimento será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca (LGPD, art. 9º, § 1º); (c) Se houver mudanças de finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o titular deverá ser informado previamente sobre tais mudanças, podendo revogar o consentimento, caso discorde das alterações (LGPD, art. 9º, § 2º); (d) As autorizações genéricas para o tratamento de dados pessoais serão consideradas nulas (LGPD, art. 8º, § 4º); (e) Será dada ao titular a opção de revogação do consentimento, a qualquer momento, mediante manifestação expressa, por procedimento gratuito e facilitado (LGPD, art. 8º, § 5º); (f) No caso de tratamento de dados de crianças e adolescentes, será solicitado o consentimento específico por pelo menos um dos pais ou pelo responsável legal (LGPD, art. 14, § 1º); (g) O art. 11 da LGPD elenca as hipóteses em que o tratamento de dados pessoais sensíveis pode ser realizado. Novamente, a lei traz a possibilidade de tratamento mediante consentimento do titular, como regra, e enumera as hipóteses que dispensa o consentimento, por meio de rol extensivo.
3	**Coleta dos Dados**	A coleta de dados pessoais implica um dever de cuidar da proteção dos dados do usuário e sua privacidade. Além de especificar quais dados são coletados, o importante, aqui, é avaliar caso a caso, uma vez que o titular deverá conhecer a hipótese legal que autoriza o processamento de seus dados pessoais. Dessa forma, para cada dado pessoal utilizado no serviço financeiro prestado, deve-se informar ao titular do dado como ele foi coletado e de que forma. Prever se as informações coletadas serão disponibilizadas a terceiros e como serão disponibilizadas e armazenadas. Deve-se respeitar o princípio da necessidade (LGPD, art. 6º, inciso III), bem como os riscos de segurança associados as funcionalidades dos dispositivos necessárias para obtenção dos dados pessoais. Tendo em vista que a coleta (art. 5º, inciso X da LGDP) representa a operação inicial de tratamento, responsável por obter os dados pessoais do usuário (titular dos dados), a realização de tal operação pela instituição somente deve ser realizada mediante o atendimento das hipóteses de tratamento (LGPD, art. 7º e 11), das medidas de segurança (LGPD, art. 46), dos princípios (LGPD, art. 6º), dos diretos do titular (LGPD, art. 17 a 22) e demais regras dispostas pela LGPD, de forma a assegurar a privacidade do titular dos dados.
4	**Finalidade do Tratamento**	Além de informar quais os dados pessoais coletados e a forma como são coletados, a instituição deve informar ao usuário (titular dos dados) qual o tratamento realizado com os dados pessoais e qual a sua finalidade. É importantíssimo estabelecer claramente a finalidade, pois é ela que justifica o tratamento e fornece os elementos para informar o titular dos dados. Nesta cláusula, é importante detalhar o que se pretende alcançar com o tratamento dos dados pessoais, considerando os exemplos de finalidades, embasados nos artigos 7º e 11 da LGPD. Desse modo, deve-se informar e detalhar qualquer finalidade do controlador (instituição de serviço financeiro) para tratamento dos dados pessoais, inclusive, no caso de a finalidade ser para atender o legítimo interesse do mesmo (art. 10 da LGPD). Nesse sentido, a finalidade apontada pelo controlador para a realização do tratamento de dados deve ser pautada em fundamentações claras e legítimas, e somente os dados reais e estritamente necessários devem ser coletados com vistas à garantia do direito a proteção à privacidade do titular. Além disso, especial atenção deve ser dedicada ao tratamento de dados pessoais realizado com base exclusivamente no consentimento do titular. Nesse caso, é importante: (i) Indicar qual(is) o(s) resultado(s) pretendido(s) para os titulares dos dados

		pessoais, informando o quão importantes são esses resultados; (ii) Informar os benefícios esperados pela instituição. **Atenção:** o tratamento de dados pessoais para finalidades não previstas nesta Política de Privacidade somente ocorrerá mediante comunicação prévia ao usuário, sendo que, em qualquer caso, os direitos e obrigações aqui previstos permanecerão aplicáveis.
5	**Compartilhamento de dados**	Para estar em conformidade com a LGPD, o serviço financeiro prestado deverá informar ao usuário (titular do dado) que utiliza o serviço sobre o uso compartilhado de dados (LGPD, art. 5º, XVI) pelo controlador e a finalidade associada a esse compartilhamento, conforme previsto no artigo 9º, inciso V da LGPD. Resumidamente devem estar presentes as seguintes informações: (i) Quais dados são compartilhados; (ii) Com quem os dados são compartilhados; e (iii) Qual a finalidade (razão) do compartilhamento. **Atenção:** (i) qualquer compartilhamento de dados deve ser feito apenas quando necessário e dentro de rígidos padrões de segurança, sempre visando a confidencialidade das informações e seguindo as normas de sigilo bancário e de proteção à privacidade; (ii) a instituição também pode fornecer os dados do usuário, sempre que estiver obrigada, seja em virtude de disposição legal, ato de autoridade competente ou ordem judicial; (iii) Ainda que o tratamento de dados pessoais do titular não exija o seu consentimento, pode ele exigir a informação quanto ao seu compartilhamento. Além disso, o controlador, sempre que solicitado pelo titular dos dados pessoais, deverá confirmar se realiza o tratamento dos mesmos imediatamente em formato simplificado e, na impossibilidade de fornecer imediatamente, terá o prazo de 15 dias para entregar ao titular, seja de forma impressa, seja em formato eletrônico, a declaração clara e completa dos dados pessoais que possui ou da inexistência de registro dos mesmos. (LGPD, art. 19, I, II, §2º I, II).
6	**Proteção de Crédito**	A instituição pode comunicar aos órgãos de proteção ao crédito (LGPD, art. 7º, inciso X) o descumprimento de qualquer obrigação do usuário ou atraso de pagamento, bem como pode fornecer aos gestores dos bancos de dados de Cadastro Positivo (Lei 12.414/2011), registrados no Banco Central do Brasil (BACEN), seus dados financeiros e de pagamento relativos a operações de crédito e obrigações de pagamento, para formação de histórico de crédito, nos termos da legislação em vigor. Se não tiver interesse em participar do Cadastro Positivo, o usuário poderá a qualquer momento solicitar o cancelamento de seu cadastro ao gestor do banco de dados. **Atenção:** o usuário deve estar ciente e poderá consentir ou não que (i) os dados das suas operações de crédito, a vencer e vencidas, inclusive em atraso e baixadas com prejuízo, bem como os valores das coobrigações que tenha assumido e das garantias que tenha prestado, sejam fornecidos ao Banco Central do Brasil e registrados no Sistema de Informações de Créditos (SCR) e que ainda (ii) poderá consultar tais dados por meio do “Registrato” (Extrato do Registro de Informações), disponível no site do Banco Central, bem como poderá, também, em caso de divergência, pedir sua correção, exclusão ou registro de medida judicial, ou de manifestação de discordância, mediante solicitação à instituição que registrou os respectivos dados no SCR.
7	**Segurança e Sigilo dos dados**	Inicialmente, convém mencionar um aspecto relevante para a proteção de dados pessoais, qual seja, a observância à metodologia da *privacy by design* (privacidade desde a concepção) e, como decorrência da primeira, à *privacy by default* (privacidade por padrão). O princípio da segurança de ponta-a-ponta (*lifecycle protection*) se refere à proteção dos dados desde a sua coleta, isto é, quando o usuário insere seus dados até a sua eliminação. Nesse sentido, a segurança é um princípio a ser observado no tratamento de dados pessoais, destacado na Lei, no art. 6º, inciso VII e pode servir como parâmetro para a instituição na execução de um programa de governança em privacidade (LGPD, art. 50, caput). No âmbito da promoção de segurança, os processos e procedimentos devem assegurar a disponibilidade, integridade e confidencialidade de todas as formas de informação, visando o sigilo dessas, observando-se sempre os mais elevados princípios éticos e legais. Dessa forma, os agentes de tratamento (o controlador e o operador) devem adotar

		medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (LGPD, art. 46, § 2º), bem como responder pelos danos decorrentes de violações de segurança aos dados pessoais. Diante disso, é importante que o usuário (titular do dado) tenha ciência das medidas de segurança que foram implementadas no serviço que trata seus dados pessoais. Além disso, o controlador deverá comunicar ao usuário (titular) e à Autoridade Nacional de Proteção de Dados (ANPD) a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante ao titular (LGPD, art. 48) e, portanto, deve informar no Termo de Uso que essa comunicação será feita nesses casos. Recomenda-se também que o serviço possua um canal para comunicação de possíveis violações, falhas e vulnerabilidades, bem como, o uso de dados biométricos para que possíveis incidentes de segurança sejam reportados, identificados e tratados de forma mais ágil e preventivamente, além de tudo isso a identificação do responsável pela segurança cibernética (devido a res. 4.658/18). Dessa feita, em todas as etapas que compreendem o desenvolvimento do produto ou serviço, torna-se necessário respeitar o consentimento e a privacidade do usuário. **Atenção:** a violação de dados pessoais é uma violação de segurança que provoca, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizado a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento. Sendo assim, a instituição se compromete a tratar os dados pessoais do usuário com total confidencialidade, dentro dos limites legais estabelecidos pela Lei Geral de Proteção de Dados (LGPD).
8	***Cookies***	É importante que, caso o serviço utilize *cookies* de terceiros, todas as informações necessárias sobre os dados coletados, o tratamento realizado e finalidade do uso dos *cookies* seja informado ao usuário. Nesse sentido, a informação prévia sobre a existência, finalidades e tipos de dados coletados é extremamente relevante, em especial para *cookies*, que são disparados por terceiros. Deve ser informado também quais medidas de segurança são implementadas em seu uso (transferência de informações somente pelo protocolo HTTP, uso de criptografia obrigatório etc.). Resumidamente devem estar presentes as seguintes informações: (i) Quais *cookies* são utilizados (*cookies* proprietários ou de terceiros); (ii) Qual os dados são coletados pelos *cookies*; (iii) Qual a finalidade do uso de *cookies*; (iv) Como o usuário pode obter mais informações sobre os *cookies* de terceiros utilizados no serviço. **Atenção:** a realidade do uso de *cookies* no Brasil está bem distante da de outros países, não há, no ordenamento jurídico brasileiro, nenhuma menção expressa a *cookies*, nem mesmo na LGPD. Porém, não devem escapar de serem criteriosamente analisados e questionados em relação à sua conformidade com a Lei. Ainda assim, é indispensável o aviso prévio específico e o consentimento sobre a utilização dos mesmos. A partir do momento em que *cookies* são caracterizados como dados pessoais, surge uma clara preocupação em relação aos riscos à privacidade na sua utilização. No que tange ao dever de informações precisam ser claras e, acima de tudo, com a finalidade do uso dos *cookies*, por quem eles serão acessados, armazenados com quem serão compartilhados, por quanto tempo serão retidos e como podem ser excluídos. Ademais, nesse cenário: (i) as informações eventualmente armazenadas em *cookies* que permitam identificar um usuário são consideradas dados pessoais. Dessa forma, todas as regras previstas nesta Política de Privacidade também lhes são aplicáveis; (ii) os dados de navegação poderão, ainda, ser compartilhados com eventuais parceiros e fornecedores de serviços do *site*, serviços e sistema, buscando o aprimoramento dos produtos e serviços ofertados ao usuário; (iii) disponibilização de alguns *links* para as páginas de ajuda e suporte dos navegadores mais utilizados, que poderão ser acessadas pelo usuário interessado em obter mais informações sobre a gestão de *cookies* em seu navegador; (iv) caso seja do interesse do usuário, ele poderá configurar o seu

		navegador para negar os *cookies* ou indicar quando um *cookie* é enviado.
9	**Tratamento posterior de dados pessoais para outras finalidades**	Determinados dados pessoais podem ser utilizados para outras finalidades além daquelas relacionadas ao serviço financeiro prestado (LGPD, art. 7º, §7º). Informações sobre os dispositivos como modelo do *hardware*, tipo de sistema operacional, navegador utilizado para o acesso, localização, dentre outros, podem ser utilizados para melhoria contínua do serviço e aprimoramento da experiência do usuário. Assim, qualquer tratamento posterior dos dados pessoais para outras finalidades deve ser comunicado ao titular do dado. Resumidamente devem estar presentes as seguintes informações: (i) Quais dados poderão ser utilizados para tratamentos posteriores; e (ii) Qual a finalidade deste tratamento posterior.
10	**Transferência internacional de dados**	Alguns serviços podem envolver transferência de dados entre países (LGPD, art.33), como, por exemplo, quando há cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução. Para esses casos, deve-se deixar claro para o titular quais os dados serão transferidos internacionalmente, para qual finalidade, quais países estão envolvidos e qual o grau de proteção e privacidade fornecido por eles. Ademais, o consentimento no caso de transferência internacional de dados deverá ser específico e em destaque, sendo que o titular deverá saber do caráter internacional da coleta de dados, o que demandará esforços consideráveis por parte do controlador. **Atenção:** A instituição pode fornecer às autoridades monetárias e fiscais competentes informações relativas a operações em moeda estrangeira realizadas pelo usuário e pode consultar informações disponibilizadas pelo Banco Central do Brasil, Receita Federal do Brasil e Ministério do Desenvolvimento, Indústria e Comércio Exterior sobre quaisquer operações realizadas pelo mesmo no mercado de câmbio.
11	**Conservação de Dados**	Mesmo após o término do tratamento de dados (LGPD, art. 15) do usuário com a instituição, estes poderão ser mantidos pela mesma pelo tempo que for necessário para cumprir com as finalidades para as quais foram coletados, inclusive para fins de cumprimento de obrigações legais, regulatórias, contratuais, de prestação de contas ou requisição de autoridades competentes, bem como para resguardar e exercer direitos seus e da instituição, inclusive para prevenção de atos ilícitos e em processos judiciais, administrativos e arbitrais. **Atenção:** todos os dados coletados serão excluídos/eliminados dos servidores da instituição quando o usuário requisitar ou quando estes não forem mais necessários ou relevantes para os serviços, ou seja, quando atingirem sua finalidade (LGPD, art.16 e 18, VI).

Estes documentos, portanto, foram elaborados com base nas primeiras impressões a respeito do tema e as discussões travadas até o momento. Trata-se de matéria dinâmica que poderá ser revisitada, caso surjam novas interpretações da LGPD pela futura Autoridade Nacional de Proteção de Dados (ANPD). Por sua vez, fora apresentado, de forma resumida, as respectivas cláusulas, coerentes e sem abusividade, de acordo com a atual legislação relacionada a proteção de dados pessoais em vigor no país, desde 18 de setembro de 2020.

6 CONCLUSÃO

O estudo que compõe o presente trabalho teve por objetivo propor a elaboração de Contratos de Termos de Uso e de Políticas de Privacidade ideais, para bancos digitais, em conformidade com a Lei Geral de Proteção de Dados garantindo, assim, maior segurança da informação desses dados, de forma a prevenir e evitar riscos, expondo formas de responsabilização por parte dos bancos digitais acerca da coleta e armazenamento de dados identificando os fundamentos para responsabilização, bem como a análise e identificação dos pontos mais relevante da LGPD, as mudanças regulamentares e a evolução dos Bancos Digitais no Brasil. A pesquisa teve um foco de alinhar os objetivos propostos.

A pesquisa documental qualitativa e a pesquisa bibliográfica, associada a revisão da literatura, foram adotadas como métodos de pesquisa na forma descritiva e de investigação com uma abordagem de coleta de dados qualitativa e quantitativa com o intuito de relacionar os dados para a interpretação e responder a problemática da pesquisa.

A pesquisa bibliográfica abrangeu aspectos relacionados a Transformação Digital, Quarta Revolução Industrial, Dados e as Novas Tecnologias Digitais, evidenciando, assim, a importância do uso e comercialização adequada dos dados apoiado em mecanismos de controle interno (*compliance*), além das profundas transformações tecnológicas e disruptivas, repleta de desafios e de necessidades por conta da pandemia do coronavírus, bem como uma análise dos pontos mais relevantes, a respeito do Mercado Financeiro, *Startups* e *Fintechs*/Bancos Digitais, apresentando conceitos e definições, tendo como base o mapeamento do mercado e os marcos regulatórios do Banco Central do Brasil (BACEN) e a Comissão de Valores Mobiliários (CVM), além das normas suplementares, que recaem em todas as instituições. Nesse contexto, são expostos os desafios e perspectivas que irão provocar uma verdadeira revolução tecnológica para o setor de serviços financeiros oferecendo serviços digitais inovadores adaptados à transformação digital.

A coleta de dados contemplou aspectos gerais e características das legislações, com dados coletados em mecanismos de pesquisa *on-line*, obras doutrinárias, artigos de revistas jurídicas, periódicos científicos, anuários, *sites*, publicações eletrônicas e legislações, com destaque para a Constituição Federal, a Lei Geral de Proteção de Dados, com enfoque à proteção da privacidade e dos

dados pessoais de clientes de bancos digitais, além de dados secundários, capturados em *web sites*, compostos por documentos públicos, arquivos, relatórios, regulamentos, onde foram cruzados e interpretados tanto em quantidade como em qualidade, com uma legislação fundamentada nos referenciais teóricos desenvolvidos.

