



**UNIVERSIDADE FEDERAL DO TOCANTINS**  
**PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO**  
**CÂMPUS DE PALMAS**  
**PROGRAMA DE PÓS-GRADUAÇÃO EM PROPRIEDADE INTELECTUAL E**  
**TRANSFERÊNCIA DE TECNOLOGIA PARA A INOVAÇÃO**

**MAURICIO CORDENONZI**

**O *COMPLIANCE* COMO FATOR DECISIVO DE CONTROLE NAS**  
**EMPRESAS DO SETOR BANCÁRIO PARA A ADAPTAÇÃO À LEI GERAL**  
**DA PROTEÇÃO DE DADOS**

Palmas, TO  
2023

**MAURICIO CORDENONZI**

**O *COMPLIANCE* COMO FATOR DECISIVO DE CONTROLE NAS EMPRESAS DO SETOR BANCÁRIO PARA A ADAPTAÇÃO À LEI GERAL DA PROTEÇÃO DE DADOS**

Dissertação apresentada ao Programa de Pós Graduação em Propriedade Intelectual e Transferência de Tecnologia para Inovação para obtenção do título de Mestre em Propriedade Intelectual e Transferência de Tecnologia para Inovação.

Orientador: Prof. Dr. Francisco Gilson Rebouças Porto Junior.

Palmas, TO  
2023

Dados da Catalogação *Anglo-American Cataloguing Rules* – AACR2

---

C794c

Cordenonzi, Mauricio

O *compliance* como fator decisivo de controle nas empresas do setor bancário para a adaptação à Lei Geral da Proteção de Dados [recurso eletrônico]. / Mauricio Cordenonzi. Palmas, TO: [S.n], 2023.  
224 f.; il. Color.

Dissertação (Mestrado Profissional em Propriedade Intelectual e Transferência de Tecnologia para a Inovação) – Universidade Federal do Tocantins (UFT) - Curso do Programa de Pós-Graduação em Propriedade Intelectual e Transferência de Tecnologia para a Inovação (Profnit), Palmas, TO, 2023.

Orientador: Prof. Dr. Francisco Gilson Rebouças Porto Junior.

1. Direito – proteção de dados. 2. *Compliance*. 3. Bancos - Clientes. 4. LGPD. I. Título.

CDD 332.1068  
CDU 347.734: 342.721(81)  
LCC KF6449.

---

Ficha Catalográfica elaborada por *Marcelo Neves Diniz* - CRB 2/1533.

[Resolução CFB nº 184, de 29 de setembro de 2017.](#)

TODOS OS DIREITOS RESERVADOS - A reprodução total ou parcial de qualquer forma ou por qualquer meio deste documento é autorizado desde que citada a fonte. A violação dos direitos do autor ([Lei nº 9.610/98](#)) é crime estabelecido pelo artigo 184 do Código Penal.

**MAURICIO CORDENONZI**

**O COMPLIANCE COMO FATOR DECISIVO DE CONTROLE NAS EMPRESAS DO SETOR BANCÁRIO PARA A ADAPTAÇÃO À LEI GERAL DA PROTEÇÃO DE DADOS**

Dissertação apresentada ao Programa de Pós-Graduação em Propriedade Intelectual e Transferência de Tecnologia para Inovação para obtenção do título de Mestre em Propriedade Intelectual e Transferência de Tecnologia para Inovação (PROFNIT), pela Universidade Federal do Tocantins.

Aprovada em:

**BANCA EXAMINADORA**

---

**Prof. Dr. Francisco Gilson Rebouças Porto Junior** (PROFNIT / UFT)

Orientador

---

**Prof<sup>ª</sup>. Dr<sup>ª</sup>. Marli Terezinha Vieira** (PROFNIT / UFT)

---

**Prof. Dr. Paulo Augusto Ramalho de Souza** (PROFNIT / UFMT)

---

**Prof<sup>ª</sup>. Dr<sup>ª</sup> Aracelis Gois Morales Rigoldi** (Pós-Doc PROFNIT / UFT)

## RESUMO

A Lei Geral de Proteção de Dados – Lei Federal 13.709/2018, trouxe extensas e significativas mudanças aos atores responsáveis pela coleta e tratamento de dados pessoais, entre elas as Instituições Financeiras. Nesse contexto, o setor de *compliance* (responsável, dentro da empresa, pelo estrito cumprimento das normas, internas e externas), foi profundamente afetado pela novel legislação, na medida e que precisou, em um curto espaço de tempo, adaptar-se aos inúmeros comandos na norma. Este projeto discorre sobre um estudo de caso, realizado no Banco da Amazônia, com o propósito de, sob a análise do novo conjunto de normativas, propor um novo modelo de *compliance*, ou seu aperfeiçoamento, para adaptação à Lei Geral da Proteção de Dados – LGPD. O objetivo do estudo é propor critérios sobre as exigências legais trazidas pela LGPD às empresas do setor bancário, de modo a identificar e especificar os procedimentos e opções práticas de *compliance* à implementação do tratamento de dados na nova realidade e inviabilizar, tanto possível, a aplicação de multas. O público alvo e sujeitos envolvidos na pesquisa foram pessoas da área jurídica, servidores e empregados públicos, profissionais de TI e auditores, em especial aqueles ligados ao setor bancário. A metodologia aplicada na pesquisa, além do estudo de caso, adota também procedimentos de cunho bibliográfico e documental partindo de um processo de revisão de literatura para compreender as exigências legais trazidas pela LGPD ao setor bancário, onde além de documentos oriundos do setor bancário, utilizados para análise de dados, adotou-se artigos, teses e dissertações encontrados em bases de dados científicas. Já quanto à abordagem de análise de dados, a pesquisa caracteriza-se como qualitativa, baseando-se na observação e compreensão dos ambientes em que os sistemas de *compliance* são utilizados para assim promover uma compreensão dos fenômenos da pesquisa. Como solução, propôs-se, para o aperfeiçoamento do atual modelo de *compliance*, a criação de uma nova Coordenação, para controle e gerenciamento de processos internos e externos, unicamente ligados ao tratamento de dados pessoais, a fim de otimizar tramitação e fluxo dos procedimentos, e mitigar, tanto quanto possível, os danos/multas decorrentes da norma. O estudo culminou na elaboração de um modelo de negócios CANVAS para o setor bancário, uma matriz SWOT, a produção de um relatório final onde foi possível apontar os gargalos existentes para propor um material didático para o modelo de *compliance* em forma de Manual de Aplicação da LGPD em Bancos.

Palavras-chave: *compliance*; LGPD; Banco da Amazonia; Tocantins (Estado).

## **ABSTRACT**

The General Data Protection Law - Federal Law 13.709/2018 brought extensive and significant changes to the actors responsible for the collection and processing of personal data, including Financial Institutions. In this context, the compliance sector (responsible, within the company, for strict compliance with internal and external rules) was deeply affected by the new legislation, as it needed to adapt to the numerous commands in the norm in a short period of time. This project discusses a case study, carried out at the Banco da Amazônia, with the purpose of, under the analysis of the new set of regulations, proposing a new compliance model, or its improvement, to adapt to the General Data Protection Law - LGPD. The objective of the study is to propose criteria on the legal requirements brought by the LGPD to companies in the banking sector, in order to identify and specify the practical compliance procedures and options for the implementation of data processing in the new reality, and to prevent, as much as possible, the application of fines. The target audience and subjects involved in the research were legal professionals, public servants and employees, IT professionals, and auditors, especially those linked to the banking sector. The methodology applied in the research, in addition to the case study, also adopts bibliographic and documentary procedures, starting from a literature review process to understand the legal requirements brought by the LGPD to the banking sector, where, in addition to documents from the banking sector used for data analysis, articles, theses, and dissertations found in scientific databases were used. Regarding the data analysis approach, the research is characterized as qualitative, based on observation and understanding of the environments in which compliance systems are used to promote an understanding of research phenomena. As a solution, it was proposed, for the improvement of the current compliance model, the creation of a new Coordination, for control and management of internal and external processes, solely related to the processing of personal data, in order to optimize the flow of procedures and mitigate, as much as possible, the damages/fines resulting from the norm. The study culminated in the elaboration of a CANVAS business model for the banking sector, a SWOT matrix, the production of a final report where it was possible to point out the existing bottlenecks to propose a didactic material for the compliance model in the form of a LGPD Application Manual in Banks.

**Keywords:** compliance; LGPD; Banco da Amazonia; Tocantins (State).

## SUMÁRIO EXECUTIVO

O trabalho aqui apresentado é um projeto de pesquisa, como requisito para a formação no mestrado Programa de Pós-Graduação em Propriedade Intelectual e Transferência de Tecnologia para a Inovação – PROFNIT, ponto focal da UFT – Universidade Federal do Tocantins. Como mestrado profissional, reclama, também, o desenvolvimento de um produto.

Nesse contexto, a fim de melhor detalhar à Banca Examinadora a concepção geral do projeto, e do produto que será gerado, abriu-se o presente tópico, na fase inicial do trabalho, onde se apresentará os objetivos que se visa alcançar/entregar, na seguinte ordem: i) tipos dos produtos; ii) aderência do projeto; iii) impacto do projeto proposto; iv) aplicabilidade dos produtos que serão gerados; v) grau de inovação e vi) grau complexidade dos produtos;

Pois bem.