Foi identificado que é necessário integrar a LGPD e a Lei de Sigilo Bancário por meio de um diálogo entre elas que evidencie não apenas as relações dos clientes com as instituições, mas ainda nas relações jurídicas das instituições financeiras entre si e nas suas demais contratações com terceiros, onde como na LGPD, a coleta e a utilização de dados financeiros devem ser informadas aos titulares dos dados e estarem baseadas em uma ou mais bases legais de tratamento, sendo que qualquer alteração de finalidade ou destinação desses dados está sujeita a penalidades em razão dos riscos de exercício da atividade de tratamento, causar danos a outrem, em violação à LGPD. Ambos os dispositivos legais apresentam fundamentos e matrizes sobre as quais se estruturam, além de possíveis semelhanças quanto as atividades que podem ser realizadas sem a violação do dever de sigilo.

Os achados obtidos sugerem um contrato de termos de uso e política de privacidade em conformidade com a Lei Geral de Proteção de Dados que estabeleça cláusulas expondo com clareza as responsabilidades no tratamento de dados, de clientes de bancos digitais, com regras, diretrizes, direitos e deveres relacionados a finalidade do seu uso, a justificativa jurídica para tanto, além de novos direitos dos usuários como portabilidade, exclusão, minimização de uso, limitação entre outros. A vista disso, esses contratos fornecem subsídios para maior segurança no tratamento e armazenamento desses dados, com cláusulas-padrão preventivas, com informações claras e objetivas que garantam a confidencialidade dos dados coletados.

É importante salientar, ainda, que estes contratos seriam aplicados ou conduzidos pela instituição no momento em que fosse tratar, armazenar e comercializar (monetizar) os dados de seus usuários. A intenção desses documentos é muito mais no sentido de fornecer instrumentos para prevenção, no sentido de evitar problemas e exposição ao risco no manuseio dos dados pessoais.

Este trabalho gera algumas implicações teóricas, gerenciais e para legisladores.

Como implicações teóricas a presente pesquisa contribui no entendimento dos bancos digitais, como um tipo de *fintech* de serviços financeiros reguladas pelo Banco Central, que funcionam de forma *online* (100% digital), que se tornaram uma alternativa viável em tempos de crise por conta da pandemia da COVID-19, pela necessidade urgente de ter acesso de forma rápida e segura dos dados bancários, com mais eficiência de maneira simples pelo aplicativo, na tela do celular, sem burocracia, sempre visando a proteção desses dados, bem como a sua monetização em conformidade com a LGPD.

Como implicações gerenciais a presente pesquisa fornece uma orientação, uma dinâmica que auxilia os gestores de bancos digitais na obtenção de um programa de *compliance* eficiente e eficaz, apoiado em mecanismos de controle interno, em conformidade com a LGPD e a Lei de Sigilo Bancário, no qual indivíduos de qualquer relação que envolva o tratamento de informações sigilosas classificadas como dados pessoais ou financeiros daqueles que utilizam serviços, ou realizam qualquer tipo de transação *on-line* que envolva o fornecimento de informações, em consonância com que estabelece a LGPD, possam prevenir e evitar resultados danosos inerentes às suas atividades. Além disso, a oportunidade de se inovar com os dados, buscando novas formas de exploração, torna-se absolutamente necessária, a fim de torná-los ainda mais valiosos e encaixá-los como um ativo significativo das instituições, ou seja, é preciso monetiza-los, através de uma tecnologia inovadora, oferecendo APIs bem estruturados e seguros dentro do contexto de cada norma. Vale mencionar que é preciso que haja a implementação de medidas técnicas e/ou organizacionais de segurança da informação, segurança digital e cibersegurança, com medição de resultados apuráveis.

Outra implicação ao presente estudo, está para legisladores, permite a compreensão das aplicações das normas atuais com relação a proteção de dados, mais especificamente, a LGPD, a Lei do Sigilo Bancário (Lei Complementar nº 105 de 2001), a Lei do Cadastro Positivo (Lei nº 12.414 de 2011), e as Resoluções e Circulares do Conselho Monetário Nacional (“CMN”) e do Banco Central do Brasil (“BACEN”), como por exemplo, a Circular nº 4.015/2020, em conjunto com, a resolução nº 1/2020, que regulamenta o *Open Banking.* Ambas as normas estão interconectadas, e estabelecem que os dados pessoais de clientes somente poderão ser compartilhados com terceiros mediante o seu consentimento. Ainda para o refinamento futuro das leis, resoluções e circulares se faz a proposta de um estudo,

mais aprofundado, quanto ao grau de proteção social, através de parâmetros específicos, pautado no consentimento, e com foco na privacidade dos dados, “sigilosos”, “financeiros” e “pessoais”, para poder estimular, obrigações e responsabilidades mais precisas, prevendo sigilo e confidencialidade.

Conforme já referido, é importante observar que os achados são específicos em relação ao corpo de literatura utilizada e sua aplicação a *fintechs* de serviços financeiros (bancos digitais). Portanto, a fim de justificar a escolha nesse tipo de *fintech* foram utilizados dados que serviram para fundamentar o tema desenvolvido, em consonância com os objetivos propostos. Desse modo, a presente pesquisa está alicerçada, única e exclusivamente, pelo aprofundamento da compreensão dos bancos digitais, do que, propriamente, em outras instituições financeiras.

Assim, com relação a estudos futuros, é recomendável que novas obrigações previstas nas normas de proteção de dados sejam revisadas, após a efetiva implementação da ANPD, prevista para agosto de 2021, sobre assuntos que necessitam de uma atenção especial, como por exemplo, dever de *report* da Lei (art. 48); a importância de a ANPD ser um órgão independente, autônomo e altamente especializado, sem qualquer vínculo; além de outros temas , por exemplo, prazos e restrições para exercício de direitos dos titulares, forma de comunicação de incidentes e diretrizes sobre os mecanismos de transferência internacional de dados.

Por fim, diante do desenvolvimento do trabalho, é concluído que *Fintechs* de serviços financeiros (bancos digitais), transformação digital, Revolução 4.0, privacidade, proteção de dados, confidencialidade e o sigilo são assuntos que vêm evoluindo bastante nos últimos anos, principalmente pela aplicação de novas tecnologias digitais, que impactam de maneira significativa o mercado financeiro e de capitais. Nesse contexto, surge a LGPD, que basicamente é o primeiro instrumento coeso e robusto sobre proteção de dados, no Brasil, trazendo, em parte, uma sistematização sobre o que já existe fragmentado em outras normas, setoriais esparsas, ainda em vigor, com a diferença de que devem ser interpretadas e aplicadas considerando o que foi estabelecido pela Lei, quanto ao sigilo e a confidencialidade. Além disso, o ano de 2020, trouxe algumas reflexões quanto a temática da privacidade e da proteção de dados que refletirão para novas pesquisas, nos próximos anos, em assuntos como: as *fintechs* de serviços financeiros respondem de forma subjetiva ou objetiva pelos danos ocasionados aos seus usuários no tratamento de seus dados? Quais os efeitos de ter uma lei de proteção

de dados que se aplica somente a pessoas naturais? Caso ocorra algum incidente de segurança que acarrete risco ou danos relevantes aos titulares, existe algum modelo específico de segurança de informação nesse caso? Qual seria exatamente o modelo de "*compliance* digital" adequado para o mercado financeiro?

REFERÊNCIAS

ABINC. **A Gartner identificou as dez principais tecnologias e tendências de IoT.** Disponível em: < https://abinc.org.br/a-gartner-identificou-as-10-principais-tecnologias-e-tendencias-de-iot/>. Acesso em: 13 set. 2020.

ABRAMOVAY, Ricardo. Inteligência artificial pode trazer desemprego e fim da privacidade **Instituto Humanista UNISINOS,** São Leopoldo, 30 abr. 2017**.** Disponível em: < http://www.ihu.unisinos.br/78-noticias/566403-inteligencia-artificial-pode-trazer-desemprego-e-fim-da-privacidade>. Acesso em: 09 set. 2020.

ABSTARTUPS – Associação Brasileira de *Startups*. **Mapeamento *edtech* 2019.** Disponível em: < https://drive.google.com/file/d/1g2N2NfzMIddIw3dulHc0WCGLg_mhb_Nz/view>. Acesso em: 27 jun. 2020.

ABSTARTUPS – Associação Brasileira de *Startups*. **O Momento da Startup Brasileira e o Futuro do Ecossistema de Inovação.** Disponível em: < https://abstartups.com.br/PDF/radiografia-startups-brasileiras.pdf>. Acesso em: 27 jun. 2020.

ACCENTURE. **Can you change privacy risk challenges into gains?** Disponível em: < https://www.accenture.com/us-en/insights/financial-services/privacy-study-financial-services>. Acesso em: 19 out. 2020.

ACCENTURE. **Inteligência Artificial:** o que significa e porque é o futuro do crescimento? Disponível em: < https://www.accenture.com/br-pt/insight-artificial-intelligence-future-growth>. Acesso em: 12 set. 2020.

ACCENTURE. **Technology Vision Consumer Survey 2020**. Disponível em: < https://www.accenture.com/us-en/insights/technology/technology-trends-2020>. Acesso em: 30 ago. 2020.

ADJUST. **Relatório Mobile - Segmento Financeiro 2020.** Disponível em: < https://a.storyblok.com/f/47007/x/b9ada2cffd/mobile_finance_report_2020_pt.pdf>. Acesso em: 19 out. 2020.

AKAMAI. **State of the Internet / Security Financial Services Report 2020. v.6, p. 08.** Disponível em: < https://www.akamai.com/br/pt/multimedia/documents/state-of-the-internet/soti-security-financial-services-hostile-takeover-attempts-report-2020.pdf>. Acesso em:13 set. 2020.

ALCARVA, Paulo. **Banca 4.0. Revolução Digital:** *fintechs, blockchain*, criptomoedas, *robo-advisers* e *crowdfunding*. Coimbra: Conjuntura Actual Editora, 2018.

AMARAL, Rodrigo. *Compliance* digital: o guia completo sobre o assunto. **Blog A&M**. São Paulo, 27 mar. 2019. Disponível em: <

http://amaralmonteiro.com.br/compliance-digital-guia-completo/>. Acesso em: 06 mar. 2020.

ANANT, Venky; DONCHAK, Lisa; KAPLAN, James; SOLLER, Henning. The consumer-data opportunity and the privacy imperative. **McKinsey&Company.** Disponível em: < https://www.mckinsey.com/business-functions/risk/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative>. Acesso em: 09 set. 2020.

ANBIMA. **Análise da Lei Geral de Proteção de Dados e da Lei de Sigilo Bancário, vis-à-vis as regras de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo.** Disponível em: < https://www.anbima.com.br/data/files/EA/44/6B/57/D2EF471095F9BF476B2BA2A8/Memorando-LC-105_LGPD_PLD-FT-Pinheiro-Neto.pdf>. Acesso em: 19 out. 2020.

ANBIMA**. Lei Geral de Proteção de Dados ("LGPD") e Lei de Sigilo Bancário.** Disponível em: < https://www.anbima.com.br/data/files/3E/F3/0E/8A/C2EF471095F9BF476B2BA2A8/Memorando-LC-105_LGPD_PLD-FT-Mattos-Filho.pdf>. Acesso em: 19 out. 2020.

ANBIMA. **Guia de cibersegurança.** 2.ed. 6 dez. 2017. Disponível em: < https://www.anbima.com.br/data/files/F5/62/AB/91/FBC206101703E9F5A8A80AC2/Guia-de-Ciberseguranca-ANBIMA.pdf>. Acesso em: 15 out. 2020.

ANDRADE, Gustavo. **Brazil Digital Report:** relatório da McKinsey indica brasileiros mais conectados, mas falta de inovação. Disponível em: < https://inteligencia.rockcontent.com/brazil-digital-report/>. Acesso em: 24 out. 2020.

A Receita pode requisitar das instituições financeiras, sem autorização judicial, informações bancárias sobre o contribuinte. Entenda a decisão do STF. **Dizer o Direito.** Disponível em: < https://www.dizerodireito.com.br/2016/02/a-receita-pode-requisitar-das.html>. Acesso em: 19 out. 2020.

ASSI, Marcos. ***Gestão de Compliance e Seus Desafios***: como implementar controles internos, superar dificuldades e manter a eficiência dos negócios. São Paulo: Saint Paul Editora, 2013.

BANCO CENTRAL DO BRASIL. **Circular nº 3.909,** de 16 de agosto de 2018. Disponível em: < https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50645/Circ_3909_v1_O.pdf>. Acesso em: 15 out. 2020.

BANCO CENTRAL DO BRASIL. **Circular nº 3.955,** de 29 de julho de 2019. Disponível em: < https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50809/Circ_3955_v1_O.pdf>. Acesso em: 15 out. 2020.

BANCO CENTRAL DO BRASIL. **Circular nº 3.978,** de 23 de janeiro de 2020. Disponível em: < https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50905/Circ_3978_v1_O.pdf>. Acesso em: 15 out. 2020.

BANCO CENTRAL DO BRASIL. **Circular nº 3.979,** de 30 de janeiro de 2020. Disponível em: < https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50913/Circ_3979_v1_O.pdf>. Acesso em: 15 out. 2020.

BANCO CENTRAL DO BRASIL. **Circular nº 4.015,** de 04 de maio de 2020. Disponível em: < https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/51025/Circ_4015_v1_O.pdf>. Acesso em: 15 out. 2020.

BANCO CENTRAL DO BRASIL. **Resolução nº 4.656,** de 26 de abril de 2018. Disponível em: < https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50579/Res_4656_v1_O.pdf>. Acesso em: 15 out. 2020.

BANCO CENTRAL DO BRASIL. **Resolução nº 4.658,** de 26 de abril de 2018. Disponível em: < https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50581/Res_4658_v1_O.pdf>. Acesso em: 15 out. 2020.

BANCO CENTRAL DO BRASIL. **Resolução nº 4.737,** de 29 de julho de 2019. Disponível em: < https://www.pwc.com.br/pt/estudos/guia-demonstracoes-financeiras/2019/bacen-19-20.pdf>. Acesso em: 15 out. 2020.

BANCO CENTRAL DO BRASIL. **Resolução nº 4.752,** de 26 de setembro de 2019. Disponível em: < https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50846/Res_4752_v1_O.pdf>. Acesso em: 15 out. 2020.

BANCO CENTRAL DO BRASIL. **Resolução nº 4.792,** de 26 de março de 2020. Disponível em: < https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50959/Res_4792_v1_O.pdf>. Acesso em: 26 jun. 2020.

BANCO CENTRAL DO BRASIL. **Resolução Conjunta nº 1,** de 04 de maio de 2020. Disponível em: < https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/51028/Res_Conj_0001_v1_O.pdf>. Acesso em: 15 out. 2020.

BANCO CENTRAL DO BRASIL. **Infraestruturas do mercado financeiro.** Disponível em: < https://www.bcb.gov.br/estabilidadefinanceira/infraestruturamercado>. Acesso em: 26 jun. 2020.

BANCO CENTRAL DO BRASIL. **Medidas de combate aos efeitos da COVID-19.** Disponível em: < https://www.bcb.gov.br/acessoinformacao/medidasdecombate_covid19>. Acesso em: 26 jun. 2020.

BANCO ORIGINAL. **Política de privacidade.** Disponível em: < https://www.original.com.br/politicaprivacidade/>. Acesso em: 19 out. 2020.

BARBIERI, Carlos. **Governança de dados:** práticas, conceitos e novos caminhos. Rio de Janeiro: Alta Books, 2019.

BARBOSA, Danilo Ricardo Ferreira; DA SILVA, Carlos Sérgio Gurgel. A COLETA E O USO INDEVIDO DE DADOS PESSOAIS: UM PANORAMA SOBRE A TUTELA DA PRIVACIDADE NO BRASIL E A LEI GERAL DE PROTEÇÃO DE DADOS. Disponível em: < http://www.cidp.pt/revistas/rjlb/2019/6/2019_06_0473_0514.pdf>. Acesso em: 5 mar. 2020.

BARSOTTI, Danilo. Lei GDPR e LGPD: qual a relação na segurança da informação e os impactos nas organizações no mundo. **Revista Estadão: 24 maio 2019.** Disponível em: < https://politica.estadao.com.br/blogs/fausto-macedo/lei-gdpr-e-lgpd-qual-a-relacao-na-seguranca-da-informacao-e-os-impactos-nas-organizacoes-no-mundo/>. Acesso em: 29 mar. 2020.

BIONI, Bruno Ricardo. INOVAR PELA LEI. **GVEXECUTIVO**, v. 18, n. 4, jul/ago 2019. FUNDAÇÃO GETULIO VARGAS. ISSN 1806-8979. Disponível em: < file:///C:/Users/Cliente/Downloads/gvexecutivo20194-190826203335.pdf>. Acesso em: 29 mar. 2020.

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

BOEHM, Jim. et al. The risk-based approach to cybersecurity. **McKinsey & Company.** Disponível em: < https://www.mckinsey.com/business-functions/risk/our-insights/the-risk-based-approach-to-cybersecurity>. Acesso em: 19 out. 2020.

BUGHIN, Jacques. et al. Artificial intelligence can deliver real value to companies. **McKinsey&Company.** Disponível em: < https://www.mckinsey.com.br/business-functions/mckinsey-analytics/our-insights/how-artificial-intelligence-can-deliver-real-value-to-companies>. Acesso em: 13 set. 2020.

BL CONSULTORIA E ADVOCACIA DIGITAL. **Circular 3979/2020 BACEN – Risco Operacional vs Risco Cibernético.** Disponível em: < https://blconsultoriadigital.com.br/circular-3979-2020-bacen/>. Acesso em: 24 out. 2020.

BLANK, Steve. **Why the lean start-up changes everything.** Harvard Business Review, v. 91, n. 5, p. 63-72, 2013.

BRADLEY, Susan. **4 tops vulnerabilities ransomware attackers exploited in 2020.** CSO. Disponível em: < https://www.csoonline.com/article/3572336/4-top-vulnerabilities-ransomware-attackers-exploited-in-2020.html>. Acesso em: 15 out. 2020.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 05 mar. 2020.

BRASIL. **Decreto nº 9.854,** de 25 de junho de 2019. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9854.htm>. Acesso em: 15 out. 2020.

BRASIL. **Decreto nº 10.222,** de 05 de fevereiro de 2020. Disponível em: < https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419>. Acesso em: 15 out. 2020.

BRASIL. Escola Nacional de Defesa do Consumidor. A proteção de dados pessoais nas relações de consumo: para além da informação creditícia. vol.2, elaboração Danilo Doneda. – Brasília: SDE/DPDC, 2010. Disponível em: < https://legado.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf>. Acesso em: 29 ago. 2020.

BRASIL. Presidente (2019 -: Jair Messias Bolsonaro). **Mensagem ao Congresso Nacional, 2020:** 2ª Sessão Legislativa Ordinária da 56ª Legislatura. – Brasília: Presidência da República, 2020. – (Documentos da Presidência da República). Disponível em: < https://static.poder360.com.br/2020/02/Mensagem-ao-Congresso-2020.pdf>. Acesso em: 29 ago. 2020.

_____. **Lei Complementar Nº 105,** de 10 de janeiro de 2001. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm>. Acesso em: 07 jul. 2020.

_____. **Lei Complementar Nº 166,** de 08 de abril de 2019. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/lcp/Lcp166.htm>. Acesso em: 07 jul. 2020.

_____. **Lei Nº 4.595,** de 31 de dezembro de 1964. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l4595.htm>. Acesso em: 07 jul. 2020.

_____. **Lei Nº 8.078,** de 11 de setembro de 1990. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>. Acesso em: 07 jul. 2020.

_____. **Lei Nº 9.311,** de 24 de outubro de 1996. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l9311.htm#:~:text=LEI%20N%C2%BA%209.311%2C%20DE%2024%20DE%20OUTUBRO%20DE%201996.&text=Institui%20a%20Contribui%C3%A7%C3%A3o%20Provis%C3%B3ria%20sobre,CPMF%2C%20e%20d%C3%A1%20outras%20provid%C3%AAncias.>. Acesso em: 07 jul. 2020.

_____. **Lei Nº 9.507,** de 12 de novembro de 1997. Lei do Habeas Data. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/L9507.htm>. Acesso em: 07 jul. 2020.

_____. **Lei 12.965/14,** de 23 de abril de 2014. Marco Civil da Internet. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 05 mar. 2020.

_____. **Lei Nº 10.406,** de 10 de janeiro de 2002. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm>. Acesso em: 07 jul. 2020.

_____. **Lei Nº 12.414,** de 9 de junho de 2011. Lei do Cadastro Positivo. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>. Acesso em: 07 jul. 2020.

_____. **Lei Nº 12.527,** de 18 de novembro de 2011. Lei do Acesso à Informação. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 07 jul. 2020.

_____. **Lei 13.709/18,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 05 mar. 2020.

_____. **Lei Nº 13.853,** de 08 de julho de 2019. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm>. Acesso em: 07 jul. 2020.

_____. **Lei Nº 14.010,** de 10 de junho de 2020. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Lei/L14010.htm>. Acesso em: 07 jul. 2020.

BRASIL. Ministério da Fazenda. Comissão de Valores Mobiliários. Instrução **nº 505,** de 27 de setembro de 2011. Disponível em: < http://www.cvm.gov.br/export/sites/cvm/legislacao/instrucoes/anexos/500/inst505.pdf >. Acesso em: 15 out. 2020.

BRASIL. Ministério da Fazenda. Comissão de Valores Mobiliários. Instrução **nº 617,** de 05 de dezembro de 2019. Disponível em: < http://www.cvm.gov.br/export/sites/cvm/legislacao/instrucoes/anexos/600/inst617.pdf >. Acesso em: 15 out. 2020.

BRODSKY, Laura; OAKES, Liz. Data sharing and open banking. **McKinsey & Company.** Disponível em: < https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking>. Acesso em: 19 out. 2020.

BXBLUE. **O que é Cédula de Crédito Bancário (CCB)?** Disponível em: < https://bxblue.com.br/aprenda/cedula-de-credito-bancario-ccb-consignado/>. Acesso em: 24 out. 2020.

Cadernos Adenauer 2014. **Cibersegurança.** ano 15. n. 4. p.07. Rio de Janeiro: Fundação Konrad Adenauer, jun. 2015. Disponível em: < https://www.kas.de/c/document_library/get_file?uuid=ed6be5d1-dd4c-2ec8-0fff-ee8f5dcf3226&groupId=265553>. Acesso em: 13 set. 2020.

Cadernos Adenauer 2019. **Proteção de dados pessoais:** privacidade versus avanço tecnológico. ano 20. n. 3. Rio de Janeiro: Fundação Konrad Adenauer, out.

2019. Disponível em: < https://www.kas.de/documents/265553/265602/Caderno+Adenauer+3+Schutz+von+pers%C3%B6nlichen+Daten.pdf/476709fc-b7dc-8430-12f1-ba21564cde06?version=1.0&t=1571685012573>. Acesso em: 09 set. 2020.

CALICCHIO, Nicola; DIAS, Yran. O futuro do futuro. **McKinsey&Company.** Disponível em: < https://www.mckinsey.com/br/our-insights/blog-made-in-brazil/o-futuro-do-futuro>. Acesso em: 09 set. 2020.

CÂMARA DOS DEPUTADOS. Legislação sobre acesso à informação, proteção de dados pessoais e internet. [recurso eletrônico] Claudio nazareno, Guilherme Pereira Pinheiro (organizadores). n.22, 1.ed. Brasília: Câmara dos Deputados, Edição Câmara, 2020.

CANTARINO BRASILEIRO. Anuário Brasileiro de Bancos (ABB) 2017. **Relatório Bancário**. São Paulo, 2017. Disponível em: < https://cantarinobrasileiro.com.br/publicacoes/anuariodebancos17/download/>. Acesso em: 29 ago. 2020.

CANTARINO BRASILEIRO. Anuário Brasileiro de Bancos (ABB) 2019. **Relatório Bancário**, 14 ed. São Paulo, 2019. Disponível em: < https://cantarinobrasileiro.com.br/publicacoes/anuariodebancos19/download/>. Acesso em: 26 ago. 2020.

CANTARINO BRASILEIRO. Anuário Brasileiro de Bancos (ABB) 2020. **Relatório Bancário**. São Paulo, 2020. Disponível em: < https://cantarinobrasileiro.com.br/publicacoes/anuariodebancos20/download/>. Acesso em: 29 ago. 2020.

CARDOSO, André Guskow. **IoT- Internet das Coisas - o Decreto 9.854 e o Plano nacional de IoT**. Disponível em: < https://www.justen.com.br/pdfs/IE148/IE148-Decreto-IoT.pdf>. Acesso em: 13 set. 2020.

CARDOSO, Oscar Valente. A Lei Geral de Proteção de Dados protege dados ou informações? **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 25, n. 6280, 10 set. 2020. Disponível em: < https://jus.com.br/artigos/85291/a-lei-geral-de-protecao-de-dados-protege-dados-ou-informacoes>. Acesso em: 09 set. 2020.

CARDOSO, Oscar Valente. Lei Geral de Proteção de Dados e o diálogo das fontes: a vez da Lei do Sigilo Bancário. **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 25, n. 6259, 20 ago. 2020. Disponível em: < https://jus.com.br/artigos/84714/lei-geral-de-protecao-de-dados-e-dialogo-das-fontes-4-lei-do-sigilo-bancario >. Acesso em: 15 out. 2020.

CARDOSO, Oscar Valente. Lei Geral de Proteção de Dados e o diálogo das fontes: 5) Lei do Cadastro Positivo. **Revista Jus Navigandi**, Teresina, ano 25, ago. 2020. Disponível em: < https://jus.com.br/artigos/84868/lei-geral-de-protecao-de-dados-e-dialogo-das-fontes-5-lei-do-cadastro-positivo>. Acesso em: 15 out. 2020.

CARDOSO, Oscar Valente. Lei Geral de Proteção de Dados e o diálogo das fontes-10) Síntese Geral. **Revista Jus Navigandi**, Teresina, ano 25, set. 2020. Disponível em: < https://jus.com.br/artigos/85659/lei-geral-de-protecao-de-dados-e-dialogo-das-fontes-10-sintese-geral >. Acesso em: 15 out. 2020.

CARVALHO, André Castro; ALVIM, Tiago Cripa et al. **Manual de *Compliance.*** Rio de janeiro: Forense, 2019. ISBN 978-85-309-8315-4.

CARVALHO, Thaís Abreu et al. **Aplicabilidade da lei geral de proteção de dados e da metodologia" privacy by design" nos termos de uso e de política de privacidade.** 2019. Disponível em: < http://191.252.194.60:8080/bitstream/fdv/781/1/TCC%20-%20Thais%20Abreu.pdf>. Acesso em: 5 mar. 2020.

CASE, Steve. **Terceira onda da internet:** a reinvenção dos negócios na era digital. Tradução: Lizandra Magnon de Almeida. Rio de janeiro: Alta Books, 2019.

CEDRO INSIGHTS. **Transformação Digital:** um panorama da visão dos principais executivos em importantes instituições financeiras do país. Disponível em: < https://d335luupugsy2.cloudfront.net/cms/files/6060/1587994328Cedro_Insights_Transformacao_Digital_Setor_Financeiro_1.pdf>. Acesso em: 26 ago. 2020.

Centro Global de Capacidade de Segurança Cibernética (GCSCC). **Revisão da capacidade de cibersegurança.** Disponível em: < http://www.oas.org/pt/ssm/cicte/docs/PORT-Revisao-da-Capacidade-de-Ciberseguranca.pdf>. Acesso em: 15 out. 2020.

CIO. **Anbima lança guia de cibersegurança para instituições financeiras.** Disponível em: < https://cio.com.br/noticias/anbima-lanca-guia-de-ciberseguranca-para-instituicoes-financeiras/>. Acesso em: 13 set. 2020.

CIO. **Internet das coisas em 2020:** mais vital do que nunca. Disponível em: < https://cio.com.br/tendencias/internet-das-coisas-em-2020-mais-vital-do-que-nunca/>. Acesso em: 13 set. 2020.

CIRILLO, Maria Eugenia. **Monetizando dados pessoais.** Disponível em: < https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/regulacao-e-novas-tecnologias/monetizando-dados-pessoais-06062020>. Acesso em: 09 set. 2020.

COMISSÃO DE DIREITO DA TECNOLOGIA DA INFORMAÇÃO - CDTI. **O que estão fazendo com os meus dados? A importância da Lei Geral de Proteção de Dados.** Coordenação Paloma Mendes Saldanha. v.15. Recife: SerifaFina, 2019. ISNB 978-85-66599-12-1. Disponível em: < https://oabpe.org.br/wp-content/uploads/2020/01/Livro-CDTI-O-que-esta%CC%83o-fazendo-com-meus-dados-v15-7.pdf>. Acesso em: 6 mar. 2020.

CORDEIRO, António Menezes; DE OLIVEIRA, Ana Perestrelo; DUARTE, Diogo Pereira. ***Fintech*:** desafios da tecnologia financeira. 2º ed. Almedina, 2019.

CÓRDOVA, Yasodara; PROL, Flávio Marques. **Repensando a distribuição democrática de dados.** Disponível em: < https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/artigos/repensando-a-distribuicao-democratica-de-dados-10032017>. Acesso em: 09 set. 2020.

COSTA, Juliana. A importância da adequação da LGPD aos programas de *compliance*. **Revista Consultor Jurídico: 21dez. 2018** Disponível em: < https://www.conjur.com.br/2018-dez-21/juliana-costa-importancia-adequacao-lgpd-compliance>. Acesso em: 29 mar. 2020.

COSTA, Juliana. ***Blockchain* x *compliance*:** facilidades e limitações impostas pela LGPD. Disponível em: < https://www.serpro.gov.br/lgpd/noticias/2020/compliance-blockchain-lgpd-dados-pessoais-empresas>. Acesso em: 24 out. 2020.

COSSETTI, Melissa Cruz. **O que é um *ransomware*?** Disponível em: < https://tecnoblog.net/275356/o-que-e-um-ransomware/>. Acesso em: 24 out. 2020.

CHEVAL, Saif. **Exploring non-financial use cases of blockchain.** *District* 3. Disponível em: < https://medium.com/district3/exploring-non-financial-use-cases-of-blockchain-2839bacd50a4>. Acesso em: 09 set. 2020.

CHISHTI, Susanne; BARBERIS, Janos. **A Revolução Fintech:** o manual das startups financeiras. Tradução: Samantha Batista. Rio de janeiro: Alta Books, 2017.

C2R ADVOCACIA PARA NEGÓCIOS INOVADORES. **Saiba como Elaborar um "Termo de Uso" e uma "Política de Privacidade" (Understand Terms and Conditions and Privacy Policy)** JusBrasil. Disponível em: < https://roseadvocaciaparastartup.jusbrasil.com.br/artigos/507868098/saiba-como-elaborar-um-termo-de-uso-e-uma-politica-de-privacidade-understand-terms-and-conditions-and-privacy-policy>. Acesso em: 19 out. 2020.

Dados. In: Wikipédia: a enciclopédia livre. Disponível em: < https://pt.wikipedia.org/wiki/Dados> Acesso em: 29 mar. 2020.

DA COSTA, Marcos. **Direito à privacidade.** Disponível em: < https://www.oabsp.org.br/noticias/2007/10/16/4475>. Acesso em: 19 out. 2020.

DAHLQVIST, Fredrik. et al. Growwing opportunities in the internet of things. **McKinsey&Company.** Disponível em: < https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things/pt-br>. Acesso em: 13 set. 2020.

DA ROCHA, Camila Pereira et al. Segurança da Informação: A ISO 27.001 como Ferramenta de Controle para LGPD. **Revista de Tecnologia da Informação e Comunicação da Faculdade Estácio do Pará**, v. 2, n. 3, p. 78-97, 2019. Disponível em: < http://www.revistasfap.com/ojs3/index.php/tic/article/view/285/246>. Acesso em: 5 mar. 2020.

DA SILVA, Luciana Vasco. Direito de privacidade no direito brasileiro e norte americano. **Revista Eletrônica do Curso de Direito - PUC Minas Serro,** n.12, p.68-82, ago. / dez. 2015 – ISSN 2176-977X. Disponível em: < http://periodicos.pucminas.br/index.php/DireitoSerro/article/view/9051>. Acesso em: 19 out. 2020.

DATAREPORTAL. **Relatório Digital 2020: Brasil.** Disponível em: <https://datareportal.com/reports/digital-2020-brazil>. Acesso em: 29 ago. 2020.

DE ALMEIDA, Cristian Machado. **Inteligência Artificial no Setor Financeiro.** Disponível em: < https://www.industria40.ind.br/artigo/18361-inteligencia-artificial-no-setor-financeiro>. Acesso em: 09 set. 2020.

DE ALMEIDA, KATIA. **Análise da evolução da metodologia utilizada nos artigos publicados na revista:** contabilidade & finanças – USP. Disponível em: < http://sistema.semead.com.br/12semead/resultado/trabalhosPDF/642.pdf>.Acesso em: 05 dez. 2020.

DE OLIVEIRA, Ana Paula. A LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA NA PRÁTICA EMPRESARIAL. **Revista Jurídica da Escola Superior de Advocacia da OAB-PR / Ordem dos Advogados do Brasil.** Seção do Paraná; Escola Superior de Advocacia; Coordenação científica por Fernando Previdi Motta, William Soares Pugliese, Adriana D'Avila Oliveira.v.4, n.1 (maio 2019). Curitiba: 2019. 336 p. Disponível em: < http://revistajuridica.esa.oabpr.org.br/wp-content/uploads/2019/05/revista-esa-9.pdf#page=172>. Acesso em: 6 mar. 2020.

DE OLIVEIRA, Neide Cardoso. **Combate aos Crimes Cibernéticos.** MPF. Disponível em: < https://www.cnmp.mp.br/portal/images/Palestras/Atua%C3%A7%C3%A3o_do_MP_no_combate_aos_crimes_cibern%C3%A9ticosINFANCIA_E_JUVENTUDE.pdf>. Acesso em: 24 out. 2020.

DELOITTE, SL Deloitte. **Além da *fintech*:** oito forças que mudam o cenário competitivo. Disponível em: < https://www2.deloitte.com/content/dam/Deloitte/br/Documents/financial-services/Al%C3%A9m%20das%20Fintechs%20-%20Oito%20For%C3%A7as%20que%20Mudam%20o%20Cen%C3%A1rio%20Competitivo.pdf>. Acesso em: 24 out. 2020.

DELOITTE, SL Deloitte. **Indústria 4.0:** o desenvolvimento dos negócios em uma era conectada. Disponível em: < https://www2.deloitte.com/br/pt/pages/technology-media-and-telecommunications/articles/industria-4-0.html#>. Acesso em: 24 out. 2020.

DE SOUZA, Ivan. **Saiba o que é segurança digital e como implantá-la no site da sua empresa.** Disponível em: < https://rockcontent.com/br/blog/seguranca-digital/>. Acesso em: 24 out. 2020.

DEVTECNOLOGIA. **IoT no Setor Financeiro:** Bank of Things. Disponível em: < https://devtecnologia.com.br/iot-no-setor-financeiro-bank-of-things/>. Acesso em: 13 set. 2020.