Na definição feita pelo Banco da Amazônia, na POL 309 – Política de Compliance, logo no preâmbulo, define:

### **1 INTRODUÇÃO**

*A atividade de Compliance busca aperfeiçoar resultados e mitigar os riscos de conformidade, implementando através de mecanismos de controle e conformidade às Normas, Leis, Regulamentos, bem como as políticas e diretrizes internas da empresa. Esta política estabelece conceitos e aplicações de forma preventiva, detectando e orientando, garantindo assim de forma efetiva a melhoria contínua dos padrões de atuação, com ética, transparência e eficiência na operacionalização das atividades no contexto das três linhas.*

### **2 OBJETIVO**

*Esta Política tem o objetivo de estabelecer diretrizes e procedimentos a serem seguidos por todos os colaboradores, dirigentes e conselheiros e prestadores de serviços terceirizados relevantes do Banco da Amazônia, quanto às regras de Compliance, zelando pelo cumprimento de leis, regulamentações, políticas, normas internas e externas, procedimentos e princípios corporativos que regem a atividade da empresa.*

A atividade de conformidade, cuja existência é obrigatória dentro de uma Instituição Financeira (desde a edição da Resolução BACEN 2554/1998), atua de forma preventiva, e pró ativa, no sentido de certificar o cumprimento das normas internas e externas, e, com isso, evitar ou mitigar a possibilidade de infrações que possam causar danos financeiros ou reputacionais à empresa.

As novas exigências oriundas da Lei Geral de Proteção da Dados – Lei 13.709/2018, impuseram profundas modificações à área de conformidade. A partir da vigência da nova lei (término do período de vacância), não só os Bancos, mas todas as empresas que mantem em seus cadastros dados de particulares, devem se reestruturar, sob pena de pagar multas que pode chegar até cinquenta milhões de reais.

Então, o objetivo do trabalho, aqui proposto, é estudar a LGPD sob o aspecto das Instituições Financeiras, no caso o Banco da Amazônia S.A. (em um **estudo de caso**) e, a partir daí, apresentar um modelo aperfeiçoado de *compliance* que possibilite a adequação dos Bancos às novas exigências da norma.

#### **a) Tipo de produto a ser entregue**

A Portaria Normativa nº 17/2009 do Ministério da Educação, em seu art. 7º, parágrafo 3º, indica quais os modelos de produto final poderão ser apresentados como trabalho de conclusão final, entre eles os *relatórios finais de pesquisa*.

Com o término de todas as etapas da fase de pesquisa, será possível entregar, além da dissertação, um relatório técnico conclusivo, contendo os principais achados acerca das exigências da Lei Geral de Proteção de Dados – Lei 13.709/2018 aplicadas às Instituições Financeiras, e, em que nível o setor de *compliance* poderá ajudar nesta adaptação.

Além do Relatório Final, o projeto tencionava apresentar um *Código de Conduta, ou de Boas Práticas* aplicadas ao Setor Bancário, guiado a partir das inovações e exigências trazidas pela nova Lei de Dados. Este documento é parte integrante de um bom programa de conformidade, ideal e extremamente necessário para nortear a alta administração e os colaboradores das organizações frente à nova forma de tratar os dados pessoais no Brasil. Todavia, diante da extensão do trabalho, e da sua envergadura, esta etapa ficará reservada a um futuro projeto, artigo ou mesmo viabilização de um doutoramento, diante da criação de um produto inédito.

Com efeito, o projeto desenvolveu e apresentou, até o momento da qualificação 02 (dois) dos 03 (três) objetivos específicos propostos: (i) examinou e detalhou as exigências legais trazidas pela LGPD ao setor bancário, por meio de uma revisão de literatura, e; (ii) identificou os procedimentos e opções práticas de *compliance* à implementação do tratamento de dados ao setor bancário.

E, com a entrega da Dissertação, do Relatório Final e do Artigo, respondeu-se o terceiro e último objetivo específico, que é o aprimoramento o sistema de compliance aplicado ao sistema bancário, o qual contemple as normas inovadoras da LGPD, e proteja as empresas de futuros dissabores, considerando as punições dela decorrentes.

A solução final, proposta e apresentada neste trabalho, culminou na criação de um novo órgão, junto à Diretoria de Riscos do Banco da Amazônia, e que poderá ser desenvolvida em qualquer Instituição Financeira, exclusivamente responsável pela gestão de compliance ligada à Lei Geral de Proteção de Dados.

Como será demonstrado e provado, no transcorrer das exposições, a gestão dos dados pessoais e a própria gestão do compliance justificam a concepção de uma área independente, na medida em que o risco das sanções legais, decorrentes da Lei 13.709/2018, vão muito além das perdas financeiras. Há o risco, iminente, das perdas reputacionais derivadas da falta de cumprimento das Leis e normas regulamentadoras, e a perda da credibilidade junto ao mercado.

#### **b) Aderência do projeto:**

No programa de mestrado PROFNIT, a produção desenvolvida deve ser validada com o critério “aderência”, visto que os produtos deverão apresentar origens nas atividades oriundas das linhas de pesquisas/atuação e projetos vinculados às linhas do programa.

O projeto tem vinculação à inovação em processo e inovação organizacional, visto que propõe o aprimoramento do sistema aplicado ao setor bancário, no caso o *compliance*. A conclusão do trabalho, juntamente com o relatório técnico conclusivo, ao indicarem as eventuais deficiências do setor e, principalmente, apresentar um novo arcabouço de normas/regras com o objetivo de aprimorar sistema de *compliance* culmina em uma reestruturação da rede, tudo com o fito de proteger as empresas das punições decorrentes da norma. Insere-se, portanto, dentro do tema de Propriedade Intelectual (inovação em processo) e Transferência de Tecnologia.

#### **c) Impacto do projeto proposto:**

O PROFNIT é dedicado ao aprimoramento da formação profissional para atuar nas competências dos Núcleos de Inovação Tecnológica (NITs) e nos Ambientes Promotores de Inovação nos diversos setores (acadêmicos, empresarial, governamental, organizações sociais, entre outros), todos habitats naturais da inovação. Desta forma, o objetivo da pesquisa e os produtos dela decorrentes devem estar inseridos nesse contexto, e propor, minimamente, a alteração de um *status quo* existente, gerando inovação. Assim, comprovada a inserção do projeto, de forma positiva, comprovado está o impacto.

Um dos *fronts* da pesquisa buscou a detecção de possíveis gargalos do setor de *compliance* das Instituições Financeiras frente à Lei Geral de Proteção de Dados, e a sua projeção frente à punição trazida pela norma. Ainda, o trabalho, objetivou e apresentou um novo conjunto de normas/regras a fim de aprimorar o sistema de *compliance*, promovendo uma reestruturação da rede e protegendo os Bancos.

Com efeito, o motivo da criação é justamente a proteção do patrimônio da Instituição Financeira, o cumprimento da Lei (LGPD) e, ao fim e o cabo, a proteção aos dados pessoais dos titulares, fim maior da norma.

#### **d) Aplicabilidade:**

A aplicabilidade dos resultados é de abrangência nacional, visto que os produtos a serem entregues e os estudos desenvolvidos poderão ser integrados à toda rede bancária.

A criação de um órgão independente, proposto pelo projeto, poderá ser adaptado às Instituições Financeiras ou agentes de mercado, no todo ou em parte, e a pesquisa desenvolvida poderá ser utilizadas no meio acadêmico e tecnológico, tanto no contexto das pesquisas quanto na formulação de novos instrumentos legais.

Com efeito, a aplicabilidade, como análise final, é de complexa. O projeto objetiva inicialmente detectar os gargalos e, ao final, propor o aperfeiçoamento do modelo existente. Regulamentar tal procedimento e dinamizar isso, ou mesmo codificar, é uma atividade simplificada. Todavia, dar efetiva aplicabilidade, dependerá de toda a rede bancária, os efetivos destinatários finais do produto, àqueles que deverão tratar os dados dos clientes e dar destinação final à norma. Nesse contexto, anota-se que a produção é de fácil emprego e, também, tem

abrangência elevada, posto que poderá ser facilmente replicada à todas as Instituições Financeiras.

#### **e) Complexidade:**

Para o PROFNIT (2019) a “complexidade pode ser entendida como uma propriedade associada à diversidade de atores, relações e conhecimentos necessários à elaboração e ao desenvolvimento de produtos técnico-tecnológicos”.

No caso, o resultado do projeto é baseado em alteração/adaptação de um conhecimento já existente (sistema e regras de *compliance* aplicado ao setor bancário) e é estabelecido sem a participação de diferentes atores, o que indica uma produção de média/baixa complexidade.

#### **f) Inovação em Processo e Organizacional**

O projeto de pesquisa, além da dissertação, previa a apresentação de 02 (dois) produtos finais, sendo o principal o *relatório técnico conclusivo*. Sobre a matéria a ser tratada, é certo que não há originalidade. As regras de *compliance* já são adotadas no setor bancário. O que se apresentou, neste trabalho, foram alterações do sistema de *compliance* a fim de adaptar-se à LGPD, ou seja, aprimorar um sistema já existente (adaptação de conhecimento existente).

Há, nesse contexto, a busca pela inovação em *processo* e *organizacional*.

Criado pela OCDE – Organização para Cooperação e Desenvolvimento Econômico em 1995, o Manual de Oslo é a principal fonte internacional de diretrizes para coleta e uso de dados sobre atividades inovadoras. Segundo o Manual, **inovação** é a introdução de um bem ou serviço novo ou significativamente melhorado, no que se refere às suas características ou usos previstos, ou ainda, à implementação de métodos ou processos de produção, distribuição, marketing ou organizacionais novos ou significativamente melhorados (OCDE, 2004).