DINIZ, Bruno. **O Fenômeno *Fintech*:** tudo sobre o movimento que está transformando o mercado financeiro no Brasil e no mundo. Rio de Janeiro: Alta Books, 2019.

DISTRITO. ***Fintech* mining report 2020.** Disponível em: < https://rdstation-static.s3.amazonaws.com/cms%2Ffiles%2F65883%2F1593523598FinTech_Report_2020_v7.pdf?utm_campaign=resposta_automatica_da_landing_page_dataminer_fintech_report_-_edicao_2020&utm_medium=email&utm_source=RD+Station>. Acesso em: 19 ago. 2020.

DOCK. **A segurança da informação para *fintechs*.** Disponível em: < https://dock.tech/blog/fintechs/seguranca-da-informacao-para-fintechs/>. Acesso em: 24 out. 2020.

Documentos da Cúpula Mundial sobre a Sociedade da Informação [livro eletrônico]: Genebra 2003 e Túnis 2005 / International Telecommunication Union; [traduzido por Marcelo Amorim Guimarães]. São Paulo: Comitê Gestor da Internet no Brasil, 2014, p.27. Disponível em: < https://www.cgi.br/media/docs/publicacoes/1/CadernosCGIbr_DocumentosCMSI.pdf >. Acesso em: 30 ago. 2020.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law (EJJL**). Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: < https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315/658>. Acesso em: 19 out. 2020.

É possível o compartilhamento, sem autorização judicial, dos relatórios de inteligência financeira da UIF e do procedimento fiscalizatório da Receita Federal com a Polícia e o Ministério Público. **Dizer o Direito.** Disponível em: < https://www.dizerodireito.com.br/2019/12/e-possivel-o-compartilhamento-sem.html>. Acesso em: 19 out. 2020.

ELLEN, Patrícia. Internet das coisas já é realidade, porém falta regulamentá-la. **McKinsey&Company.** Disponível em: < https://www.mckinsey.com.br/our-insights/blog-made-in-brazil/internet-das-coisas-ja-e-realidade-porem-falta-regulamenta-la>. Acesso em: 13 set. 2020.

ENGEL, Paulo Martins. **Inteligência Artificial.** Disponível em: < http://www.inf.ufrgs.br/~engel/data/media/file/inf01048/introducao.pdf>. Acesso em: 09 set. 2020.

Enciclopédia Jurídica da PUCSP, tomo II (recurso eletrônico): direito administrativo e constitucional / coord. Vidal Serrano Nunes Jr. et al. - São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: <

https://enciclopediajuridica.pucsp.br/pdfs/direito-a-privacidade_58e9502c41f94.pdf>. Acesso em: 19 out. 2020.

EQUIPE TD. **A Transformação Digital no Financeiro é obrigatória – e urgente!** Disponível em: < https://transformacaodigital.com/financeiro/a-transformacao-digital-no-financeiro-e-obrigatoria-e-urgente/>. Acesso em: 24 out. 2020.

EROLES, Pedro. ***Fintechs*, Bancos Digitais e Meios de Pagamento:** aspectos regulatórios das novas tecnologias financeiras. São Paulo: Quartier Latin, 2019.

FARIAS, Pedro. **Serviços públicos à distância:** o que a pandemia nos ensinou. Disponível em: < https://blogs.iadb.org/brasil/pt-br/servicos-publicos-a-distancia-o-que-a-pandemia-nos-ensinou/ >. Acesso em: 19 jun. 2020.

FEBRABAN. **Como Fazer os Juros Serem mais baixos no Brasil – Uma proposta dos bancos ao governo, Congresso, Judiciário e à sociedade.** 2º edição. São Paulo: Febraban, 2019. Disponível em: < https://jurosmaisbaixosnobrasil.com.br/febraban_ed2.pdf>. Acesso em: 26 jun. 2020.

FEBRABAN. **Clientes pessoas físicas fizeram 74% das transações bancárias pelos canais digitais em abril.** Disponível em: < https://portal.febraban.org.br/noticia/3474/pt-br/>. Acesso em: 27 jul. 2020.

FEBRABAN. **Observatório Febraban (IV). Set. 2020**. Disponível em: < https://cmsportal.febraban.org.br/Arquivos/documentos/PDF/200926_iD_%20OBSERVAT%C3%93RIO%20FEBRABAN%20IV_%20SETEMBRO%202020%20%23BRASILONLINE_final.pdf>. Acesso em: 29 ago. 2020.

FEBRABAN. **Pandemia do Covid-19 acelera uso dos canais digitais nos bancos**. Disponível em: < https://portal.febraban.org.br/noticia/3476/pt-br/>. Acesso em: 26 jun. 2020.

FILHO, Renato Valbert de Casto; LUZ, Thiago Terin Luz. **Cuide do seu negócio. Esteja em *compliance* com a LGPD.** Disponível em: < https://www.migalhas.com.br/depeso/307191/cuide-do-seu-negocio-esteja-em-compliance-com-a-lgpd>. Acesso em: 29 mar. 2020.

FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. PRIVACIDADE e LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS. **Revista de Direito Brasileira**, v. 23, n. 9, p. 284-301, 2020. Disponível em: < https://indexlaw.org/index.php/rdb/article/view/5343/4545>. Acesso em: 5 mar. 2020.

FINTECHLAB. **BC informa já ter autorizado 30 *fintechs* de crédito entre SCD e SEP.** Disponível em: < https://fintechlab.com.br/index.php/2020/06/29/bc-informa-ja-ter-autorizado-30-fintechs-de-credito-entre-scd-e-sep/>. Acesso em: 26 jun. 2020.

FINTECHLAB. **Febraban revela que contas abertas pelo *smartphone* cresceram 66% em 2019.** Disponível em: < https://fintechlab.com.br/index.php/2020/06/22/febraban-revela-que-contas-abertas-pelo-smartphone-cresceram-66-em-2019/>. Acesso em: 26 jun. 2020.

FINTECHLAB. ***Fintechs* e a Segurança da Informação.** Disponível em: < https://fintechlab.com.br/index.php/2016/08/15/fintechs-e-a-seguranca-da-informacao/>. Acesso em: 13 set. 2020.

FINTECHLAB. **Radar FintechLab mapeia mais de 600 iniciativas.** Disponível em: < https://fintechlab.com.br/index.php/2019/06/12/8a-edicao-do-radar-fintechlab-registra-mais-de-600-iniciativas/>. Acesso em: 19 jun. 2020.

FINTECHLAB. **Novo Radar FintechLab detecta 270 novas fintechs em um ano.** Disponível em: < https://fintechlab.com.br/index.php/2020/08/25/edicao-2020-do-radar-fintechlab-detecta-270-novas-fintechs-em-um-ano/>. Acesso em: 13 set. 2020.

FINTECHLAB. **Report Fintechlab 2016.** Disponível em: < http://fintechlab.com.br/wp-content/uploads/2017/02/Report_FintechLab_2016_alta.pdf >. Acesso em: 26 jun. 2020.

FINTECHLAB. **Report Fintechlab 2017.** Disponível em: < http://fintechlab.com.br/wp-content/uploads/2017/02/Report_FintechLab_2017.pdf>. Acesso em: 26 jun. 2020.

FONTOURA, Paula Renata. **Alan Turing, o pai da computação.** Disponível em: < http://www.invivo.fiocruz.br/cgi/cgilua.exe/sys/start.htm?infoid=1370&sid=7>. Acesso em: 09 set. 2020.

FONTES, Edison Luiz Gonçalves. **Segurança da Informação:** gestão e governança. 1.ed. São Paulo, 2020. Livro eletrônico.

FORBES. **Os melhores bancos do mundo:** Nubank é o primeiro entre os dez mais no Brasil. Disponível em: < https://forbes.com.br/listas/2020/06/os-melhores-bancos-do-mundo-nubank-e-o-primeiro-entre-os-dez-mais-no-brasil/>. Acesso em: 25 jun. 2020.

FOSSE, Gustavo; BIAGINI, Sergio. **Pesquisa FEBRABAN de Tecnologia Bancária 2020. Ano-base 2019.** FEBRABAN, [S. l.], p. 1-57, 1 jan. 2020. Disponível em < https://cmsportal.febraban.org.br/Arquivos/documentos/PDF/Pesquisa%20Febraban%20de%20Tecnologia%20Banc%C3%A1ria%202020%20VF.pdf>. Acesso em 26 jun. 2020.

FURLAN, Fabiano Ferreira. **Sigilo bancário.** Prefácio Carlos Alberto Rohrmann. Belo Horizonte: Fórum, 2008.

FRAZÃO, Ana; TEPENDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** 2.ed. São Paulo: Thomson Reuters Brasil, 2020

FRAZÃO, Ana. **Nova LGPD**: principais repercussões para a atividade empresarial. Disponível em: < https://www.jota.info/opiniao-e-analise/colunas/constituicao-

empresa-e-mercado/nova-lgpd-principais-repercussoes-para-a-atividade-empresarial-29082018>. Acesso em: 06 mar. 2020.

GARTNER. **Fact vs Fiction:** Finance Use of AI. Disponível em: < https://www.gartner.com/smarterwithgartner/fact-vs-fiction-finance-use-of-ai/>. Acesso em: 13 set. 2020.

GARTNER. **Insight Report 10 Strategic Technology Trends for 2019.** Disponível em: < https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2019/>. Acesso em: 09 set. 2020.

GARTNER. **Insight Report 10 Strategic Technology Trends for 2021.** Disponível em: < https://www.gartner.com/smarterwithgartner/gartner-top-strategic-technology-trends-for-2021/>. Acesso em: 09 set. 2020.

GARTNER. **Machine Learning.** Disponível em: < https://www.gartner.com/en/information-technology/glossary/machine-learning>. Acesso em: 13 set. 2020.

GARTNER. **Robotic Process Automation (RPA) Role in Finance Automation.** Disponível em: < https://www.gartner.com/en/finance/insights/robotics-in-finance>. Acesso em: 13 set. 2020.

GARTNER. **The Call for Legal and Compliance to Minimize Data Privacy Risk.** Disponível em: < https://www.gartner.com/smarterwithgartner/call-legal-compliance-minimize-data-privacy-risk/>. Acesso em: 19 out. 2020.

GARTNER IT SYMPOSIUM/XPO. **Transformação Digital nos Negócios.** Disponível em: < https://www.gartner.com/pt-br/conferences/la/symposium-brazil/featured-topics/digital-transformation>. Acesso em: 26 ago. 2020.

GUIA DE BOAS PRÁTICAS LEI GERAL DE PROTEÇÃO DE DADOS (LGPD). v.1 (abril 2020). Brasília 2020. Disponível em: < https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf>. Acesso em: 19 out. 2020.

GTI DIGITAL. **Política de Privacidade e LGPD.** Disponível em: < https://www.gtidigital.com/lgpd/>. Acesso em: 19 out. 2020.

HAGSTRÖM, Carlos Alberto. **Comentários à lei do sigilo bancário:** Lei Complementar nº105, de 10 de janeiro de 2001. Porto Alegre: Sergio Antônio Fabris Ed., 2009.

Heitor Martins, H.; Bartolumeu Dias, Y.B.; Castilho, P.; Leite, P. Transformações digitais no Brasil: *insights* sobre o nível de maturidade digital das empresas no país. ***McKinsey&Company*.** Disponível em: <https://www.mckinsey.com/br/our-insights/transformacoes-digitais-no-brasil#>. Acesso em: 26 ago. 2020.

HENRIQUE, Lygia Maria M. Molina; CHIAVASSA, Marcelo. **DPO e a figura do Diretor de Compartilhamento de Dados na Resolução do BACEN.** Disponível em: < https://www.jota.info/opiniao-e-analise/artigos/dpo-e-a-figura-do-diretor-de-

compartilhamento-de-dados-na-resolucao-do-bacen-28052020>. Acesso em: 26 ago. 2020.

HINTZBERGEN, Jule et al. **Fundamentos de Segurança da Informação:** com base na ISO 27001 e na ISO 27002.1ºEd. Brasport, 2018. Livro eletrônico, não paginado.

HORN, Guilherme. As tendências e benefícios da Inteligência Artificial em Serviços Financeiros. **Instituto Humanista UNISINOS,** São Leopoldo, 20 jul. 2017**.** Disponível em: < http://www.ihu.unisinos.br/78-noticias/569800-as-tendencias-e-beneficios-da-inteligencia-artificial-em-servicos-financeiros>. Acesso em: 09 set. 2020.

HSM UNIVERSITY. **A transformação digital nos bancos e o surgimento das *fintechs*.** São Paulo, 2019. Disponível em: < https://hsmuniversity.com.br/blog/transformacao-digital-bancos/>. Acesso em: 26 ago. 2020.

IMGBIN. **Computing Machinery And Intelligence Turing Test Venn Diagram Bletchley Park**. Disponível em: < https://imgbin.com/png/3LQxAx7m/computing-machinery-and-intelligence-turing-test-venn-diagram-bletchley-park-png>. Acesso em: 09 set. 2020.

INAFA.ORG. **10 melhores bancos digitais disponíveis no Brasil.** Disponível em: < https://en.inafa.org/10-best-digital-banks-available-brazil>. Acesso em: 19 jun. 2020.

INOVASOCIAL. **Unisys Security Index (USI) 2020:** o que os brasileiros pensam sobre a LGPD?
Disponível em: < https://inovasocial.com.br/solucoes-de-impacto/unisys-security-index-2020-lgpd/>. Acesso em: 19 out. 2020.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). Governança Corporativa. Disponível em: < http://www.ibgc.org.br/governanca/governanca-corporativa >. Acesso em: 27 ago. 2020.

ISO / IEC 27001. **Gestão de segurança da informação**. Disponível em: < https://www.iso.org/isoiec-27001-information-security.html>. Acesso em: 12 set. 2020.

ITS. **Privacidade e Segurança Online.** Disponível em: < https://itsrio.org/pt/cursos/privacidade-e-seguranca-online-2/>. Acesso em: 19 out. 2020.

JIMENE, Camilla do Vale; VAINZO, Rony. **Cinco pontos fundamentais de *compliance* digital para o seu programa de *compliance*.** Disponível em: < https://d335luupugsy2.cloudfront.net/cms/files/28354/1521065508Compliance_Digital.pdf>. Acesso em: 09 set. 2020.

Julia**.** Termos de uso e Política de Privacidade: Entenda o que são e qual a Importância? **Blog P&M.** Guaíba, 31 jan. 2019. Disponível em: <

https://www.pereiraemallmann.com.br/termos-de-uso-e-politica-de-privacidade/>. Acesso em: 06 mar. 2020.

JUNQUEIRA, Daniel. **Nos EUA, 87% consideram a privacidade de dados como um direito humano.** Disponível em: < https://olhardigital.com.br/noticia/nos-eua-87-consideram-a-privacidade-de-dados-como-um-direito-humano/104819>. Acesso em: 24 out. 2020.

KASPERSKY. **O que é cibersegurança?** Disponível em: < https://www.kaspersky.com.br/resource-center/definitions/what-is-cyber-security>. Acesso em: 15 out. 2020.

KELLER, Elaine. **Privacidade, lei geral de proteção de dados e covid-19.** Disponível em: < https://migalhas.uol.com.br/depeso/324959/privacidade-lei-geral-de-protecao-de-dados-e-covid-19>. Acesso em: 19 out. 2020.

KPMG. **Consumers and the new reality.** Disponível em: < https://home.kpmg/br/pt/home/insights/2020/07/consumers-and-the-new-reality.html>. Acesso em: 29 ago. 2020.

KPMG. **Inteligência Artificial:** conheça os cinco pilares que conduzem a aplicação. Disponível em: < https://home.kpmg/br/pt/home/insights/2020/02/inteligencia-artificial-pilares.html>. Acesso em: 13 set. 2020.

KPMG. **The new imperative for corporate data responsibility.** Disponível em: < https://advisory.kpmg.us/content/dam/advisory/en/pdfs/2020/consumer-data-report-kpmg.pdf>. Acesso em: 19 out. 2020.

KREMER, Bianca. **LGPD em vigor:** por que racializar a proteção de dados é tão importante? Disponível em: < https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/artigos/lgpd-em-vigor-protecao-dados-importante-01102020>. Acesso em: 19 out. 2020.

LAMARRE, Eric; MAY, Brett. Ten trends shaping the Internet of things business landscape. **McKinsey&Company.** Disponível em: < https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/ten-trends-shaping-the-internet-of-things-business-landscape/pt-br>. Acesso em: 13 set. 2020.

LAZARO, Roberto; LOUREIRO, Vitor. **Boas práticas em Governança de Dados.** 2019. Disponível em: < https://www.serasaexperian.com.br/blog/boas-praticas-em-governanca-de-dados>. Acesso em: 29 mar. 2020.

LEE, Kai-Fu. **Inteligência artificial:** como os robôs estão mudando o mundo, a forma como amamos, nos relacionamos, trabalhamos e vivemos. Tradução: Marcelo Barbão. 1º ed. Rio de janeiro: Globo Livros, 2019.

Lei 13.709/2018: Lei Geral de Proteção de Dados Pessoais. **Dizer o Direito.** Disponível em: < https://www.dizerodireito.com.br/2018/08/lei-137092018-lei-geral-de-protecao-de.html>. Acesso em: 05 mar. 2020.

Liferay, Inc. O que é Transformação Digital? Disponível em: < https://www.liferay.com/pt/resources/l/digital-transformation>. Acesso em: 29 mar. 2020.

LOGBANK. ***Fintechs* e a importância da segurança de dados.** Disponível em: < https://logbank.com.br/2019/04/29/fintechs-e-a-importancia-da-seguranca-de-dados/#:~:text=A%20seguran%C3%A7a%20da%20informa%C3%A7%C3%A3o%20deve,tratadas%20com%20cautela%20e%20privacidade.>. Acesso em: 12 set. 2020.

LUVIZAN, Simone S. DESAFIOS DE USAR DADOS PARA NOVOS FINS. **GVEXECUTIVO**, v. 18, n. 4, jul/ago 2019. FUNDAÇÃO GETULIO VARGAS. ISSN 1806-8979. Disponível em: < file:///C:/Users/Cliente/Downloads/gvexecutivo20194-190826203335.pdf>. Acesso em: 29 mar. 2020.

LLORENTE, José Antônio. A Transformação digital. **Revista UNO:** 2016, n. 24, p. 04-66. Disponível em: < https://www.revista-uno.com.br/wp-content/uploads/2013/09/160520_UNO24_BR.pdf>. Acesso em: 29 ago. 2020.

MACEDO, Fernanda dos Santos; BUBLITZ, Michelle Dias; RUARO, Regina Linden. A *privacy* norte-americana e a relação com o direito brasileiro. **Revista Jurídica Cesumar.** v. 13 n. 1, p. 161-178, jan./jun.2013 - ISSN 1677-64402. Disponível em: < https://periodicos.unicesumar.edu.br/index.php/revjuridica/article/view/2666/1898>. Acesso em: 19 out. 2020.

MAGRANI, Eduardo. **Entre dados e robôs:** ética e privacidade na era da hiperconectividade. Rio de Janeiro: Konrad Adenauer Stiftung, 2018. 196p. ISBN 978-85-7504-223-6. Disponível em: < https://www.kas.de/documents/265553/265602/Entre+dados+e+robos++Etica+e+Privacidade+HiperconectividadeFINAL.pdf/15aff602-9e8b-055b-008a-65319951eddc?version=1.0&t=1567793718597>. Acesso em: 24 out. 2020.

MACHADO, Felipe Nery Rodrigues; DE ABREU, Mauricio Pereira. **Projeto de banco de dados:** uma visão prática. Editora Érica, 17º edição. São Paulo, 2018.

MALERBA, F.; ADAMS, P. Sectoral Systems of Innovation. In: DOGDGSON, M.; GANN, D. M.; PHILLIPS, N. The Oxford Handbook of Innovation Management. Oxford, Oxford University Press. 2015. (Cap. 10)

Marco Civil da Internet. In: Wikipédia: a enciclopédia livre. Disponível em: < https://pt.wikipedia.org/wiki/Marco_Civil_da_Internet> Acesso em: 6 mar. 2020.

MARTINEZ, José Roberto. **Sua *Fintech* e a LGPD: cuidados sobre o tratamento de dados.** Jusbrasil. Disponível em: < https://ndmadvogados.jusbrasil.com.br/artigos/776543520/sua-fintech-e-a-lgpd-cuidados-sobre-o-tratamento-de-dados>. Acesso em: 24 out. 2020.

MARTINS, Gabriel da Silva. **Segurança digital:** o guia para segurança na internet. 1º ed. São Paulo Brutal Security, 2015**.** Livro eletrônico, não paginado.

MIKKELSEN, Daniel; SOLLER, Henning; STRANDELL-JANSSON, Malin**.** What will Europe's e-privacy regulation mean for your business? **McKinsey&Company.** Disponível em: < https://www.mckinsey.com/business-functions/risk/our-insights/what-will-europes-eprivacy-regulation-mean-for-your-business>. Acesso em: 19 out. 2020.

MONTEIRO, Renato Leite. et al. **Proteção de Dados no Setor Financeiro.** Disponível em: < http://baptistaluz.com.br/wp-content/uploads/2017/12/Brazil-Data-Protection-in-the-Financial-Sector_2017_PORT.pdf>. Acesso em: 19 out. 2020.

MONTEIRO, Renato Leite. et al. **LGPD e Fintechs:** um novo cenário para o *compliance* digital. Disponível em: < https://baptistaluz.com.br/institucional/lgpd-fintechs-compliance-digital-2/?utm_campaign=newsletter__dezembro_2020&utm_medium=email&utm_source=RD+Station> Acesso em: 21 dez. 2020.

MORAIS, Felipe. **Transformação digital.** São Paulo: Saraiva Educação, 2020.

MORIBE, Gabriela Tiemi; SILVA, Gustavo Henrique Luz. **O que ainda não te contaram sobre a "nova" Lei do Cadastro Positivo?** Disponível em: < https://baptistaluz.com.br/wp-content/uploads/2020/01/lei_cadastro_positivo_VF.pdf>. Acesso em: 19 out. 2020.

MORIBE, Gabriela Tiemi. **Série Open Banking no Brasil:** a proteção de dados pessoais na regulação do Open Banking. Disponível em: < https://baptistaluz.com.br/wp-content/uploads/2020/09/BLUZ_Open-banking-lgpd.pdf>. Acesso em: 19 out. 2020.

MUKNICKA, Rosana. Você está em *compliance* com a LGPD? **Revista Estadão: 11 jun 2019.** Disponível em: < https://politica.estadao.com.br/blogs/fausto-macedo/voce-esta-em-compliance-com-a-lgpd/>. Acesso em: 29 mar. 2020.

MURITIBA, José. **A resposta do ecossistema de startups à pandemia.** Disponível em: < https://www.jornaldocomercio.com/_conteudo/ge2/noticias/2020/05/738210-a-resposta-do-ecossistema-de-startups-a-pandemia.html>. Acesso em: 27 jun. 2020.

MCKINSEY&COMPANY. **Relatório Brazil Digital Report.** 1º edição, 2019. Disponível em: <https://www.mckinsey.com.br/~/media/McKinsey/Locations/South%20America/Brazil/Our%20Insights/Brazil%20Digital%20Report/Brazil-Digital-Report-1st-Edition_Portuguese-vAjustado.pdf>. Acesso em: 29 ago. 2020.

MCKINSEY&COMPANY. **[Report]** Smartening up with artificial intelligence (AI). Disponível em:<https://www.mckinsey.com.br/industries/semiconductors/our-insights/smartening-up-with-artificial-intelligence>. Acesso em: 29 ago. 2020.

NAMBISAN, Satish et al. Digital Innovation Management: Reinventing innovation management research in a digital world. Mis Quarterly, v. 41, n. 1, 2017.VAN ALSTYNE, Marshall W.; PARKER, Geoffrey G.; CHOUDARY, Sangeet Paul.

NETTO, Abner da Silva; DA SILVEIRA, Marco Antônio Pinheiro. **Information security management:** factors that influence its adoption in small and mid-sized businesses. SciELO, 2007. Disponível em: < https://www.scielo.br/scielo.php?script=sci_arttext&pid=S1807-17752007000300007>. Acesso em: 12 set. 2020.

NUBANK. **O que é um Banco Digital? Qual a diferença para um banco tradicional?** Disponível em: < https://blog.nubank.com.br/banco-digital-o-que-e/>. Acesso em: 19 jun. 2020.

OIOLI, Erik Frederico. **Manual de direito para startups**.2. ed. ver., atual. e ampl. São Paulo: Thomson Reuters, 2020.

OLIVEIRA, Carlos Eduardo Elias de. **Aspectos Principais da Lei nº 12.965, de 2014, o Marco Civil da Internet: subsídios à comunidade jurídica.** Brasília: Núcleo de Estudos e Pesquisas/CONLEG/ Senado, abr./2014 (Texto para Discussão nº 148). Disponível em: < https://www12.senado.leg.br/publicacoes/estudos-legislativos/tipos-de-estudos/textos-para-discussao/td-148-aspectos-principais-da-lei-no-12.965-de-2014-o-marco-civil-da-internet-subsidios-a-comunidade-juridica>. Acesso em: 6 mar. 2020.

OLIVEIRA, Denis Marcelo. et al. **Guia de Elaboração de Termo de Uso para serviços públicos.** v.1 (setembro 2020). Brasília: 2020. Disponível em: < https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaTermoUso.pdf>. Acesso em: 19 out. 2020.

PALHARES, Felipe. et al. **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020.

PARO, João Pedro. **Estratégia brasileira de segurança cibernética (E-Ciber).** Disponível em: < https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/compliance-pelo-mundo/estrategia-brasileira-de-seguranca-cibernetica-e-ciber-09022020>. Acesso em: 24 out. 2020.

PEIXOTO, Erick Lucena Campos; JÚNIOR, Marcos Ehrhardt. Os desafios da compreensão do direito à privacidade no sistema jurídico brasileiro em face das novas tecnologias**. REVISTA JURÍDICA LUSO-BRASILEIRA (RJLB)**, ANO 6 (2020), n.º 2, ISSN: 2183-539X, p.389-418. Disponível em: < https://www.cidp.pt/revistas/rjlb/2020/2/2020_02_0389_0418.pdf>. Acesso em: 19 out. 2020.

PELLINI, Rudá. **O futuro do dinheiro: banco digital, *fintechs, criptomoedas* e *blockchain*:** entenda de uma vez por todos esses conceitos e saiba como a tecnologia dará liberdade e segurança para você gerar riqueza. São Paulo: Editora Gente, 2019.

PELOSO PIURCOSKY, Fabrício et al. A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos. **Suma de Negócios**, v. 10, n. 23, p. 89-99, 2019. Disponível em: < http://www.scielo.org.co/pdf/sdn/v10n23/2215-910X-sdn-10-23-89.pdf>. Acesso em: 5 mar. 2020.

PEREIRA, Luís Moniz. **Inteligência Artificial:** mito e ciência. ResearchGate. Disponível em: < https://www.researchgate.net/publication/242109725_INTELIGENCIA_ARTIFICIAL_-_MITO_E_CIENCIA>. Acesso em: 09 set. 2020.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais:** comentários à Lei nº 13.709/2018 (LGPD). 2º ed. São Paulo: Saraiva Educação, 2020**.**

PINHEIRO, Patrícia Peck. **Direito Digital**. 5 ed. São Paulo: Editora Saraiva, 2013. Livro eletrônico, não paginado.

Pipelines, platforms, and the new rules of strategy. Harvard business review, v. 94, n. 4, p. 54-62, 2016.

Política de Privacidade: o que é e como montar uma! **Blog da Rock Content:** Software e Estratégias de Marketing de Conteúdo. 11 nov. 2018. Disponível em: < https://rockcontent.com/blog/politica-de-privacidade/>. Acesso em: 06 mar. 2020.

PORTO, Éderson Garin. ***Compliance* & Governança Corporativa:** uma abordagem prática e objetiva. Porto Alegre: Lawboratory, 2020.

PORTO, Éderson Garin. **Manual jurídico da startup:** como desenvolver projetos inovadores com segurança. 2.ed. ver. E atual. Porto Alegre: Livraria do Advogado, 2020.

PORTULANS INSTITUTE. **Relatório The Networked Readiness Index (NRI).** 2ºed. 2020. Disponível em: < https://networkreadinessindex.org/wp-content/uploads/2020/10/NRI-2020-Final-Report-October2020.pdf>. Acesso em: 29 ago. 2020.

PRICE WATERHOUSE COOPERS (PWC). **Pesquisa *Fintech Deep Dive* 2019.** Disponível em: < https://www.pwc.com.br/pt/estudos/setores-atividades/financeiro/2020/fintech_deep_dive_pwc_fintechs_2019.pdf >. Acesso em: 13 set. 2020.

PRICE WATERHOUSE COOPERS (PWC). **Plano Nacional de Internet das Coisas - Decreto Federal nº 9.854/2019.** Disponível em: < https://www.pwc.com.br/pt/sinopse-legislativa/outros-assuntos/plano-nacional-internet-coisas-decreto-federal-9854-2019.html>. Acesso em: 13 set. 2020.

PRICE WATERHOUSE COOPERS (PWC). **Tendências do setor de bancos e mercado de capitais em 2020: lançando as bases para o crescimento.** Disponível em: < https://www.pwc.com.br/pt/estudos/setores-atividade/financeiro/2020/tendencias-do-setor-de-bancos-e-mercado-de-capitais-em-2020-lancando-as-bases-para-o-crescimento.html>. Acesso em: 13 set. 2020.

RAFAEL, Luana GALETTI; SANTOS, Gabriel Teixeira. A ADVOCACIA E A PROTEÇÃO DE DADOS NA REVOLUÇÃO INDUSTRIAL DO SÉCULO XXI. **ETIC-ENCONTRO DE INICIAÇÃO CIENTÍFICA-ISSN 21-76-8498**, v. 15, n. 15, 2019.

Disponível em: < http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/7876/67648594>. Acesso em: 5 mar. 2020.

Regulamento Geral sobre a Proteção de Dados. In: Wikipédia: a enciclopédia livre. Disponível em: < https://pt.wikipedia.org/wiki/Regulamento_Geral_sobre_a_Prote%C3%A7%C3%A3o_de_Dados> Acesso em: 6 mar. 2020.

Revista CIAB - FEBRABAN. 2019. **Bancos dão a largada ao novo Cadastro Positivo.** Disponível em: < https://noomis.febraban.org.br/temas/regulacao/bancos-dao-a-largada-ao-novo-cadastro-positivo?pesquisa=nova-lei-do-cadastro-positivo>. Acesso em: 13 set. 2020.

Revista CIAB - FEBRABAN. 2019. **Sofisticação abre as portas para o 'banco das coisas'.** Disponível em: < https://noomis.febraban.org.br/temas/internet-das-coisas/sofisticacao-abre-as-portas-para-o-banco-das-coisas>. Acesso em: 13 set. 2020.

Revista CIAB - FEBRABAN. 2020. **A gestão dos riscos cibernéticos e a crise da covid-19.** Disponível em: < https://noomis.febraban.org.br/especialista/patricia-peck-pinheiro/a-gestao-dos-riscos-ciberneticos-e-a-crise-da-covid-19>. Acesso em: 26 jun. 2020.

Revista CIAB - FEBRABAN. 2020. **A IA irá potencializar a humanidade, não destruir.** Disponível em: < https://noomis.febraban.org.br/especialista/chris-skinner/a-ia-ira-potencializar-a-humanidade-nao-destruir>. Acesso em: 12 set. 2020.

Revista CIAB - FEBRABAN. 2020. **Brasil está atrasado na corrida por inteligência artificial.** Disponível em: < https://noomis.febraban.org.br/temas/inteligencia-artificial/brasil-esta-atrasado-na-corrida-por-inteligencia-artificial?pesquisa=prote%C3%A7%C3%A3o%20de%20dados>. Acesso em: 12 set. 2020.

Revista CIAB - FEBRABAN. 2020. **Brasil é vice em interações diárias de inteligência artificial no mundo.** Disponível em: < https://noomis.febraban.org.br/noomisblog/brasil-e-vice-em-interacoes-diarias-de-inteligencia-artificial-no-mundo?utm_source=newsletter&utm_medium=sub1&utm_campaign=noomisletter56>. Acesso em: 13 set. 2020.

Revista CIAB - FEBRABAN. 2020. **Brasileiros se preocupam com *fake news* e são dependentes da internet, mostra estudo.** Disponível em: < https://noomis.febraban.org.br/videos/brasileiros-se-preocupam-com-fake-news-e-sao-dependentes-da-internet-mostra-estudo?pesquisa=prote%C3%A7%C3%A3o%20de%20dados>. Acesso em: 19 out. 2020.

Revista CIAB - FEBRABAN. 2020. **Canais digitais respondem por 74% das transações bancárias em abril**. Disponível em: < https://noomis.febraban.org.br/temas/inovacao/canais-digitais-respondem-por-74-das-transacoes-bancarias-em-abril>. Acesso em: 26 jun. 2020.

Revista CIAB - FEBRABAN. 2020. **Como as financeiras devem se preparar para 2020:** o ano da LGPD. Disponível em: < https://noomis.febraban.org.br/especialista/patricia-peck-pinheiro/como-as-financeiras-devem-se-preparar-para-2020-o-ano-da-lgpd?pesquisa=nova-lei-do-cadastro-positivo>. Acesso em: 19 out. 2020.

Revista CIAB - FEBRABAN. 2020. **Data protection officer – quem é o nosso encarregado**. Disponível em: < https://noomis.febraban.org.br/especialista/renato-opice-blum/data-protection-officer-quem-e-o-nosso-encarregado>. Acesso em: 19 out. 2020.

Revista CIAB - FEBRABAN. 2020. **Fundo de investimento vai acelerar startups de IoT.** Disponível em: < https://noomis.febraban.org.br/noomisblog/fundo-de-investimento-vai-acelerar-startups-de-iot>. Acesso em: 13 set. 2020.

Revista CIAB - FEBRABAN. 2020. **Inovação e segurança devem ser inseparáveis no segmento financeiro.** Disponível em: <https://noomis.febraban.org.br/especialista/patricia-peck-pinheiro/inovacao-e-seguranca-devem-ser-inseparaveis-no-segmento-financeiro>. Acesso em: 26 jun. 2020.

Revista CIAB - FEBRABAN. 2020. **Lei de proteção de dados ganha confiança de consumidor, mas enfrenta despreparo das empresas.** Disponível em: < https://noomis.febraban.org.br/noomisblog/lei-de-protecao-de-dados-ganha-confianca-de-consumidor-mas-enfrenta-despreparo-das-empresas>. Acesso em: 19 out. 2020.