A atividade bancária é, essencialmente, de prestação de serviço e venda de produtos. O Banco vende dinheiro, e utiliza diversos expedientes para atingir seu objetivo final: *marketing*/propaganda; atração do cliente; coleta os dados pessoais e patrimoniais do público alvo, para a formação do cadastro (**objetivo da LGPD e do**

**presente estudo**); analisa os produtos e serviços disponíveis (análise de riscos) e o interesse em negociar, e; concretiza (ou não) o negócio jurídico.

E a integração desse complexo sistema exige uma robusta área de conformidade: primeiro por que a lei assim normatiza<sup>1</sup>; segundo que, frente à gestão de riscos, um setor dentro da empresa que garanta estar a organização em conformidade com as leis (internas e externas), é garantia de evitar multas e outras penalidades.

A LGPD alterou drasticamente a coleta, tratamento e gestão dos dados pessoais, justamente na formação do cadastro, vital aos agentes financeiros. Se antes a propriedade dos dados coletados era matéria nebulosa, agora pacificou-se ser do titular esse domínio. E as sanções previstas na lei, para os avanços dos controladores de dados frente aos direitos dos titulares, vão desde as multas milionárias à proibição do acesso aos dados, o que, para os bancos, é a vedação final à realização dos negócios.

Nesse sentido, a pesquisa desenvolvida, com as adaptações dos modelos de *compliance* já existentes, a elaboração de Relatório Final, desaguou em uma nova forma de fazer negócio. Os bancos alteraram significativamente suas rotinas de trabalho, para identificar a forma como coletam os dados, a natureza destes, a base legal para tratá-los, eventual descarte, até a possibilidade final de compartilhamento.

O trabalho envolveu, portanto, conceitualmente, **inovação em processo**, que é:

[...] a implementação de um método de produção ou distribuição novo ou significativamente melhorado. Incluem-se mudanças significativas em técnicas, equipamentos e/ou softwares.

As inovações de processo podem visar reduzir custos de produção ou de distribuição, melhorar a qualidade, ou ainda produzir ou distribuir produtos novos ou significativamente melhorados.

Os métodos de produção envolvem as técnicas, equipamentos e softwares utilizados para produzir bens e serviços. São exemplos de novos métodos de produção a introdução de novos equipamentos de automação em uma linha de produção e a implementação de design auxiliado por computador para o desenvolvimento de produto.

Os métodos de distribuição dizem respeito à logística da empresa e seus equipamentos, softwares e técnicas para fornecer insumos, alocar suprimentos, ou entregar produtos finais. Um exemplo de um novo método de distribuição é a introdução de um sistema de rastreamento de bens por código de barras ou de identificação ativa por frequência [*sic*] de rádio.

As inovações de processo incluem métodos novos ou significativamente melhorados para a criação e a provisão de serviços. Elas podem envolver

---

<sup>1</sup> A Resolução 4595/2017 exige a criação e regulamentação da área de *compliance* a todas as Instituições Financeiras.

mudanças substanciais nos equipamentos e nos softwares utilizados em empresas orientadas para serviços ou nos procedimentos e nas técnicas que são empregados para os serviços de distribuição. São exemplos a introdução de dispositivos de rastreamento para serviços de transporte, a implementação de um novo sistema de reservas em agências de viagens e o desenvolvimento de novas técnicas para gerenciar projetos em uma empresa de consultoria. (GN) (OCDE, 2004, p. 58-59, grifo nosso).

O setor de conformidade deverá adaptar-se às novas regras da LGPD, o que irá desaguar na reformulação na forma de controle da matriz do Banco para com as Superintendências, agências da rede, terceirizados, prestadores de serviços e fornecedores, enfim, todos aqueles que, de certa forma, gerenciem dados próprios e de terceiros. Para além do controle interno, os contratos com os clientes deverão ser reformulados, a fim de garantir o **consentimento**, sem o qual, em regra, o tratamento do dado é ilegal.

Em conclusão, todo o panorama dos processos internos e externos serão revistos, alterados, modificados para a adaptação a lei, um novo modelo de gestão deverá ser implementado à luz das regras e dentro do setor de *compliance*, o que conduz à *inovação em processo*.

D'outro lado, a alteração do sistema de *compliance*, objeto do trabalho, apresenta natureza de inovação organizacional, que “é a implementação de um novo método organizacional nas práticas de negócios da empresa, na organização do seu local de trabalho ou em suas relações externas” (OCDE, 2004, p. 61).

Ainda:

Os aspectos distintivos da inovação organizacional, comparada com outras mudanças organizacionais em uma empresa, é a implementação de um método organizacional (em práticas de negócios, na organização do local de trabalho ou nas relações externas) que não tenha sido usado anteriormente na empresa e que seja o resultado de decisões estratégicas tomadas pela gerência.

As inovações organizacionais em práticas de negócios compreendem a implementação de novos métodos para a organização de rotinas e procedimentos para a condução do trabalho. Isso inclui, por exemplo, a implementação de novas práticas para melhorar o compartilhamento do aprendizado e do conhecimento no interior da empresa. Um exemplo é a primeira implementação de práticas para a codificação do conhecimento, por exemplo pelo estabelecimento de bancos de dados com as melhores práticas, lições e outros conhecimentos, de modo que se tornem mais acessíveis a outros. Outro exemplo é a primeira implementação de práticas para o desenvolvimento dos empregados e melhorias na permanência do trabalhador, como os sistemas de educação e de treinamento. Outros exemplos são a primeira introdução de sistemas de gerenciamento para a produção geral ou para as operações de abastecimento, tais como sistemas de gerenciamento da cadeia de

fornecedores, reengenharia de negócios, produção enxuta e sistemas de gerenciamento da qualidade.

As inovações na organização do local de trabalho envolvem a implementação de novos métodos para distribuir responsabilidades e poder de decisão entre os empregados na divisão de trabalho existente no interior das atividades da empresa (e unidades organizacionais) e entre essas atividades. Participam também novos conceitos para a estruturação de atividades, tais como a integração de diferentes atividades de negócio. Um exemplo de inovação no local de trabalho é a primeira implementação de um modelo organizacional que confere aos empregados de uma empresa maior autonomia na tomada de decisões e os encoraja a contribuir com suas idéias [*sic*]. (OCDE, 2004, p. 62, grifo nosso).

Como dito, a implantação de um novo modelo de conformidade, ou sua alteração substancial, necessariamente caracteriza um novo método organizacional: novos conceitos e definições; atribuições de novas responsabilidades, aqueles que irão analisar os riscos e os dados pessoais existentes; aqueles que irão tratar os dados; aqueles que irão adaptar as novas rotinas e segmenta-las com todas as unidades da organização; aqueles que irão compartilhar os dados etc. Estas novas rotinas e responsabilidades se reveste em um novo modelo organizacional, e, por isso, inova neste segmento.

A própria lei traz a exigência de um novo responsável pela operação dos dados, comumente chamado de DPO - *Data Protection Officer*. É o operador dos dados, criado pelo art. 5º, VIII, da Lei 13.708/2018, e que tem suas funções regulamentadas no artigo 41, § 2º, da norma. O conceito de inovação organizacional ocorre quando há a previsão de maior autonomia na tomada de decisões a um colaborador, o que, neste caso, foi feito pela própria lei, em que pese o operador possa ter terceirizado ou até mesmo exercido por uma pessoa jurídica.

Ainda neste particular, há inovação organizacional quando a empresa altera, substancialmente, a forma de tratamento de negócios externos. Os Bancos detêm sob sua responsabilidade uma infinidade de dados pessoais, o que reclama especial atenção quando do compartilhamento destes com terceiros, na relação com fornecedores e prestadores de serviços, e, até mesmo, nos dados pessoais dos colaboradores (os quais inclusive podem ser sensíveis, a rigor do conceito do art. 7º, da LGPD). Desta forma, as alterações para adaptação do *compliance*, e um novo Código de Conduta certamente impactarão na forma de relacionamento dos bancos com os agentes externos, na formulação dos contratos e transmissão dos dados, o que caracteriza inovação organizacional.

### **g) Transferência de Tecnologia. Possibilidade**

De acordo com o Instituto Nacional de Propriedade Industrial (INPI), é considerado *Transferência de Tecnologia* um comprometimento firmado entre duas partes envolvidas no qual é **formalizado a transação de conhecimentos técnicos, artísticos ou científicos.**

A transferência de tecnologia é um dos principais gargalos quando se trata de inovação. É por meio desse negócio jurídico que se transferem os direitos sobre determinada tecnologia, conhecimento e/ou demais ativos imateriais para que parceiros possam fazer uso dessa tecnologia e, com isso, desenvolvam e explorem esses conhecimentos em seus produtos e/ou serviços inovadores. (AREAS; FREY, 2019, p. 45).

A transferência de tecnologia se faz, portanto, através de contrato de cessão, onde se repassará a terceiro os direitos sob determinada tecnologia ou conhecimento adquirido, enquanto bens intangíveis/imateriais. E seu objetivo primordial é fomentar a economia do país, por meio da difusão do conhecimento através de novos produtos e processos.

O Instituto Nacional da Propriedade Industrial (INPI) define alguns tipos de contratos relacionados à transferência de tecnologia, dentre eles:

Fornecimento de Tecnologia: contratos que objetivam a aquisição de conhecimentos e técnicas não amparados por direitos de propriedade industrial, destinados à produção de produtos e/ou processos;  
Prestação de Serviços de Assistência Técnica e Científica: contratos que estipulam as condições de obtenção de técnicas, métodos de planejamento e programação, bem como pesquisas, estudos e projetos destinados à execução ou prestação de serviços especializados; (INPI, 2017, p. 9).

Os produtos desenvolvidos neste projeto podem ser transferidos (transferência de tecnologia) ou alienados (gratuita ou onerosa) a terceiros. O trabalho apontou as novas exigências trazidas pela LGPD ao setor bancário, os gargalos existentes quando comparados ao modelo anterior, e como o setor de compliance da organização poderá atuar, como ator principal, para a adaptação da empresa à estas novas exigências.

Já o Relatório Técnico Conclusivo, como produto final, resumiu os impactos criados pela norma, e apontou uma solução viável ao compliance a fim de fazer face às novas exigências.

Ambos os produtos são o resultado do projeto de pesquisa, se inserem no conceito de conhecimento para fins contratuais, e podem ser objeto de cessão por meio de contratos de transferência, seja para fornecimento de tecnologia (destinado a produção de processos inovadores) ou prestação de serviços de assistência técnica e científica (projetos destinados à execução ou prestação de serviços especializados).

## LISTA DE ILUSTRAÇÕES E TABELAS

Tabela 1	Frequência de itens recuperados em bases de dados .....	33
Figura 1	O Compliance como Pilar da Governança em Mercados Regulados .....	42
Figura 2	Tendências, Perspectivas e desafios de Compliance .....	43
Tabela 2	Bases Legais da LGPD .....	59
Figura 3	Rota do FNO.....	74
Gráfico 1	Fundo Constitucional de Financiamento do Norte .....	75
Gráfico 2	Organograma .....	80
Gráfico 3	Estrutura Organizacional .....	81
Figura 4	Gerencia de Controles Internos .....	85
Figura 5	Modelos de Três linhas de Defesa.....	89
Figura 6	GECIN .....	95

## SUMARIO

1	<b>INTRODUÇÃO</b> .....	19
2	<b>OBJETIVOS</b> .....	20
2.1	<b>Objetivo Geral</b> .....	20
2.2	<b>Objetivos Específicos</b> .....	20
3	<b>JUSTIFICATIVA</b> .....	21
4	<b>REVISÃO DE LITERATURA</b> .....	25
5	<b>METODOLOGIA</b> .....	31
5.1	<b>Classificação da pesquisa</b> .....	31
5.2	<b>Levantamento bibliográfico</b> .....	31
5.3	<b>Etapas da pesquisa</b> .....	33
6	<b>RESULTADOS</b> .....	36
6.1	<b>Compliance - A origem</b> .....	36
6.2	<b>Compliance e as Instituições Financeiras</b> .....	38
6.3	<b>Compliance e a Inovação</b> .....	45
6.4	<b>Compliance e a LGPD</b> .....	48
6.5	<b>A Lei de Dados Pessoais em um panorama geral e no contexto histórico</b> .....	49
6.6	<b>As exigências legais trazidas pela LGPD ao setor bancário</b> .....	54
6.6.1	As bases legais. O consentimento. Artigo 7º, I, da LGPD .....	60
6.6.2	As bases legais. A execução de contrato. Artigo 7º, V, da LGPD .....	62
6.6.3	As bases legais. A proteção do crédito. Artigo 7º, X, da LGPD.....	63
6.6.4	As bases legais. Cumprimento de obrigação legal. Artigo 7º, II, da LGPD .....	67
6.7	<b>O Legítimo Interesse utilizado na atividade bancária. Uma base legal questionada</b> .....	67
6.8	<b>Os Procedimentos e as opções práticas de <i>compliance</i> disponíveis à implementação do tratamento de dados ao setor bancário. Os desafios</b> .....	69
6.9	<b>O estudo de caso do Banco da Amazônia S.A.</b> .....	72
6.9.1	O Banco da Amazônia e a LGPD.....	76
6.9.1.1	<i>A implantação da LGPD</i> .....	76
6.9.1.1.1	<u>Primeira Etapa</u> .....	77

6.9.1.1.2	<u>Segunda Etapa</u> .....	77
6.9.1.1.3	<u>Terceira Etapa</u> .....	79
<b>6.9.2</b>	<b>O compliance dentro do Banco da Amazônia e a estrutura organizacional da Instituição</b> .....	80
<b>6.10</b>	<b>Proposta do trabalho: A alteração do modelo de compliance junto ao Banco da Amazônia para adaptação à LGPD</b> .....	90
6.10.1	Aspecto inovativo do trabalho .....	90
6.10.2	A importância de um modelo de compliance independente para cumprimento da Lei de Proteção de Dados .....	92
6.10.3	Criação de uma Coordenação independente para cumprimento e fiscalização da LGPD. Estrutura e organização .....	95
<b>7</b>	<b>CONCLUSÃO</b> .....	98
	<b>REFERÊNCIAS</b> .....	103
	<b>APÊNDICE A - CANVAS</b> .....	111
	<b>APÊNDICE B - MATRIZ SWOT / FOFA</b> .....	112
	<b>APÊNDICE C - RELATÓRIO TÉCNICO CONCLUSIVO</b> .....	113
	<b>APÊNDICE D - CARTILHA</b> .....	172

## 1 INTRODUÇÃO

O trabalho realizou um estudo sobre quais os pilares do *compliance* poderão ser estruturados nas empresas do setor bancário para que se adaptem ao tratamento de dados, segundo a Lei Geral da Proteção de Dados.

A área de *compliance* é uma das mais sensíveis e necessárias às Instituições Financeiras, e foi profundamente alterada com a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018. As novas exigências, para proteger os dados, criadas pela norma, impuseram profundas modificações à área de conformidade.

A partir da vigência da nova lei (término do período de vacância), não só os Bancos, mas todas as empresas que mantem em seus cadastros dados de particulares, devem se reestruturar, sob pena de pagar multas que pode chegar até cinquenta milhões de reais.

Assim, a partir da concepção inicial, apresentou-se um projeto de criação de uma nova estrutura dentro da Instituição Financeira estudada (estudo de caso), com o aperfeiçoamento do então vigente modelo de *compliance*, o qual contemplou as inovações impostas pela LGPD. O trabalho foi realizado via de um produto dissertativo, apresentando um estudo científico retrospectivo, com o objetivo de reunir, analisar e interpretar informações e apresentar um resultado.

Com a problemática identificada que questionou, “De que forma é possível adaptar o sistema de *compliance* para o setor bancário, de modo que atenda as inovações criadas pela Lei Geral de Proteção de Dados, e, de consequência, reduza os riscos de danos administrativos e financeiros dela decorrentes?”, o estudo desenvolveu, como dito, um novo projeto para a criação de uma nova Coordenação na área de *compliance* para o setor bancário, a qual incorporou as inovações criadas pela Lei Geral de Proteção de Dados. Com a implantação da proposta, a ideia é adaptar o sistema de *compliance* às novas exigências da norma e, com isso, reduzir os riscos de danos administrativos e financeiros decorrentes das multas pelo descumprimento da lei.

## 2 OBJETIVOS

Para apresentar um modelo inovador ou aperfeiçoado de *compliance*, ao sistema bancário, o qual contemple as normas inovadoras da LGPD, e proteja as empresas de futuros dissabores, considerando as punições dela decorrentes, fez-se explanação com os objetivos, geral e específicos, a seguir.

### 2.1 Objetivo geral

Examinar as exigências legais trazidas pela LGPD às empresas do setor bancário, de modo a identificar e especificar os procedimentos e opções práticas de *compliance* à implementação do tratamento de dados na nova realidade. Analisar o sistema de conformidade do Banco da Amazônia S.A. (estudo de caso) e propor o seu aperfeiçoamento, em um modelo de aplicação geral/universal, e inviabilizar, tanto possível, a aplicação das penalidades decorrentes da lei.

### 2.2 Objetivos específicos

- a) Examinar as exigências legais trazidas pela LGPD ao setor bancário, por meio de uma revisão de literatura;
- b) Identificar os procedimentos e opções práticas de *compliance* à implementação do tratamento de dados ao setor bancário;
- c) Aprimorar o sistema de *compliance* aplicado ao sistema bancário, notadamente do Banco da Amazônia, o qual contemple as normas inovadoras da LGPD, e proteja as empresas de futuros dissabores, considerando as punições dela decorrentes.

### 3 JUSTIFICATIVA

A Lei 13.709, de 14 de agosto de 2018, conhecida como LGPD – Lei Geral de Proteção de Dados, dispõe sobre o tratamento de dados pessoais, 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 e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018, p. 59).

A referida norma legal trouxe mudanças poderosas às empresas que detém, em seu patrimônio, dados pessoais de pessoas físicas e jurídicas, e que, de alguma forma, utilizam destes dados no cotidiano. Doravante, com o término do período de vacância da norma, estes conglomerados (e aí se ligam boa parte da indústria, comércio e até o setor público), passaram a ter responsabilidades direta no tratamento dos dados pessoais, com implicações significativas para eventuais lesões causadas à terceiros.

Segundo a pesquisa *“The end of the beginning – Unleashing the transformational power of GDPR”*, realizada em 2018, 60% das empresas já adotam a regulamentação de tratamento de dados na União Europeia (IBM, 2018). No Brasil, com o início da vigência da Lei, ocorrida no ano de 2020, houve uma alteração profunda no cenário de tratamento de dados no país, exigindo das empresas uma nova postura, diante do alcance da norma, a qual vem estabelecido no artigo 3º:

Art. 3º Esta Lei aplica-se 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, desde que:

I - a operação de tratamento seja realizada no território nacional;

II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou [\(Redação dada pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei. (GN) (BRASIL, 2018b, p. 59, grifo nosso).