Revista CIAB - FEBRABAN. 2020. **LGPD em vigor: como a nova lei afeta as instituições financeiras.** Disponível em: < https://noomis.febraban.org.br/especialista/patricia-peck-pinheiro/lgpd-em-vigor-como-a-nova-lei-afeta-as-instituicoes-financeiras?pesquisa=nova-lei-do-cadastro-positivo>. Acesso em: 19 out. 2020.

Revista CIAB - FEBRABAN. 2020. **Novo mundo:** quais tendências vão te guiar? Disponível em: < https://noomis.febraban.org.br/especialista/gustavo-fosse/novo-mundo-quais-tendencias-vao-te-guiar?pesquisa=internet%20das%20coisas>. Acesso em: 13 set. 2020.

Revista CIAB - FEBRABAN. 2020. **Open banking:** cibersegurança e gestão de dados no Sistema Financeiro Aberto. Disponível em: < https://noomis.febraban.org.br/especialista/patricia-peck-pinheiro/open-banking-ciberseguranca-e-gestao-de-dados-no-sistema-financeiro-aberto?pesquisa=sigilo-bancario>. Acesso em: 19 out. 2020.

Revista CIAB - FEBRABAN. 2020. **O que era uma opção virou necessidade:** a transformação digital em tempos de pandemia! Disponível em: < https://noomis.febraban.org.br/especialista/alessandra-montini/o-que-era-uma-opcao-virou-necessidade-a-transformacao-digital-em-tempos-de-pandemia>. Acesso em: 29 ago. 2020.

Revista CIAB - FEBRABAN. 2020. **O que realmente significa transformação digital?** Disponível em: < https://noomis.febraban.org.br/especialista/chris-skinner/o-que-realmente-significa-transformacao-digital>. Acesso em: 26 jun. 2020.

Revista CIAB - FEBRABAN. 2020. **Treine bem seus algoritmos para evitar decisões tendenciosas.** Disponível em: < https://noomis.febraban.org.br/temas/inteligencia-artificial/treine-bem-seus-algoritmos-para-evitar-decisoes-tendenciosas>. Acesso em: 13 set. 2020.

RIBEIRO, Janete. **IoT e Leis de Privacidade.** ABINC. Disponível em: < https://abinc.org.br/iot-e-leis-de-privacidade/>. Acesso em: 13 set. 2020.

RIES, Eric. **A startup enxuta:** como os empreendedores atuais utilizam a inovação contínua para criar empresas extremamente bem-sucedidas. Tradução: Texto Editores. São Paulo: Lua de Papel, 2012. Disponível em: < https://edisciplinas.usp.br/pluginfile.php/4453282/mod_resource/content/1/a-startup-enxuta-eric-ries-livro-completo.pdf>. Acesso em: 26 jun. 2020.

ROBERTS, Edward. **Bad Bot Report 2020:** Bad Bots Strike Back. Imperva. Disponível em: < https://www.imperva.com/blog/bad-bot-report-2020-bad-bots-strike-back/>. Acesso em: 15 out. 2020.

RODRIGUES, Vivian Machado. Tecnologias 4.0 nos bancos e os impactos no emprego bancário. **Revista ciências do trabalho**: ISSN 2319-0574, nº 9, dez. 2017. Disponível em: < https://rct.dieese.org.br/index.php/rct/article/view/153/pdf>. Acesso em: 30 ago. 2020.

ROESCH, S. M. Azevedo. **Projetos de estágio e de pesquisa em Administração:** guia para estágios, trabalho de conclusão, dissertações e estudos de caso. 3.ed. São Paulo: Atlas, 2000.

ROGERS, David L. **Transformação digital:** repensando o seu negócio para a era digital. Tradução: Afonso Celso da Cunha Serra. 1º ed. São Paulo: Autêntica Business, 2019.

ROMAN, Juliana. **A proteção de dados pessoais na lei nº 13.709/2018:** uma análise sobre consentimento e direito à autodeterminação informativa na lei geral de proteção de dados. v.1, n.20, 2020. Disponível em: < http://ajuris.kinghost.net/OJS2/index.php/Anais-dos-Congressos/article/view/1090/632>. Acesso em: 19 out. 2020.

ROQUE, André. A TUTELA COLETIVA DOS DADOS PESSOAIS NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD). **Revista Eletrônica de Direito Processual**, v. 20, n. 2, 2019. Disponível em: < https://www.e-

publicacoes.uerj.br/index.php/redp/article/view/42138/30270>. Acesso em: 5 mar. 2020.

RUARO, Regina Linden; COELHO GLITZ, Gabriela Panfolfo. PANORAMA GERAL DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NO BRASIL E A INSPIRAÇÃO NO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS PESSOAIS EUROPEU. **Revista de Estudos e Pesquisas Avançadas do Terceiro Setor**, v. 6, n. 2 JUL/DEZ, p. 340-356, 2020. Disponível em: < file:///C:/Users/Cliente/Downloads/11545-51117-1-PB%20(1).pdf>. Acesso em: 5 mar. 2020.

RUBINI, Agustin. **A Fintech em um Flash**. Tradução: Fernanda Belokurows. Babelcube Inc., 2017. Livro eletrônico, não paginado.

RUSSELL, Stuart J.; NORVIG, Peter. **Inteligência Artificial.** Tradução: Regina Célia Simille. 3.ed. Rio de Janeiro: Elsevier, 2013. Livro eletrônico, não paginado.

SALESFORCE. **O que é CRM?** Disponível em: < https://www.salesforce.com/br/crm/#crm-definicao-e-conceitos-scroll-tab>. Acesso em: 24 out. 2020.

SANTANDER. **Política de segurança da informação para correspondente bancário do Santander.** Disponível em: < https://www.santander.com.br/document/wps/politica_seguranca_informacao_fev_13.pdf>. Acesso em: 12 set. 2020.

SANTOS, Pedro Miguel Pereira. **Internet das coisas:** o desafio da privacidade. Dissertação (mestrado em sistemas de informação organizacionais) – Escola Superior de Ciências Empresariais, Instituto Politécnico de Setúbal, Setúbal, 2016. Disponível em: < https://comum.rcaap.pt/bitstream/10400.26/17545/1/Disserta%C3%A7%C3%A3o%20Pedro%20Santos%20140313004%20MSIO.pdf>. Acesso em: 09 set. 2020.

SANTOS, Viviane Bezerra de Menezes. **Lei Geral de Proteção de Dados:** fundamentos e *Compliance*. 2019. Disponível em: < http://repositorio.ufc.br/bitstream/riufc/49370/1/2019_tcc_vbmsantos.pdf>. Acesso em: 05 mar. 2020.

SARAIVA FILHO, Oswaldo Othon de Pontes; GUIMARÃES, Vasco Branco. **Sigilos bancário e fiscal:** homenagem ao Jurista José Carlos Moreira Alves. 2. ed. revista e ampliada. Belo Horizonte: Fórum, 2015.

SARTORI, Adriana. ***Compliance* digital e LGPD:** tudo para seu escritório praticar. 2019. Disponível em: < https://blog.sajadv.com.br/compliance-digital-e-lgpd/>. Acesso em: 29 mar. 2020.

SENADO FEDERAL. **Lei Geral de Proteção de Dados entra em vigor**, publicado em Agência Senado. 2020. Disponível em: < https://www12.senado.leg.br/noticias/materias/2020/09/18/lei-geral-de-protecao-de-dados-entra-em-vigor>. Acesso em: 19 out. 2020.

SENADO FEDERAL. **Projeto do governo cria marco legal das startups e do empreendedorismo inovador**, publicado em Agência Senado. 2020. Disponível em: < https://www12.senado.leg.br/noticias/materias/2020/10/21/projeto-do-governo-cria-marco-legal-das-startups-e-do-empreendedorismo-inovador>. Acesso em: 13 set. 2020.

SERPRO. **O que muda com a LGPD.** Disponível em: < https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd>. Acesso em: 13 set. 2020.

SIMPLY. **Banco digital:** o desafio para o setor financeiro. Disponível em: < https://blog.simply.com.br/banco-digital-desafio-setor-financeiro/>. Acesso em: 26 jun. 2020.

SIMPLY. **Desmistificando a inteligência artificial.** Disponível em: < https://rdstation-static.s3.amazonaws.com/cms%2Ffiles%2F18483%2F1590000458Ebook_Inteligncia_Artificial.pdf>. Acesso em: 12 set. 2020.

SIMPLY. **Nove tendências tecnológicas para 2021.** Disponível em: < https://d335luupugsy2.cloudfront.net/cms%2Ffiles%2F18483%2F1605271418Ebook_Tendncias_Tecnolgicas_2021.pdf>. Acesso em: 19 out. 2020.
SIMPLY. **Tecnologia Bancária 2020:** evolução do setor e impacto do Covid-19. Disponível em: < https://blog.simply.com.br/tecnologia-bancaria-2020/>. Acesso em: 12 set. 2020.

SIMPLY. **Tendências do mercado financeiro para 2020.** Disponível em: < https://rdstation-static.s3.amazonaws.com/cms%2Ffiles%2F18483%2F1578600779Ebook_Tendncias_do_Mercado_Financeiro_Para_2020.pdf >. Acesso em: 26 jun. 2020.

SOARES, Matias Gonsales. **A Quarta Revolução Industrial e seus possíveis efeitos no direito, economia e política.** Disponível em: < https://migalhas.uol.com.br/arquivos/2018/4/art20180427-05.pdf>. Acesso em: 30 ago. 2020.

SOLOVE. Daniel J. **Privacy Self-Management and the Consent Dilemma.** LinkedIn. Disponível em: < https://www.linkedin.com/pulse/20130521143630-2259773-my-new-article-privacy-self-management-and-the-consent-dilemma>. Acesso em: 19 out. 2020.

SCHWAB, Klaus. **A quarta revolução industrial.** Tradução: Daniel Moreira Miranda. São Paulo: Edipro,2016.

SCHWAB, Klaus; DAVIS, Nicholas. **Aplicando a quarta revolução industrial**. Tradução: Daniel Moreira Miranda. São Paulo: Edipro, 2018.

SHARDA, Ramesh; DELEN, Dursun; TURBAN, Efraim. ***Business intelligence* e análise de dados para gestão do negócio.** Tradução: Ronald Saraiva de Menezes. 4.ed. Porto Alegre: Bookman, 2019.

SNEADER, Kevin; STERNFELS, Bob From surviving to thriving: reimagining the post-covid-19 return. **McKinsey & Company.** Disponível em: < https://www.mckinsey.com/featured-insights/future-of-work/from-surviving-to-thriving-reimagining-the-post-covid-19-return/pt-br>. Acesso em: 19 out. 2020.

STRAFACCI, Gilberto. **Um resumo do cenário da Transformação Digital no Brasil.** Disponível em: <https://www.setecnet.com.br/artigo-um-resumo-do-cenario-da-transformacao-digital-no-brasil/>. Acesso em: 26 ago. 2020.

SWINHOE, Dan. **11 biggest cybersecurity M&A deals in 2020.** CSO. Disponível em: < https://www.csoonline.com/article/3574730/10-biggest-cybersecurity-manda-deals-in-2020.html>. Acesso em: 15 out. 2020.

TAVARES, Nathália. **O que podemos concluir do Brazil Digital Report.** Disponível em: < https://troposlab.com/brazil-digital-report/>. Acesso em: 24 out. 2020.

TECNOBLOG. **Exclusivo:** Akamai vê uso de internet crescer 112% no Brasil durante pandemia. Disponível em: < https://tecnoblog.net/344896/exclusivo-akamai-ve-uso-de-internet-crescer-112-no-brasil-durante-pandemia/>. Acesso em: 13 set. 2020.

TEIXEIRA, Márcio Andrey. **Normas ISO 27000.** Instituto Federal de São Paulo, 2020. Disponível em: < http://200.133.218.36:8005/si-2020/Aula.04-SEG_ISO_27000_NormasSI_MA.pdf>. Acesso em: 12 set. 2020.

TEIXEIRA, Tarcísio. **Empresas e a implementação da Lei Geral de Proteção de Dados.** 1.ed. Salvador: Editora JusPodivm, 2021.

TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei geral de proteção de dados pessoais:** comentado artigo por artigo. 2.ed. ver., atual e ampl. Salvador: Editora JusPodivm, 2020.

TEIXEIRA, Tarcísio; LOPES, Alan Moreira; TAKADA, Thalles. **Manual jurídico da inovação e das startups.** 2.ed. Salvador: Editora JusPodivm, 2020.

TESSARINI, Geraldo; SALTORATO, Patrícia. Impactos da indústria 4.0 na organização do trabalho: uma revisão sistemática da literatura. **Revista Produção Online**, Florianópolis, SC, v. 18, n. 2, p. 743-769, jun. 2018. ISSN 16761901. Disponível em: < https://www.producaoonline.org.br/rpo/article/view/2967/1678>. Acesso em: 24 out. 2020.

TIGRE, Paulo Bastos; PINHEIRO, Alessandro Maia. **Inovação em serviços na economia do compartilhamento.** São Paulo: Saraiva Educação, 2019.

TI INSIDE ONLINE. **Senado aprova projeto de lei de incentivo para IoT**. Disponível em: < http://www.ihu.unisinos.br/78-noticias/591067-inteligencia-artificial-a-servico-da-especulacao-financeira>. Acesso em: 20 nov. 2020.

TOLCACHIER, Javier. Inteligência artificial a serviço da especulação financeira. **Instituto Humanista UNISINOS,** São Leopoldo, 25 jul. 2019. Disponível em: < http://www.ihu.unisinos.br/78-noticias/591067-inteligencia-artificial-a-servico-da-especulacao-financeira>. Acesso em: 09 set. 2020.

TOP-DIREITO DO MERCADO DE VALORES MOBILIARIOS. Comissão de Valores Mobiliários, Comitê - Consultivo de Educação. 1º ed. Rio de Janeiro: CVM, 2017. Disponível em: < https://www.investidor.gov.br/portaldoinvestidor/export/sites/portaldoinvestidor/publicacao/Livro/Livro_top_Direito.pdf>. Acesso em: 26 jun. 2020.

TOP-DIREITO DO MERCADO DE VALORES MOBILIARIOS. Comissão de Valores Mobiliários, Comitê - Consultivo de Educação. 4º ed. Rio de Janeiro: CVM, 2019. Disponível em: < https://www.investidor.gov.br/portaldoinvestidor/export/sites/portaldoinvestidor/publicacao/Livro/livro_TOP_mercado_de_valores_mobiliarios_brasileiro_4ed.pdf>. Acesso em: 26 jun. 2020.

TUMELERO, Thays. **Por que a privacidade importa tanto?** Disponível em: < https://www.nsctotal.com.br/noticias/por-que-a-privacidade-importa-tanto>. Acesso em: 19 out. 2020.

THALESGROUP. **Relatório de Ameaças de Dados Thales de 2020.** Disponível em: < https://www.thalesgroup.com/en/group/journalist/press-release/global-cloud-tipping-point-2020-thales-data-threat-report-global>. Acesso em: 27 jul. 2020.

THOMSON REUTERS. Veja as mudanças que a Quarta Revolução Industrial traz para o mundo. **Thomson Reuters**, São Paulo, dez. 2019. Disponível em: < https://www.dominiosistemas.com.br/blog/industria-4-0-qual-sera-seu-impacto-na-transformacao-digital/>. Acesso em: 24 out. 2020.

TRIPULAÇÃO ET. **Transformação digital:** o futuro dos bancos. Disponível em: < https://estrategiasquetransformam.com.br/transformacaodigital/transformacao-digital-o-futuro-dos-bancos/>. Acesso em: 24 out. 2020.

UPX. ***Fintechs* e segurança da informação:** por que investir? Disponível em: < https://www.upx.com/post/fintechs>. Acesso em: 24 out. 2020.

VELLOZA ADVOGADOS. **Novas regras para abertura, manutenção e encerramento de contas de depósito.** NEWS BANCÁRIO Nº 534. Disponível em: < http://velloza.com.br/blog/arquivos/news/news-bancario-no-534>. Acesso em: 24 out. 2020.

VERDASCA, Guilherme. **Por que se preocupar com segurança digital?** Conexão Fintech. Disponível em: < https://www.conexaofintech.com.br/fintech/por-que-se-preocupar-com-seguranca-digital/>. Acesso em: 13 set. 2020.

VERGARA, Sylvia Constant. **Projetos e relatórios de pesquisa em administração.** 8. ed. São Paulo: Atlas, 2006.

VERGILI, Gabriela Machado. **Análise comparativa entre direito à privacidade e direito à proteção de dados pessoais e relação com o regime de dados públicos previsto na Lei Geral de Proteção de Dados.** Disponível em: < https://dataprivacy.com.br/analise-comparativa-entre-direito-a-privacidade-e-direito-a-protecao-de-dados-pessoais-e-relacao-com-o-regime-de-dados-publicos-previsto-na-lei-geral-de-protecao-de-dados/>. Acesso em: 19 out. 2020.

VIEIRA, Nathan. **Principais ameaças cibernéticas apontadas pelo Fórum Econômico Mundial para 2020.** Disponível em: < https://canaltech.com.br/seguranca/principais-ameacas-ciberneticas-apontadas-forum-economico-mundial-2020-161647/>. Acesso em: 24 out. 2020.

WANDSCHEER, Lucelaine dos Santos Weiss; JARUDE, Jamile Nazaré Duarte Moreno; VITA, Jonathan Barros. O SISTEMA FINANCEIRO ABERTO (OPEN BANKING) SOB A PERSPECTIVA DA REGULAÇÃO BANCÁRIA E DA LEI GERAL DE PROTEÇÃO DE DADOS. **Revista Brasileira de Filosofia do Direito**, v. 6, n. 1, p. 78-95, 2020. Disponível em: < https://www.indexlaw.org/index.php/filosofiadireito/article/view/6455/pdf>. Acesso em: 24 out. 2020.