Neste novo cenário de mudanças, a alteração do sistema de *compliance* dos Bancos é altamente recomendável. Como é cediço, o *compliance* tem a função de proporcionar segurança e minimizar riscos de instituições e empresas, garantindo o cumprimento dos atos, regimentos, normas e leis estabelecidos interna e externamente.

Nesse contexto, e agora voltado para o cerne do trabalho, dentro das Instituições Financeiras, é essencial que a área de *compliance* esteja organizada para adaptar-se às novas exigências da LGPD, seus requisitos e, principalmente, as implicações em vergar as regras estabelecidas, diante das multas, que podem alcançar cifras milionárias, além da suspensão do direito de acessar as bases de dados.

Os bancos têm, em sua área de cadastro, um ponto nevrálgico de seu funcionamento. E é no cadastro do cliente que se acessam, e depositam, os dados pessoais. O deferimento de um crédito passa, necessariamente, pela análise da vida pregressa, financeira e patrimonial do indivíduo, tudo ligado, portanto, aos seus dados internos, justamente o que é regulado pela LGPD. É, portanto, uma das áreas mais sensíveis das Instituição Financeiras, o que potencializa o cuidado no tratamento dos dados pessoais, e a necessidade de cumprimento integral da Lei 13.709/2018. Uma eventual multa que estabeleça a perda de acesso de dados pode, em um fim, impedir novos negócios, como a estabelecida no artigo 52, V e VI, da LGPD:

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: [\(Vigência\)](#)  
I - advertência, com indicação de prazo para adoção de medidas corretivas;  
II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;  
III - multa diária, observado o limite total a que se refere o inciso II;  
IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;  
V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;  
VI - eliminação dos dados pessoais a que se refere a infração; (BRASIL, 2018b, p. 64).

Buscou-se assim, como resultado do trabalho, apresentar uma solução para aperfeiçoar o sistema de *compliance* ao sistema bancário, **especialmente ligado aos Bancos Públicos (Banco da Amazônia S.A., Banco do Brasil S.A etc.)** o qual

contemplasse as normas inovadoras da LGPD, e protegesse as empresas de futuros dissabores, considerando as punições dela decorrentes. E nesse ponto surgem os benefícios. Ampliar e melhorar a área de *compliance* certamente tornará mais robusta a fiscalização e mapeamento do tratamento dos dados exigidos pela LGPD, evitando o pagamento de multas milionárias.

Com efeito, os Bancos Públicos, como os citados, têm grande parte do seu capital pertencente à União Federal, e, desta forma, o trabalho está a beneficiar toda a coletividade, eis que tem o escopo de proteger o patrimônio público. E as indicadas Instituições Financeiras estão abarcadas pela norma, de forma categórica, conforme se vê do artigo 24, da Lei:

Art. 24. As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no [art. 173 da Constituição Federal](#), terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.

Parágrafo único. As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos deste Capítulo. (BRASIL, 2018b, p. 62).

D’outra banda, o benefício também é estendido ao proprietário dos dados, pois, na medida em que as empresas aumentam o grau de confiabilidade no tratamento dos dados, a proteção destes é igualmente certificada, o que, ao fim e ao cabo, é o objetivo da norma, conforme descrito no artigo 1º:

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, 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 e o livre desenvolvimento da personalidade da pessoa natural.** (GN). (BRASIL, 2018b, p. 59, grifo nosso).

O estudo, portanto, contemplou todos os lados envolvidos: o setor público (a proteção ao patrimônio público), e os particulares, quanto ao direito e segurança de seus dados pessoais, produzindo um trabalho final que culminou:

- I. no aprimoramento das normas internas do setor de *compliance* do banco, visando dar vazão às exigências da LGPD;
- II. em aprimorar os procedimentos de controle do *compliance* junto à toda rede bancária, as quais de fato coletam e tratam os dados (e que são o

objeto principal da Lei), tudo com o objetivo de melhorar a governança do setor e cumprir as exigências da norma;

## 4 REVISÃO DE LITERATURA

O projeto reuniu o arcabouço normativo existente, que engloba Leis, Decretos e outros atos normativos, como Portarias do Banco Central do Brasil, com artigos científicos e literaturas relevantes sobre o tema em questão.

A LGPD aborda o manuseio de informações de cunho pessoal, seja por indivíduos ou entidades públicas ou privadas, em qualquer meio, incluindo o ambiente digital. Seu principal propósito é resguardar os direitos fundamentais de liberdade, privacidade e desenvolvimento pessoal dos indivíduos.

Dentro das Instituições Financeiras, a LGPD traz dois pontos cruciais a serem observados: a transparência e o consentimento.

O primeiro ponto se refere à clareza de informações sobre todo tratamento que será aplicado ao dado coletado e consentimento trata da autorização do uso desses dados. É mapear os fluxos e identificar a tomada de consentimento nas interações com clientes, e verificar se a autorização por parte do usuário foi realizada de acordo com as novas normativas. (EXECUTIVE REPORT, [2019?], p. 3).

A norma legal alterou profundamente a rotina das Instituições Financeiras e, notadamente, as públicas, que têm no cadastro de dados dos clientes um ponto sensível de sua engrenagem. Os Bancos públicos mereceram um artigo especial, dentro da lei, quanto a sua aplicação, conforme descrito no artigo 24 da norma.

As Instituições Financeiras tratam, em geral, de um amplo e completo cadastro de informações do cliente (os bancos fazem vários tipos diferentes de tratamento de dados, p. ex: cadastro, consulta, abertura de contas, verificação para envio ao Banco Central, etc), que compõem a base de dados da empresa, e que são utilizados na análise do risco, na decisão final para o deferimento do crédito e na geração de futuros contratos. São dados sensíveis, e que deverão ser tratados, na forma do artigo 11, da LGPD (BRASIL, 2018b, p. 61):

### Seção II

#### Do Tratamento de Dados Pessoais Sensíveis

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

- b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
- c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
- d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da [Lei nº 9.307, de 23 de setembro de 1996 \(Lei de Arbitragem\)](#) ;
- e) proteção da vida ou da incolumidade física do titular ou de terceiro;
- f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou [\(Redação dada pela Lei nº 13.853, de 2019\)](#) [Vigência](#)
- g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

§ 2º Nos casos de aplicação do disposto nas alíneas “a” e “b” do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.

§ 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.

§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: [\(Redação dada pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

I - a portabilidade de dados quando solicitada pelo titular; ou [\(Incluído pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo. [\(Incluído pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

§ 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários. [\(Incluído pela Lei nº 13.853, de 2019\)](#) [Vigência](#).

É, portanto, uma das áreas mais sensíveis das Instituição Financeiras, o que potencializa o cuidado no tratamento dos dados, e a necessidade de cumprimento integral da Lei 13.709/2018. As multas estabelecem cifras astronômicas, além da perda de acesso aos dados, o que pode, em um fim, impedir novos negócios, como a sanção prevista no artigo 52, II, V e VI, da LGPD:

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: (Vigência)  
 I - advertência, com indicação de prazo para adoção de medidas corretivas;  
 II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a **R\$ 50.000.000,00 (cinquenta milhões de reais) por infração**;  
 III - multa diária, observado o limite total a que se refere o inciso II;  
 IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;  
 V - **bloqueio dos dados pessoais** a que se refere a infração até a sua regularização;  
 VI - eliminação dos dados pessoais a que se refere a infração; (GN). (BRASIL, 2018b, p. 64).

Calha esclarecer, neste particular, que a redação originária da norma previa outras sanções, ainda mais severas, mas que foram alvo de veto pela Medida Provisória 869/2018<sup>2</sup>. (vide BRASIL, 2018c). O texto primitivo trazia a *suspensão – parcial ou total – do funcionamento do banco de dados a que se refere a infração até a regularização da atividade de tratamento pelo controlador; à suspensão do próprio exercício da atividade de tratamento dos dados pessoais a que se refere a infração; e à proibição – parcial ou total – do exercício de atividades relacionadas a tratamento de dados.*

Tais vetos tiveram o seguinte fundamento:

As sanções administrativas de suspensão ou proibição do funcionamento/exercício da atividade relacionada ao tratamento de dados podem gerar insegurança aos responsáveis por essas informações, bem como impossibilitar a utilização e tratamento de bancos de dados essenciais a diversas atividades, a exemplo das aproveitadas pelas instituições financeiras, dentre outras, podendo acarretar prejuízo à estabilidade do sistema financeiro nacional. (BRASIL, 2018a, p. 81).

Com efeito, e ainda no périplo normativo, às instituições financeiras se aplica a Resolução 4658/2018, do Banco Central do Brasil (BACEN), que dispõe sobre a política de segurança cibernética e sobre os requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem. Nos termos da Resolução (art. 3º), as instituições financeiras devem implantar uma política de segurança cibernética que contemple, entre outras medidas:

---

<sup>2</sup> Medida Provisória publicada em 28 de dezembro de 2018 e atualmente sujeita à aprovação do Congresso Nacional, nos termos do art. 62 da Constituição Federal.

- (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 efeitos de incidentes relevantes para as atividades da instituição; e
- (iv) os mecanismos para disseminação da cultura de segurança cibernética na instituição. (BANCO CENTRAL DO BRASIL, 2018, p. 2).