WEIBLEN, Tobias; CHESBROUGH, Henry W. Engaging with startups to enhance corporate innovation. California Management Review, v. 57, n. 2, p. 66-90, 2015.

WORLD ECONOMIC FORUM. **The Global Risks Report 2020**. 15.ed. Disponível em: < http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf>. Acesso em: 15 out. 2020.

ANEXO A – MEMORANDO ANBIMA

Para devida compreensão do tema, faz-se necessário apresentar, questões supostamente relevantes de um memorando elaborado a pedido da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (ANBIMA), que tem por objetivo analisar determinados aspectos relacionados à Lei Geral de Proteção de Dados (“LGPD”) e à Lei Complementar 105, de 10 de janeiro de 2001 (“Lei de Sigilo Bancário” ou “LC 105/01”), vis-à-vis as regras de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (“PLDFT”), conforme questionário encaminhado pela ANBIMA, aos escritórios Pinheiro Neto Advogados e Mattos Filho para devido esclarecimento. Dessa forma, a análise realizada, pelos escritórios, foi feita com base nas primeiras impressões a respeito do tema e as discussões travadas até o momento. Trata-se de matéria dinâmica que deverá ser revisitada pela ANBIMA, caso surjam novas interpretações da LGPD pela futura Autoridade Nacional de Proteção de Dados. Por sua vez, será apresentado, de forma resumida, as respostas e considerações, às questões formuladas pela ANBIMA, conforme se verá a seguir.

Questão nº1: A Lei de Sigilo Bancário se aplica às gestoras de recursos?

Conforme já mencionado, a Lei Complementar nº 105/01 (Lei de Sigilo Bancário), estabelece que: (a) são consideradas instituições financeiras (art. 1º, § 1º), e estão sujeitas às disposições da Lei, e (b) não se enquadram no conceito de “instituição financeira”, mas que devem obedecer às disposições da referida lei (art. 1º, § 2º). Assim, as gestoras de recursos, devidamente registradas na CVM nos termos da Instrução da Comissão de Valores Mobiliários (“CVM”) nº 558, de 26 de março de 2015, a qual estabelece, em seu artigo 21, incisos I e III, a obrigação de gestoras de recursos em (i) assegurar o controle de informações confidenciais a que tenham acesso os administradores, empregados e colaboradores da gestora de recursos; assim como de (ii) implantar e manter programa de treinamento de administradores, empregados e colaboradores que tenham acesso a informações confidenciais, participem de processo de decisão de investimento ou participem de processo de distribuição de cotas de fundos de investimento. Em outras palavras, via de regra, a LC 105/01 não deve se aplicar às gestoras de recursos. A despeito da não aplicabilidade da Lei de Sigilo Bancário, ressalta-se que tais entidades estão sujeitas a uma série de obrigações de sigilo e confidencialidade dos dados

cadastrais de investidores e cotistas de fundos de investimentos, tratados pelas gestoras de recursos no desenvolvimento de suas atividades, conforme a Instrução CVM 558.

Questão nº2: A Lei de Sigilo Bancário se aplica entre os prestadores de serviços do fundo de investimento?

Conforme anteriormente mencionado, entende-se que o rol de entidades sujeitas às disposições da Lei de Sigilo Bancário é taxativo. Dessa forma, a regra geral estabelecida pela Lei de Sigilo Bancário é que as entidades referidas (art. 1º, §§ 1º e 2º) devem manter o sigilo das operações ativas e passivas e serviços contratados por seus clientes. Assim, se os prestadores de serviços do fundo de investimento não forem instituições financeiras ou identificados no rol de entidades mencionadas, a Lei de Sigilo Bancário não deve ser aplicável a tais prestadores. A despeito de não haver uma orientação do CMN e/ou do BACEN nesse sentido, entende-se que há argumentos para defender que o dever de sigilo estabelecido pela Lei de Sigilo Bancário se refere aos dados transacionais de clientes (operações ativas e passivas e serviços prestados) e não a dados cadastrais dos clientes (tais como nome, endereço residencial, CPF, etc.), fornecidos pelos clientes às entidades sujeitas às disposições da Lei de Sigilo Bancário. Isso porque as atividades que envolvem o tratamento de dados pessoais no Brasil – o que inclui, para os fins da presente análise, o compartilhamento de dados cadastrais de clientes – serão regidas pelas disposições da LGPD. Não obstante, ressalta-se que não se trata de posição uniforme ou mesmo consolidada na jurisprudência, razão pela qual ressalta-se a possibilidade de entendimento diverso. Fora dessas hipóteses, a Lei de Sigilo Bancário não se aplica a outros prestadores de serviços de fundos de investimento. Em adição, vale lembrar que a Lei de Sigilo Bancário estabelece algumas hipóteses que não caracterizam violação do dever de sigilo (art. 1º, § 3º), cabe, aqui, destacar duas em especial: (i) a troca de informações entre instituições financeiras, para fins cadastrais, inclusive por intermédio de centrais de risco, observadas as normas baixadas pelo CMN e pelo Banco Central do Brasil (“BACEN”); (ii) a revelação de informações sigilosas com o consentimento expresso dos interessados. Dito isso, poder-se-ia concluir que se entende ser possível argumentar que o compartilhamento de dados no âmbito da Lei de Sigilo Bancário seria referente a dados transacionais (entre instituições financeiras ou entre uma instituição financeira e terceiros com respaldado no consentimento do cliente, independentemente da

finalidade do referido compartilhamento). Por sua vez, entende-se que o eventual compartilhamento de dados pessoais (entre instituições financeiras, exclusivamente para fins cadastrais, pode ser respaldado, sem a necessidade de obtenção de consentimento do cliente) em uma das bases legais estabelecidas pela LGPD para ser legalmente realizado.

Questão nº3: Fundo de investimento "A" é registrado no Brasil e sua carteira de investimentos é gerida pelo gestor de recursos "X". O gestor "X" também atua como distribuidor das cotas do fundo "A", conforme autorizado pela Instrução CVM 558.

3A- O compartilhamento de dados pessoais de seus clientes (que são cotistas do fundo "A") por "X" (na qualidade de distribuidor) com os demais prestadores de serviços do fundo "A", para fins de identificação do beneficiário final (de acordo com a legislação e regulamentação de PLDFT), pode ser respaldado pela LGPD (i.e., existe base legal que justificaria tal compartilhamento)?

A Lei Geral de Proteção de Dados (Lei nº 13.709/18 – "LGPD") estabelece um rol taxativo de hipóteses que justificam o tratamento de dados pessoais (art.7º, LGPD), sendo de particular interesse para esta análise três delas: (a) o consentimento; (b) o cumprimento de obrigação legal ou regulatória; e (c) o legítimo interesse. No que tange a dados pessoais sensíveis, a LGPD, também, estabelece um rol taxativo de hipóteses que justificam o tratamento de tais dados (art.11, LGPD). Nos termos da LGPD, o controlador de dados deve avaliar cuidadosamente qual base legal deve ser adotada para justificar uma dada atividade de tratamento de dados pessoais, considerando as características e as peculiaridades da referida atividade no caso concreto. O compartilhamento de dados pessoais de clientes (que incluem seus dados cadastrais) pelo distribuidor com os demais prestadores de serviços do fundo se enquadra como uma das atividades de tratamento de dados que deve ser respaldada em uma das bases legais previstas na LGPD para ser legalmente realizada. Assim sendo, pode-se sustentar que a base legal "cumprimento de obrigação legal ou regulatória", prevista no arts. 7, II e 11, II, "a", da LGPD, permite tal compartilhamento. Ressalta-se, entretanto, que a referida base legal somente pode ser adotada para justificar o compartilhamento de dados pessoais (incluindo os dados cadastrais) dos clientes do distribuidor que sejam necessários para fins cadastrais. Nesse sentido, recomenda-se que o distribuidor observe a razoabilidade do repertório de dados pessoais (incluindo os dados

cadastrais) a ser compartilhado com os demais prestadores de serviços do fundo de investimento, o qual deve ter relação direta e necessária com o cumprimento das obrigações impostas pela Instrução CVM nº 617/19 e/ou da Circular BACEN nº 3.978/20, a tais prestadores de serviços. Há, conhecimento de que podem haver outras hipóteses de compartilhamento de dados pessoais (incluindo dados cadastrais) dos clientes do distribuidor com outros prestadores de serviços do fundo, as quais não guardam relação com as obrigações estabelecidas pela Instrução CVM nº 617/19 e/ou pela Circular BACEN nº 3.978/20. A esse respeito, recomenda-se que o controlador dos dados avalie a finalidade de tais hipóteses de compartilhamento de dados pessoais e o repertório de dados pessoais compartilhados para determinar, com precisão, qual será a base legal mais apropriada para respaldar tais atividades de compartilhamento de dados pessoais à luz da LGPD. Assim sendo, o compartilhamento dos dados necessários para fins de identificação do beneficiário final, nos termos da legislação aplicável, poderia ser justificado tanto pelo legítimo interesse do controlador, quanto de terceiros. De toda forma, apesar da possibilidade de utilização do legítimo interesse, considerando haver legislação específica que seria suficiente para justificar o compartilhamento por meio da base legal de cumprimento de obrigação legal ou regulatória, sugere-se não utilizar a base legal do legítimo interesse para esses casos. Vale dizer que o compartilhamento de dados cadastrais entre o Distribuidor e os demais prestadores de serviços deve ser respaldado pela assinatura de um contrato de transferência de dados, de modo a regular as responsabilidades entre as partes envolvidas.

3B- O compartilhamento de dados pessoais de seus clientes (que são cotistas do fundo “A”) por “X” (na qualidade de distribuidor) com os demais prestadores de serviços do fundo “A”, para fins de identificação do beneficiário final (de acordo com a legislação e regulamentação de PLDFT), pode ser respaldado pela Lei de Sigilo Bancário?

Para análise dessa questão é necessário distinguir dois cenários: (i) Cenário A: no qual os demais prestadores de serviços do fundo “A” são instituições sujeitas à Lei de Sigilo Bancário, conforme discutido nos comentários à questão 1 acima; e (ii) Cenário B: no qual os demais prestadores de serviços do fundo “A” não são instituições sujeitas à LC 105/01, conforme discutido. No caso do Cenário A, a LC 105/01 em seu artigo 1º, §3º, I estabelece que: “não constitui violação do dever de sigilo 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". Nesse sentido, nos termos do dispositivo legal transcrito e assumindo que os demais prestadores de serviços do fundo "A" são instituições financeiras ou instituições equiparadas a instituições financeiras, para fins da Lei de Sigilo Bancário, entende-se pela possibilidade do compartilhamento de dados pessoais dos clientes por "X", na qualidade de distribuidor. Em relação ao Cenário B, isto é, assumindo que os demais prestadores de serviços do fundo "A" não estejam sujeitos ao cumprimento do dever de sigilo de que fala a LC 105/01, à primeira vista a resposta à possibilidade de compartilhamento seria negativa pela ausência de previsão legal ou regulamentar permitindo a quebra do dever de sigilo bancário. Contudo, dado que a leitura do artigo 1º da LC 105/01 prescreve a manutenção do sigilo sobre "operações ativas e passivas e serviços prestados", e não há uma definição clara acerca de quais dados seriam considerados sigilosos no âmbito de uma relação comercial e, portanto, abarcados pelo dispositivo, abre-se margem para discussão a respeito de quais informações estão abarcadas pela lei. Verifica-se, sobretudo, divergência quanto à aplicabilidade do conceito de sigilo bancário aos dados cadastrais, informações não relacionadas diretamente com movimentações ou operações financeiras junto às instituições financeiras. Nesse sentido, é possível identificar, em especial, dois posicionamentos jurisprudenciais e doutrinários expostos a seguir. O primeiro (i) defende que o conceito de sigilo bancário atinge todos os dados relacionados às operações e movimentações financeiras, incluindo os dados cadastrais dos clientes, enquanto o segundo (ii) acredita que informações cadastrais não estão protegidas por nenhuma das nuances que se buscou proteger por meio do sigilo bancário. Apesar de persistirem os posicionamentos jurisprudenciais e doutrinários expostos acima, o Superior Tribunal de Justiça ("STJ") entendeu, em decisão proferida em 2018, que dados cadastrais bancários de correntistas não estão protegidos pelo sigilo bancário, ao contrário dos dados relacionados aos serviços. Seguindo a linha argumentativa do precedente, há argumentos para defender a possibilidade do compartilhamento de dados cadastrais dos clientes por "X", na qualidade de distribuidor no Cenário B. Em todo caso, insta salientar que tais argumentos seriam prejudicados para se defender que informações cadastrais mais sensíveis e que envolvam relações de convivência privada não estão abarcadas pelo sigilo bancário – tais como: data de relacionamento com o cliente, interrupções de prestação de

serviços, razões pelas quais os serviços foram interrompidos, interesses e outros. Por último, vale também destacar o já mencionado artigo 1º, §3º da LC 105/01, que determina situações nas quais o fornecimento de informações sigilosos poderá ocorrer legalmente, dentre as exceções, há o consentimento expresso dos interessados. Em miúdos, o compartilhamento de informações, ante o Cenário B, também seria possível a partir da anuência concedida pelos quotistas, nos termos do artigo 1º, §3º, V da LC 105/01. A esse respeito, é importante compreender de que forma tal anuência poderá ser obtida, para fins de validade perante as autoridades. Idealmente, a autorização da parte interessada deve ser expressa no que diz respeito à divulgação de suas informações confidenciais e, ainda, ser feita com base em autorização específica, e não em autorização genérica dada pelo cliente ao iniciar a relação com a entidade obrigada ao sigilo. A despeito disso, não há indicação legal ou regulamentar sobre como exatamente esse consentimento deva ser manifestado. Por essa razão, e considerando precedentes próximos ao assunto na área consumerista, entende-se que no contexto de um contrato, a autorização deve ser realizada separadamente e de forma destacada (i) por meio de *check-box* com ênfase dos trechos principais em negrito, no qual o contratante possa clicar para manifestar seu consentimento, ou alternativamente, (ii) mediante disponibilização de termo e/ou contrato em apartado, tratando especificamente da referida anuência. Em termos práticos, a escolha da ferramenta para obtenção da anuência pode variar de acordo com o serviço prestado e depende do nível de conforto para comprovar o consentimento expresso do cliente, no caso de eventual questionamento. Além disso, salienta-se que, mesmo nas situações em que a instituição está autorizada a promover a quebra do sigilo, é fundamental que todas as providências necessárias à defesa dos interesses de seus clientes devem ser observadas, cabendo à instituição selecionar com cuidado as informações a serem compartilhadas e verificar se todos os requisitos legais para o compartilhamento foram cumpridos. Vale dizer que o compartilhamento de dados entre o Distribuidor e os demais prestadores de serviços deve ser respaldado pela assinatura de um contrato de transferência de dados, de modo a regular as responsabilidades entre as partes envolvidas.

Questão nº4: Fundo de investimento "A" é registrado no Brasil. Fundo de investimento "B" é registrado no Brasil e investe seus recursos integral ou majoritariamente em cotas do fundo "A".

4A - O compartilhamento de dados pessoais dos cotistas pelos prestadores de serviços do fundo "B" com os prestadores de serviços do fundo "A", para fins de identificação do beneficiário final (de acordo com a legislação e regulamentação de PLDFT), pode ser respaldado pela LGPD (i.e., existe base legal que justificaria tal compartilhamento)?

Sob a perspectiva da LGPD, entende-se que a situação exposta neste item 4 tem fundamentação jurídica e conclusão similares à resposta exposta no item 3.A, com base nos mesmos argumentos, as bases legais do consentimento, do cumprimento de obrigação legal ou regulatória e do legítimo interesse poderiam ser utilizadas para justificar tal compartilhamento. Tal como o distribuidor de cotas do fundo de investimento retratado no item 3.A, os prestadores de serviços do fundo "B" e do fundo "A" se enquadram na definição de "Prestadores de Serviços no Mercado de Valores Mobiliários" e, portanto, são obrigados a observar a legislação e regulamentação de PLDFT, incluindo, mas sem se limitar, ao cumprimento das obrigações de cadastro e identificação dos beneficiários finais de um determinado investidor (i.e., cotista do fundo de investimento), nos termos dos arts. 11 e seguintes da Instrução CVM nº 617/19 e/ou pela Circular BACEN nº 3.978/20. Porém, este é o caso, por exemplo, do compartilhamento de dados entre o gestor de recursos (que não atua como distribuidor de cotas do fundo de investimento do qual é gestor) e os demais prestadores de serviços do fundo, para fins que não guardam relação com o cumprimento das regras de PLDFT impostas ao referido gestor. A esse respeito, recomenda-se que o controlador dos dados avalie a finalidade de tais hipóteses de compartilhamento de dados pessoais e o repertório de dados pessoais compartilhados para determinar, com precisão, qual será a base legal mais apropriada para respaldar tais atividades de compartilhamento de dados pessoais à luz da LGPD.

4B- O compartilhamento de dados pessoais dos cotistas pelos prestadores de serviços do fundo "B" com os prestadores de serviços do fundo "A", para fins de identificação do beneficiário final (de acordo com a legislação e regulamentação de PLDFT), pode ser respaldado pela Lei de Sigilo Bancário?