Esse conjunto de dispositivos encontrados na legislação brasileira foi aplicado em diversas situações nas quais se procurava reconhecer a proteção de dados pessoais e, ao mesmo tempo, sancionar aqueles que violavam os seus preceitos<sup>3</sup>.

Neste novo cenário de mudanças, a alteração do sistema de *compliance* dos Bancos é altamente recomendável. Como é cediço, a área de *compliance* tem a função de proporcionar segurança e minimizar riscos de instituições e empresas, garantindo o cumprimento dos atos, regimentos, normas e leis estabelecidos interna e externamente. *Compliance*, na acepção jurídica, refere-se:

[...] ao conjunto de ações a serem adotadas no ambiente corporativo para que se reforce a anuência da empresa à legislação vigente, de modo a prevenir a ocorrência de infrações ou, já tendo ocorrido o ilícito, propiciar o imediato retorno ao contexto de normalidade e legalidade. (FRAZÃO, 2007, p. 42).

Dentro das Instituições Financeiras, é essencial que a área de *compliance* esteja organizada para adaptar-se às novas exigências da LGPD, seus requisitos e, principalmente, as implicações em vergar as regras estabelecidas, diante das multas, que podem alcançar cifras milionárias, além da suspensão do direito de acessar as bases de dados.

Sobre a importância da área do *compliance*, lecionam Blum e Zamperlin (2015):

O *compliance* de dados pessoais volta-se justamente para auxiliar os agentes de tratamento a aplicar de forma eficaz as normas de proteção de dados e “conduzirá a pessoa jurídica a manter esses dados e toda sua atividade dentro dos ditames legais, utilizando a segurança da informação

---

<sup>3</sup> A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro - Ed. 2019. Capítulo 3. Primeiras impressões sobre o tratamento de dados pessoais nas hipóteses de interesse público e execução de contratos Advogada. Mestre e Doutora em Direito das Relações Sociais pelo Programa de Pós-Graduação da Universidade Federal do Paraná. Professora do UniCuritiba. Membro da Comissão de Educação Jurídica da Ordem dos Advogados do Brasil, Seccional do Paraná.

em prol da minimização de incidentes que impliquem na responsabilidade empresarial.

E sobre a evolução e consolidação dos mecanismos de *compliance*, diretamente voltados à LGPD, Frazão; Oliva; Abilio (2019, p. 695-698) indicaram três fatores para robustecer seu papel:

Em **primeiro lugar**, o amplo escopo de incidência da LGPD (decorrência, como visto, do conceito de dado pessoal, de tratamento e de banco de dados) torna necessária a adaptação não apenas de atividades centralizadas na coleta e/ou tratamento de dados, mas também de qualquer operação que perpassa, ainda que indiretamente, a utilização de informações relacionadas ou relacionáveis a pessoas naturais. À luz do conceito de dado pessoal, até mesmo as mais simples atividades terão que se adequar à lei, vez que demandam, em alguma medida, o armazenamento de informações tuteladas pela lei – basta cogitar das informações atinentes aos empregados ou, ainda, das listas de clientes. Mesmo operações laterais – como o que ocorre nos condomínios edifícios ao coletarem e armazenarem dados de condôminos, visitantes, funcionários – também se sujeitam à LGPD.

Nesse contexto, observa-se que o *compliance* de dados não se limita apenas ao relacionamento com consumidores, mas acaba por repercutir em várias esferas da atividade empresarial, a demandar adaptação também de setores que, inicialmente, não estariam diretamente relacionados com a LGPD. O *compliance* de dados assume caráter transversal, a tornar necessário rever os padrões de conduta estabelecidos para cumprimento de outras normas. Remeta-se, mais uma vez, à relação de trabalho: as regras de conformidade adotadas nesse setor deverão ser atualizadas para contemplar também os preceitos da LGPD, evitando-se, por exemplo, a coleta de dados desnecessários ou cujo emprego possa ser considerado discriminatório.

O **segundo fator** está associado ao primeiro: uma vez que são diversas as entidades que deverão cumprir os preceitos da LGPD, há, dentro de cada comando da lei, níveis de exigência distintos e adaptações necessárias à luz das hipóteses de tratamento de dados envolvidas, 35 até mesmo com vistas a evitar que a proteção termine por inviabilizar a exploração econômica de certas atividades.

A proteção de dados não tem por objetivo inviabilizar a coleta de dados para conhecimento do público alvo e aprimoramento das atividades empresariais. Todo empresário tem legítimo interesse de conhecer quem são seus consumidores, empregados e candidatos a emprego. Entretanto, a LGPD esclarece que os dados coletados para essa finalidade legítima pertencem às pessoas físicas às quais os dados se referem e precisam ser tratados e coletados em respeito a essa relação de pertencimento.

Nessa direção, importante papel pode ser assumido pelas entidades de classe, também autorizadas pelo art. 50 a formularem regras de boas práticas, na medida em que, conhecedoras das especificidades da atividade, podem contribuir para o estabelecimento de critérios adequados à cada hipótese, para além de traduzir os preceitos legais em ações concretas a serem tomadas pelos agentes econômicos. 37 Esses, a seu turno, beneficiar-se-iam da segurança decorrente da (adequada) estruturação de normas de governança fixadas pela entidade, capaz de sugerir uniformização dos padrões aplicáveis àquele mercado. A efetiva atribuição de valor a esses

parâmetros por terceiros (incluindo-se a ANPD e o Poder Judiciário) é essencial para que se construa a segurança com eles pretendida.

Por fim, **um terceiro fator** consiste na necessidade de conferir concretude a alguns preceitos empregados pela LGPD e, assim, permitir que sejam adotados comportamentos em conformidade com a lei. Como consequência do (necessário) recurso a cláusulas gerais pelo legislador, 38 muitos dos comandos legais comportam significativa margem interpretativa. É o caso, por exemplo, do conceito de ‘legítimo interesse do controlador’ (empregado no artigo 7º, inciso IX como hipótese autorizativa para o tratamento de dados): 39 muito embora o artigo 10 tenha procurado delimitar seu conteúdo e o art. 37, a seu turno, recrudesça o controle sob as operações realizadas com base em tal exceção ao consentimento, verifica-se margem de discricionariedade cuja avaliação, no comum dos casos, será feita a posteriori pelos órgãos competentes. Abre-se, assim, mais um espaço de complementação a ser realizada pelos programas de *compliance*. Em observância dos deveres de transparência exigidos pela LGPD – no que concerne ao legítimo interesse, bastante reforçado – as regras de governança podem dispor sobre as hipóteses específicas em que o tratamento será considerado pela entidade como fundamentado no seu legítimo interesse.

Todos esses elementos corroboram a extrema relevância de se estabelecerem normas de governança no âmbito do tratamento de dados pessoais que sejam bem estruturadas e atendam aos comandos legais. Apenas a partir da concreta identificação das necessidades específicas de adaptação de cada agente será possível garantir a conformidade com a nova legislação.

E finalizam, os referidos autores Frazão; Oliva; Abilio (2019, p. 711), acerca da importância do tema e seus desafios:

Como se pode denotar das considerações anteriores, a implementação de efetivo programa de *compliance* em matéria de proteção de dados consiste em tarefa mais que desafiadora. Apenas se garantindo intensa colaboração de inúmeros setores das pessoas jurídicas – exemplificativamente, recursos humanos, tecnologia da informação, jurídico – e a construção de estruturas (até mesmo de softwares) capazes de atender a todos os rígidos padrões estabelecidos pela LGPD se poderá pavimentar caminho de conformidade com a norma. Os custos, por consequência, certamente serão significativos. Daí a necessidade de se contrapor aos elevados gastos incentivos concretos à implantação dos mecanismos de governança.

Com efeito, diante do cenário posto em discussão, o estudo, a implementação e a efetiva aplicação do programa de *compliance* em matéria de proteção de dados, ligados à LGPD, exige árdua atuação dos agentes envolvidos. Segundo Frazão; Oliva; Abilio (2019, p. 711), no ambiente empresarial, a engrenagem não é alcançada sem a intensa atuação da área de recursos humanos, tecnologia da informação, jurídico e a “construção de estruturas (até mesmos de softwares) capazes de atender a todos os rígidos padrões estabelecidos pela LGPD, se poderá pavimentar o caminho de conformidade com a norma”.

## **5 METODOLOGIA**

A metodologia pode ser compreendida por um conjunto de métodos e procedimentos utilizados para a realização de algo. Essa seção visa explicar sobre como a pesquisa foi desenvolvida para atingir os seus objetivos. Apresenta-se, inicialmente a classificação de pesquisa, seguindo para as etapas da pesquisa, com a delimitação do tempo e do espaço empregados bem como as ferramentas para a coleta e análise dos dados.

### **5.1 Classificação da pesquisa**

A pesquisa buscou resolver um problema do setor financeiro em face da introdução de um novo arcabouço legal e, dessa forma, caracteriza-se como uma pesquisa aplicada. Em relação aos objetivos, não se pretendeu explicar ou descrever um fenômeno, mas sim "proporcionar uma maior familiaridade com o problema, com vista a torná-lo mais explícito ou a constituir hipóteses" (GIL, 2009, p. 41) e, dessa forma, a pesquisa classificou-se como exploratória.

Em relação aos procedimentos adotados, caracterizou-se como bibliográfica e documental pois partiu-se de um processo de revisão de literatura para compreender as exigências legais trazidas pela LGPD ao setor bancário. Tal revisão ocorreu tanto em artigos científicos como em outros documentos como leis, normas e regulamentos relativos ao compliance.

Ainda, quanto aos procedimentos, caracterizou-se como estudo de caso pois visou retratar exhaustivamente os aspectos relativos ao compliance em uma instituição financeira, no caso o Banco da Amazônia S.A.

Por fim, quanto à abordagem de análise de dados, a pesquisa caracterizou-se como qualitativa pois baseou-se na observação e compreensão dos ambientes em que os sistemas de compliance são utilizados com a intenção de promover uma compreensão do fenômeno em sua totalidade (GIL, 2009; WAINER, 2017).

### **5.2 Levantamento bibliográfico**

Adotou-se o Tesauro Jurídico da Justiça Federal que inclui as terminologias específicas do Direito nas áreas de competência jurídica para

maximizar o uso da informação atingindo mais uniformidade da informação tratada com termos adotados nos bancos de pesquisa bem como adotando o termo Compliance que não foi encontrado no tesouro.

Em novembro de 2022, utilizando os termos de busca “*Compliance*” e “*LGPD*” na base **Web Of Science**, foram recuperados [14](#) documentos, onde oito destes são do ano de 2021 (57.143%), e dois para cada ano de 2019 (14.286%), 2020 (14.286%) e 2022 (14.286%) (**QUADRO 1**). O autor com maior número de artigos recuperados na pesquisa foi a Edna Dias Canedo com quatro resultados (**QUADRO 2**).

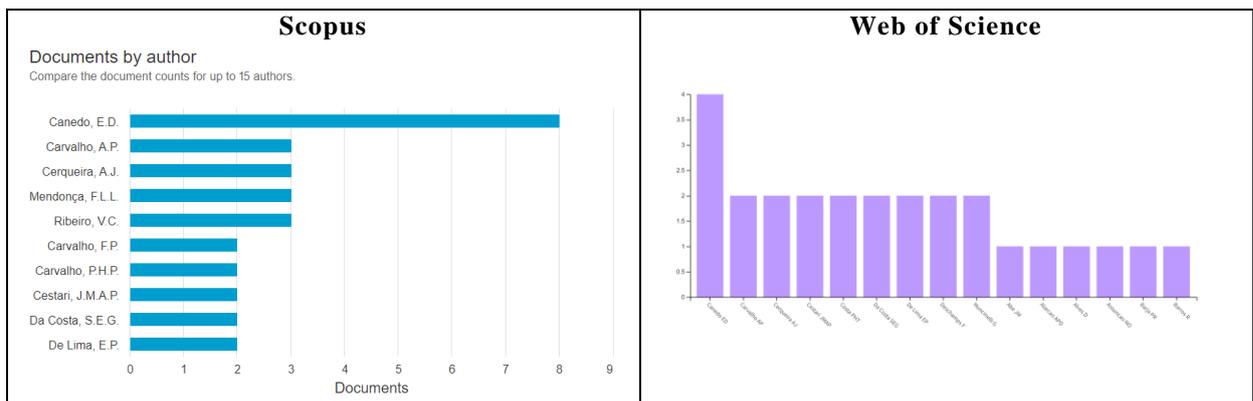
Na mesma data, utilizando os termos de busca “*Compliance*” e “*LGPD*” na base **Scopus** (Elsevier), foram recuperados [18](#) documentos, onde dez destes são do ano de 2021 e três no ano de 2022, quatro no ano de 2020 e apenas um no ano de 2019 (**QUADRO 1**). O autor com maior número de artigos recuperados na pesquisa foi a Edna Dias Canedo com oito resultados (**QUADRO 2**).

**Quadro 1 - Resultado por ano na base Scopus e Web of Science**

Web of Science			Scopus	
Selecionar todos <input type="checkbox"/>	Campo: Anos da publicação	Contagem do registro	Year ↓	Documents ↑
<input type="checkbox"/>	2021	8	2022	3
<input type="checkbox"/>	2019	2	2021	10
<input type="checkbox"/>	2020	2	2020	4
<input type="checkbox"/>	2022	2	2019	1
Tabela de dados de análise				

Fonte: o Autor, com dados das bases Scopus; Web of Science [2022]

**Quadro 2 - Resultado por autores na base Scopus e Web of Science**



Fonte: o Autor, com dados das bases Scopus; Web of Science [2022]

Realizada a busca com os mesmos termos, “*Compliance*” e “*LGPD*”, na Base de Dados de Teses e Dissertações – **BDTD** do IbiCT, encontrou-se [15](#) documentos, sendo 3 teses e 12 dissertações.

**Tabela 1 – Frequência de itens recuperados em bases de dados**

Base de dados	Descritores / Termos / Palavras-Chave	Total
<i>Web of Science</i>	“ <i>Compliance</i> ” e “ <i>LGPD</i> ”	<a href="#">14</a>
<i>Scopus</i> (Elsevier),		<a href="#">18</a>
BDTD		<a href="#">15</a>
		<b>47*</b>

Fonte: O autor

\* São 38 itens encontrados: os resultados da *Web of Science* e nas *Scopus* trazem artigos iguais.

As Bases *Web of Science* e *Scopus* apresentam artigos semelhantes. Dos 14 artigos encontrados na primeira base, os nove primeiros também estão na base *Scopus*, o que revela o número real de **38** itens recuperados.

### 5.3 Etapas da pesquisa

A pesquisa ocorreu entre os meses de julho de 2021 a dezembro de 2022, e foi aplicada em uma Instituição Financeira do estado do Tocantins, em 3 grandes fases: Revisão jurídica e bibliográfica, Coleta de dados na instituição financeira participante e Análise comparativa e proposição de solução.

Na primeira fase, foi realizada uma revisão de literatura para examinar tanto as exigências legais quanto as iniciativas presentes nos estudos científicos já realizados no sentido de aplicar no novo regramento da *LGPD* na prática. Para a revisão de estudos, foi realizado um mapeamento das referências em periódicos científicos responsáveis pela difusão de resultados de pesquisas e o registro dos avanços da produção acadêmica nas áreas de interesse do presente estudo. Tal revisão bibliográfica ocorreu em 4 (quatro) etapas, a saber: a) identificação e ajustes nas palavras-chave, b) coleta dos dados, c) leitura dos títulos e resumos para identificar os estudos mais relevantes, d) leitura integral e fichamento dos estudos.

Foram coletados artigos científicos publicados entre os anos de 2010 e 2021 nas coleções indexadas no portal de periódicos da Capes. Os estudos coletados

forneceram subsídios para a resposta à pergunta da pesquisa. Dessa forma, para garantir uma recuperação ampla de artigos considerou-se as palavras-chaves mais significativas dentro do problema focalizado e seus termos correlatos em português e inglês, a saber: LGPD - "Lei geral de proteção de dados", Dados pessoais sensíveis, Compliance, Instituição Financeira. Após a etapa de ajuste a string de busca, foi aplicada na base de dados escolhida e os estudos recolhidos foram organizados em uma tabela para apoiar o processo de identificação dos estudos mais relevantes. Tal tabela foi formada pelos campos: autores, ano, título do estudo, resumo, decisão de inclusão e justificativa. Por fim, após a identificação dos estudos mais relevantes, procedeu-se a leitura e fichamento integral dos mesmos.

Após a revisão de literatura, a pesquisa voltou-se a compreender como a instituição financeira escolhida para análise realiza seu sistema de compliance. Nessa etapa foram realizadas a análise documental dos regimentos, regulamentos e demais documentos que normatizam os procedimentos dentro da instituição.

Por fim, foi realizada uma análise comparativa entre os regimentos e soluções apresentados na revisão bibliográfica e os dados coletados na instituição financeira e, com base nessa análise, foi apresentada uma solução ao sistema de compliance, ajustado ao novo arcabouço legal.

Como proposto, o trabalho final apresentado foi um relatório técnico conclusivo. A área de conformidade é extremamente sensível dentro da Instituição Financeira, e tem a responsabilidade em detectar possíveis gargalos existentes dentro da organização, saná-los e evitar ou minimizar prejuízos advindos. Nesse contexto, era presumível que o agente financeiro escolhido como base para o trabalho não autorizasse a reprodução de seu sistema de *compliance*, tampouco eventuais inconformidades existentes, o que limitou a extensão da pesquisa.

Durante a execução do trabalho, haveria a possibilidade de exploração de inúmeros outros dados e elementos de pesquisa, tais como os fluxos de processos existentes na gestão de *compliance*, a forma de tratamento, o tempo e a devolutiva, com a respectiva solução. Contudo, além de ser um dado extremamente sensível ao Banco, não houve tempo suficiente para estratificar as informações, o que poderá, certamente, ser alvo de um futuro trabalho, via artigo científico ou mesmo tese de doutoramento, dado ao seu ineditismo.

Desta forma, o trabalho final proposto e o relatório técnico tiveram a pretensão de apontar, de uma forma sistêmica, as exigências de um novo modelo de *compliance* frente às obrigações trazidas pela LGPD, de uma maneira geral.

## 6 RESULTADOS

A revisão bibliográfica foi uma das primeiras etapas da pesquisa e consistiu em buscar referências teóricas e normativas relevantes.

### 6.1 *Compliance* - A origem

A expressão *compliance* tem origem do verbo *to comply*, que, traduzido ao português, significa atuar de acordo com uma norma, uma lei, uma regra, uma ordem ou um pedido. No mundo empresarial e institucional, e no meio corporativo, *compliance* pode ser entendido como conjunto de ações que visam ao cumprimento das normas legais e regulamentares, das políticas e diretrizes do negócio e das atividades da instituição ou empresa, visando-se, sobretudo, a evitar, detectar e solucionar quaisquer desvios ou inconformidades que venham a acontecer (FEBRABAN, 2009; MORAIS, 2005; SZTAJN; SILVA, 2020).