Conforme discutido nas questões 1 e 2, o primeiro passo para se conseguir identificar a aplicabilidade da Lei de Sigilo Bancário é saber se os prestadores de serviços sejam do fundo “A” ou “B” são destinatários da referida lei. Assim, caso tais prestadores sejam (i) instituições financeiras; ou (ii) instituições equiparadas a tal para fins da LC 105/01, conforme rol taxativo descrito no artigo 1º, §§ 1º e 2º da LC 105/01, é possível encontrar respaldo na lei para a troca de informações entre as duas instituições, para fins cadastrais, conforme excetua o §3º, I do artigo 1º da LC 105/01. Ante hipótese contrária, caso os prestadores não sejam nenhuma das instituições indicadas em (i) e (ii) acima, não há falar em respaldo da Lei de Sigilo Bancário, por não ser esta aplicável. Vale notar a importância de documentar de maneira pormenorizada e formal o compartilhamento, quando permitido, de modo a construir prova de cumprimento das disposições legais em caso de questionamento por parte das autoridades.

Questão nº5: Fundo de investimento “A” é registrado no Brasil e investe integral ou majoritariamente em cotas de um fundo de investimento “B” (ou veículo de investimento similar) registrado no exterior.

5A. O compartilhamento de dados pessoais dos cotistas pelos prestadores de serviços do fundo “A” com os prestadores de serviços do fundo *offshore* “B”, para fins de cumprimento da legislação e regulamentação de PLDFT de outro país, pode ser respaldado pela LGPD (i.e., existe base legal que justificaria tal compartilhamento)?

Novamente, tal qual mencionado para a resposta 3.A, entende-se que, a depender de especificidades da operação, o compartilhamento poderia ser justificado pelas bases legais do consentimento, do cumprimento de obrigação legal ou regulatória, e do legítimo interesse. Esta hipótese, porém, traz alguma limitação à base legal do cumprimento de obrigação legal ou regulatória. Isso porque, não há na legislação brasileira qualquer obrigação aplicável ao fundo “A que determine o compartilhamento de informações para cumprimento de legislações de outras jurisdições. Desta forma, o que definirá a possibilidade de utilização dessa base legal será o fato de a legislação estrangeira ser ou não aplicável ao fundo “A”, ainda que indiretamente. Por exemplo, se houver na legislação estrangeira qualquer disposição no sentido de que, para se investir em fundos naquela jurisdição deve-se cumprir com as obrigações relacionadas à legislação de PLDFT local, ou contribuir com seu cumprimento pelo investido, poder-se-ia dizer que o fundo “A”, para investir

no fundo “B”, deve contribuir com suas obrigações de PLDFT e, portanto, seriam obrigações também aplicáveis ao fundo “A”. Nesses casos, poder-se-ia justificar tal compartilhamento pela base legal de cumprimento de obrigação legal ou regulatória. Se, por outro lado, a legislação estrangeira não for aplicável ao fundo “A”, enquanto investidor, entende-se que essa base legal não poderia ser utilizada. Isso porque, a LGPD determina que o cumprimento de obrigação legal ou regulatória deve se dar pelo controlador (que, neste caso, para fins de LGPD, é o fundo “A”), e, portanto, se a obrigação não se aplica a ele, não poderia justificar o cumprimento de obrigação legal de terceiros por meio dessa base legal. Nesses casos, apesar de não existir obrigação específica nesse assunto, recomenda-se que os titulares de dados sejam informados acerca da sujeição do fundo a tais normas e, portanto, das atividades de tratamento que dela decorrem, como boas práticas de transparência. Para tanto, recomenda-se a aplicação ao caso concreto da metodologia desenvolvida por doutrinadores europeus denominada de “teste de três partes”, ou *balancing test* para sopesamento de interesses, na ordem descrita abaixo: (i) identificar o interesse legítimo: a primeira etapa do teste consiste em verificar se é possível identificar um interesse do controlador ou de terceiros que seja legítimo; (ii) demonstrar que o tratamento é necessário para atingir esse interesse: em seguida, a segunda etapa do teste consiste em analisar se o tratamento de dados pessoais é necessário para a finalidade almejada pelo controlador de dados; e (iii) balancear o interesse com os direitos e liberdades individuais do titular dos dados: a terceira e última etapa do teste consiste em sopesar os interesses das partes, no sentido de verificar se os interesses do titular dos dados devem ou não prevalecer sobre o interesse do controlador. Por fim, a ANPD poderá solicitar a elaboração de um relatório de impacto à proteção de dados (*Data Protection Impact Assessment* – “DPIA”), que é recomendado nos casos em que o tratamento de dados pessoais possa gerar riscos às liberdades civis e aos direitos fundamentais do titular. Vale dizer, que por se tratar de uma transferência internacional de dados pessoais, sugere-se a adoção de BCRs ou cláusulas-padrão contratuais para regular tal transferência. Portanto, em não sendo possível utilizar a base legal do cumprimento de obrigação legal ou regulatória, o compartilhamento poderia ser justificado pelas bases legais do consentimento ou do legítimo interesse, desde que cumpridos os requisitos mencionados na resposta da pergunta 3A. Tal qual sugerido na resposta à pergunta 3A, entende-se que a utilização do legítimo interesse parece mais vantajosa, em

razão da possibilidade de revogação do consentimento e consequente cessação da atividade de tratamento.

5B- O compartilhamento de dados pessoais dos cotistas pelos prestadores de serviços do fundo “A” com os prestadores de serviços do fundo *offshore* “B”, para fins de cumprimento da legislação e regulamentação de PLDFT de outro país, pode ser respaldado pela Lei de Sigilo Bancário?

Conforme anteriormente mencionado, a Lei de Sigilo Bancário prevê a possibilidade de compartilhamento de dados entre instituições financeiras, para fins cadastrais, sem que isso seja considerado violação à obrigação de sigilo lá estabelecida. Diferentemente de outras legislações, o dispositivo não se refere a “instituições financeiras sediadas no Brasil” ou “instituições financeiras integrantes do Sistema Financeiro Nacional”, mencionando apenas “instituições financeiras”. Além disso, conforme disposto na resposta à pergunta 1 acima, entende-se possível defender que o compartilhamento de dados cadastrais não transacionais entre uma instituição financeira e uma outra entidade não financeira no exterior não viola a Lei de Sigilo Bancário. Considerando que o dispositivo da lei que permite o compartilhamento de dados, para fins cadastrais, entre instituições financeiras não estipula a necessidade de que essa troca de informações ocorra entre pessoas nacionais ou aqui estabelecidas, não há óbice para a hipótese de que troca ocorra com uma das partes localizada fora do território nacional. Nesse caso, deve-se verificar qual a base legal mais adequada para esse compartilhamento, a depender dos dados compartilhados e sua finalidade, nos termos da LGPD.

Questão nº6: 6A- Existem outras hipóteses de compartilhamento de dados pessoais dos cotistas entre os prestadores de serviços de um fundo de investimento, para fins de PLDFT, que poderiam ser respaldadas pela LGPD (i.e., existe(m) base(s) legal(is) que justificariam outras hipóteses de compartilhamento)?

Considerando especificamente atividades de tratamento previstas na regulação e, portanto, justificáveis por meio da base legal de cumprimento de obrigação legal ou regulatória, no âmbito da regulamentação da CVM, a própria Instrução CVM 617, assim como a Instrução CVM 505, permitem a realização de cadastro simplificado de investidor não-residente por intermediário estrangeiro, desde que observadas as disposições das correspondentes regras (as quais envolvem a troca de informações entre Prestadores de Serviço com Obrigação de

Cadastro e o intermediário estrangeiro). No âmbito do Banco Central, por sua vez, a Circular nº 3.978, de 23 de janeiro de 2020 (“Circular nº 3.978/20”) permite situações como: (i) a realização de comunicações por meio do Sistema de Controle de Atividades Financeiras (Siscoaf) de forma centralizada por meio de instituição do conglomerado prudencial, em nome da instituição na qual ocorreu a operação; e (ii) nos casos de relação de negócio com cliente residente no exterior, que também seja cliente de instituição do mesmo grupo no exterior, fiscalizada por autoridade supervisora com a qual o Banco Central mantenha convênio para a troca de informações, admite-se que as informações relativas ao beneficiários final e pessoa exposta politicamente sejam obtidas da instituição no exterior, desde que assegurado o acesso à autoridade monetária das informações e procedimentos adotados. Essas hipóteses se encaixam na base legal de “cumprimento de obrigação legal ou regulatória”, prevista no arts. 7, II e 11, II, “a”, da LGPD. Em relação a outras atividades de tratamento, seria necessário entender com mais profundidade os dados que se pretende compartilhar e as respectivas finalidades para que se possa identificar se há ou não a possibilidade de justificar tal tratamento por meio de uma ou mais bases legais da LGPD.

6B- Existem outras hipóteses de compartilhamento de dados pessoais dos cotistas entre os prestadores de serviços de um fundo de investimento, para fins de PLDFT, que poderiam ser respaldadas pela Lei de Sigilo Bancário?

Além do compartilhamento entre instituições financeiras, para fins cadastrais, a outra hipótese de compartilhamento de dados transacionais entre entidades privadas (ou seja, excluindo-se o BACEN, a Secretaria da Receita Federal e outras autoridades) prevista na Lei de Sigilo Bancário seria mediante consentimento expresso dos clientes.

Questão nº7. A Instrução CVM nº 617/19 e a Circular BACEN nº 3.978/20 determinam que as instituições financeiras contem com mecanismos de compartilhamento de informações com áreas internas de conglomerados financeiros ou com clientes/parceiros que tenham relacionamento comercial direto com o cliente.

7A- No contexto de compartilhamento com entidades sediadas no exterior, quais critérios seguir para observar o disposto nos arts. 33 e seguintes da LGPD, dado que até o momento a Autoridade Nacional de Proteção de Dados não definiu o conteúdo das cláusulas padrão (art. 35)?

O compartilhamento de dados pessoais por entidades localizadas no Brasil com entidades sediadas no exterior configura uma transferência internacional de dados nos termos da LGPD e, por consequência, exige que os controladores de dados atendam a requisitos específicos. Dentre outras hipóteses, a LGPD estabelece que transferências internacionais de dados são permitidas nas hipóteses do artigo 33 da LGPD.[1] Parte dos mecanismos internacionais de transferência de dados elencados nesse artigo requer uma regulamentação adicional da ANPD. Apesar da ausência de diretrizes, para fins de demonstração de boas práticas e zelo com a legislação, o controlador de dados, ao compartilhar dados pessoais ou dados sensíveis com entidades localizadas no exterior pode se valer das seguintes condições: (i) quando a transferência for realizada com entidade integrante do seu grupo econômico, deve-se estabelecer normas corporativas vinculantes (*Binding Corporate Rules* – BCRs), que são disposições internas que se aplicam a todo conglomerado financeiro ou grupo econômico. Tais regras devem – como o próprio nome sugere – ser juridicamente vinculantes e aplicáveis a todas as entidades pertencentes ao conglomerado financeiro ou ao grupo econômico. Tão logo seja possível, as referidas normas corporativas globais devem ser submetidas à aprovação da ANPD e até que isso ocorra, as BCRs aprovadas pelas autoridades de proteção de dados europeia podem servir de uma boa referência; (ii) quando a transferência for realizada com entidade que não integre seu conglomerado

---

[1] Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;
II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:
a) cláusulas contratuais específicas para determinada transferência;
b) cláusulas-padrão contratuais;
c) normas corporativas globais;
d) selos, certificados e códigos de conduta regularmente emitidos;
III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;
IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;
V - quando a autoridade nacional autorizar a transferência;
VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;
VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou
IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

econômico, sugere-se a celebração de um contrato de compartilhamento de dados com as entidades receptoras dos dados por meio do qual essas entidades se comprometem a fornecer um nível de proteção de dados semelhante ao estabelecido pela LGPD e aceitem que o instrumento seja revisado em caso de mudanças na legislação ou regulação.

7B- Seria possível estabelecer antecipadamente à manifestação da ANPD algum padrão mínimo dessas cláusulas, para que as instituições financeiras já comecem a trabalhar em seus documentos?

Ao analisar as disposições das normas corporativas globais ou das cláusulas-padrão, a ANPD deverá considerar os requisitos, as condições e as garantias mínimas para a transferência internacional de dados, devendo observar os direitos, as garantias e os princípios da LGPD (art. 35, § 1º, LGPD).[2] Para além dessa disposição legal, a LGPD não estabelece orientações detalhadas a respeito do conteúdo das normas corporativas globais ou das cláusulas-padrão contratuais, tema que ficará a cargo da ANPD tão logo se torne uma entidade operacional. Todavia, tais cláusulas não poderiam, na ausência de manifestação da ANPD, ser consideradas como mecanismos válido de transferência internacional, tão somente como boas práticas.

Questão nº8: A Instrução CVM nº 617/19 e a Circular BACEN nº 3.978/20 determinam a coleta de informações pessoais de representantes legais de pessoas jurídicas para fins de PLDFT. Estas informações são entregues pelas pessoas jurídicas sem que as instituições financeiras tenham contato direto com estas pessoas naturais.

8A- Conquanto seja possível enquadrar a necessidade de coleta de tais dados em diversos dispositivos do art. 7º da LGPD (obrigação regulatória, legítimo interesse, necessário para a execução de contratos, etc.), quais seriam os cuidados ou pontos de atenção – se é que haveria algum – para as instituições financeiras em relação aos seus clientes (as pessoas jurídicas) no fornecimento de dados pessoais

---

[2] Art. 35. A definição do conteúdo de cláusulas-padrão contratuais, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, a que se refere o inciso II do caput do art. 33 desta Lei, será realizada pela autoridade nacional.
§ 1º Para a verificação do disposto no caput deste artigo, deverão ser considerados os requisitos, as condições e as garantias mínimas para a transferência que observem os direitos, as garantias e os princípios desta Lei.

de pessoas naturais com quem não têm relacionamento direto (os representantes legais dessas PJs)?

Ao tratar dados pessoais de representantes legais ou procuradores de clientes diretos da instituição financeira constituídos na forma de pessoa jurídica (“Clientes PJ”), poder-se-ia recomendar a adoção das seguintes medidas: (i) Transparência: a instituição financeira deve garantir que o titular tenha acesso a informações sobre as atividades de tratamento de dados envolvendo seus dados pessoais, bem como as respectivas finalidades. Tais informações devem ser inseridas na política de privacidade da instituição, a qual deve ser disponibilizada em local de fácil acesso (por exemplo, na página inicial do site da instituição), conforme o art. 18 da LGPD; (ii) Razoabilidade dos dados tratados: para que os interesses e direitos do titular dos dados sejam respeitados e não se sobreponham aos interesses da instituição financeira, esta última poderá tratar somente os dados pessoais estritamente necessários para a finalidade pretendida, os quais devem ser analisados no caso concreto, conforme art. 6º, inciso III, LGPD; (iii) Declarações do Cliente PJ: na hipótese dos dados pessoais do representante legal ou procurador serem compartilhados pelo Cliente PJ (ao invés de serem voluntariamente fornecidos pelo próprio titular dos dados), a instituição financeira pode contratualmente exigir que o Cliente PJ declare que (a) o compartilhamento dos dados pessoais do representante legal ou procurador é realizado de acordo com a LGPD, quer dizer, que o Cliente PJ possui legitimidade para fornecimento de tais dados, e (b) assume quaisquer responsabilidades pelo descumprimento da LGPD. Portanto, é importante que as instituições financeiras atuem para garantir transparência aos titulares de dados pessoais acerca da existência dessas atividades de tratamento. Considerando que não haverá relação direta com essas pessoas, sugere-se que as instituições considerem cláusulas específicas em seus contratos determinando que os clientes garantam transparência aos seus representantes legais acerca do compartilhamento de dados com as instituições financeiras, e as respectivas finalidades.

Questão nº9: A Instrução CVM nº 617/19 autoriza a realização de cadastro simplificado, pelo qual as informações cadastrais de clientes estrangeiros serão coletadas por intermediário estrangeiro com quem o intermediário brasileiro mantém contrato (obrigando o intermediário estrangeiro a realizar o cadastro dos clientes, enviar informações mínimas, e encaminhar outros dados a requerimento dos reguladores).

9A- Os direitos previstos na LGPD se aplicariam aos investidores não residentes que são cadastrados neste modelo (e que, portanto, não interagem diretamente com a entidade brasileira)?

Salvo algumas exceções (art. 4º), a LGPD se aplica a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, conforme art. 3º, LGPD. Assumindo que os dados pessoais do cliente estrangeiro são coletados pelo intermediário estrangeiro para fins cadastrais, são compartilhados com a entidade brasileira para fins cadastrais e posteriormente tratados pela entidade brasileira para as mais diversas finalidades (por exemplo, para fins relacionados à PLDFT) no Brasil, a LGPD se aplica à referida operação de tratamento de dados realizada pela entidade brasileira, a despeito da entidade brasileira não ter um relacionamento comercial direto com o cliente estrangeiro. Portanto, caberá à entidade brasileira assegurar os direitos dos titulares e observar os princípios e as demais disposições estabelecidas pela LGPD.

9B- Caso a resposta ao item anterior seja positiva, eles se aplicariam a todas as informações, ou apenas as que forem compartilhadas efetivamente com a entidade brasileira?

Considerando a situação fática deste item 9, a LGPD se aplica tão somente às atividades de tratamento de dados pessoais que forem realizadas no território brasileiro. Dessa forma, as disposições da LGPD se aplicam somente com relação aos dados pessoais de clientes estrangeiros que forem efetivamente compartilhados pelo intermediário estrangeiro com a entidade brasileira.