“Estar em *compliance*” traduz, em suma, o dever de achar-se em conformidade e de fazer cumprir leis, regulamentos e diretrizes, em geral, “com o objetivo de mitigar o risco atrelado à reputação e o risco legal/regulatório” (COIMBRA; MANZI, 2010, p. 2).

No mundo corporativo, empresarial e, também institucional/governamental, a reputação passou a ter importância destacada, com ligação de como os clientes, acionistas ou mesmo os eleitores enxergam a organização. O risco relativo à reputação é, no conceito de Coimbra e Manzi (2010, p. 2), “a perda de rendimento, litígios caros, redução da base de clientes e, nos casos mais extremos, até a falência”.

No mesmo sentido, Maeda (2013, p. 167) assevera que a terminologia referida é adotada, em geral, para “designar os esforços adotados pela iniciativa privada para garantir o cumprimento de exigências legais e regulamentares relacionadas às suas atividades e observar princípios de ética e integridade corporativa”.

De acordo com Manzi (2008), o *compliance* teve origem nas instituições financeiras, com a criação do Banco Central Americano (Board of Governors of the Federal Reserve), em 1913. Logo após a quebra da Bolsa de Nova York de 1929, foi

criada a política intervencionista *New Deal*, em uma tentativa de intervir na economia para “corrigir as distorções naturais do capitalismo”<sup>4</sup>.

Com efeito, muito embora tenha origem no setor bancário, onde obteve progresso exponencial, é certo que o *compliance* é um modelo de gestão que se expandiu para muito além das fronteiras das Instituições Financeiras. Atualmente, existem inúmeros modelos e formatos de *compliance*, a depender da atividade desenvolvida, seja ligado a área empresarial, trabalhista, tributária, bancária, ambiental etc.

Como citado pela referida autora (MANZI, 2008, p. 1), o *compliance* tem vazão e aplicabilidade em todas as organizações, desde empresas do terceiro setor, como entidades de natureza pública, até empresas de capital aberto e empresas fechadas de todas as regiões do mundo.

[...] o *compliance* também apresenta impactos positivos para a imagem e a inserção da pessoa jurídica no mercado, haja vista que a adoção de programas de integridade desperta confiança nos seus parceiros comerciais, consumidores, funcionários, colaboradores e todos aqueles que com ela travam algum tipo de relação jurídica. (OLIVA; SILVA, 2018, p. 2709).

Vale destacar, ainda, que um bom programa de *compliance*, como bem delineado pelos autores citados, deve obedecer e especificar, de forma clara, as fases de implantação e consecução de seus objetos e objetivos. Por exemplo, explica Silva-Sánchez (2003 *apud* HIJAZ, 2016, p. 165), no tocante ao *compliance criminal*, a inserção de critérios gerenciais de relação com riscos deve obedecer a cinco fases de realização:

1) Processo descritivo das condutas lesivas, de perigo concreto ou mesmo abstrato; (2) Descrição das condutas lesivas integradas a determinados contextos, geralmente típicos de bens coletivos; (3) Determinação de indícios; (4) Determinação de indícios de descumprimento idôneos à autorização de um procedimento administrativo sancionador; e (5) Procedimentos de inspeção.

No Brasil, o CADE – Conselho Administrativo e Defesa Econômica, autarquia federal, vinculada ao Ministério da Justiça, com sede e foro no Distrito Federal, exerce, em todo o Território nacional, as atribuições dadas pela Lei nº

---

<sup>4</sup> A importância do *compliance* para a efetivação de medidas anticorrupção no contexto da sociedade de risco e do Direito Penal Econômico Tailine Fátima Hijaz Analista do Ministério Público da União (apoio

12.529/2011, e tem como missão zelar pela livre concorrência no mercado, sendo a entidade responsável, no âmbito do Poder Executivo, não só por investigar e decidir, em última instância, sobre a matéria concorrencial, como também fomentar e disseminar a cultura da livre concorrência.

Nesse diapasão, a fim de guiar a área empresarial, o referido Conselho edita o seu “Guia Programas de *Compliance*”<sup>5</sup>, para a identificação de programas robustos de *compliance* concorrencial, tais como: comprometimento da alta administração; recursos adequados às particularidades da organização (porte, mercado de atuação etc.); autonomia e independência do órgão ou funcionário responsável pela implementação dos programas de *compliance*; análise contínua dos riscos aos quais a entidade está exposta; realização de treinamento e instrução dos colaboradores para a implementação da política de integridade da pessoa jurídica, bem como para a utilização de canais de denúncia; monitoramento contínuo e efetivo do programa; documentação das iniciativas relacionadas ao *compliance*; aplicação de punições internas nas hipóteses de infração às disposições legais e ao Código de Ética da corporação; revisão e adaptação do programa ao longo do tempo e em atenção à modificação das atividades da pessoa jurídica.

Esse é, portanto, o contexto generalizado da origem do *compliance*, sua aplicabilidade e a importância atual dentro das organizações.

## 6.2 *Compliance* e as Instituições Financeiras

O setor de governança e conformidade tem ligação umbilical com as Instituições Financeiras, como outrora mencionado, ao ponto de alguns autores indicarem o surgimento destes mecanismos justamente na área bancária. Em razão disso, as normas aplicadas a este setor evoluíram sobremaneira. Com efeito, vale registrar que a legislação aplicada aos Bancos, e ligada ao sigilo e tratamento dos dados e documentos dos clientes, remonta há muitos anos antes da promulgação da Lei 13.709/2018 – a Lei Geral de Proteção de Dados.

---

jurídico/Direito). Pós-graduada pela Fundação Escola do Ministério Público do Paraná e pela Academia Brasileira de Direito Constitucional. Graduada em Direito pela Universidade do Extremo Sul Catarinense

<sup>5</sup> Cf (CADE. Guia Programas de *Compliance*, pp. 15-29. Fonte: [http://www.cade.gov.br/aceso-a-informacao/publicacoes-institucionais/guias\\_do\\_Cade/guia-compliance-versao-oficial.pdf](http://www.cade.gov.br/aceso-a-informacao/publicacoes-institucionais/guias_do_Cade/guia-compliance-versao-oficial.pdf). Acesso em 22.04.2018 às 17h). V. tb. art. 42 do Decreto 8.420/2015 e o Programa de Integridade: Diretrizes para Empresas Privadas elaborado pela Controladoria-Geral da União (CGU).

As Instituições Financeiras, notadamente após as deliberações do CMN – Conselho Monetário Nacional (a partir de 1994), e depois do Primeiro Acordo de Basileia, de 1988, passaram a adotar procedimentos de controle rígidos a fim de minimizar impactos financeiros decorrentes de riscos operacionais. Já, neste período, entendia-se os riscos aplicados ao manuseio dos dados pessoais. Todavia, nos últimos anos, escândalos têm marcado a vida de grandes bancos, no Brasil e no exterior, com sérias consequências para as organizações, seus empregados e principalmente os clientes.

O caso envolvendo a Enron e a Lehman Brothers, que ocorreram no final do século XX e início do XXI, deixaram marcas profundas na credibilidade das Instituições Financeiras, tanto nos investidores quanto na sociedade em geral. No Brasil, pode-se citar os episódios do Banco Nacional, o qual desaguou em prejuízos superiores a US\$ 9 bilhões<sup>6</sup>, do Banco Marka, do Banestado e, por último, do Banco Rural, citado no caso do mensalão.

Escândalos atacam diretamente a reputação da empresa e, assim, o seu valor de mercado. E a reputação, como outrora exposto, é a linha frontal de defesa do *compliance*, com vista a minimizar diretamente o risco de descontinuidade dos negócios através da implantação de sistemas e métodos de controles que visam à observação das normas referentes ao mercado em que atuam e aos procedimentos internos (SOUZA, 2013).

Assim, tanto o mercado regulatório, quanto os órgãos de controle estatais entenderam a necessidade de implementação de instrumentos de governança e conformidade nas Instituições Financeiras, como órgãos obrigatórios, a fim de dinamizar os riscos ao setor, e minimizar os prejuízos, como nas fraudes outrora verificadas.

No ano de 1998, surge, então, a Resolução BACEN 2554/1998, cujo artigo primeiro, chancelou:

Art. 1º **Determinar às instituições financeiras** e demais instituições autorizadas a funcionar pelo Banco Central do Brasil **a implantação e a implementação de controles internos** voltados para as atividades por elas desenvolvidas, seus sistemas de informações financeiras, operacionais e gerenciais e o cumprimento das normas legais e regulamentares a elas aplicáveis.

---

<sup>6</sup> Cf. ENTENDA o caso do Banco Nacional. In: FOLHA DE SÃO PAULO, São Paulo, domingo, 1 out. 2000. Brasil. Disponível em: <https://www1.folha.uol.com.br/fsp/brasil/fc0110200003.htm>. Acesso em: 15 mar. 2022.

§ 1º Os controles internos, independentemente do porte da instituição, devem ser efetivos e consistentes com a natureza, complexidade e risco das operações por ela realizadas. (GN) (BANCO CENTRAL DO BRASIL, 1998, p. 1, grifo nosso).

Estava, na ocasião, definitivamente criado o sistema obrigatório de conformidade aos bancos, por expressa determinação do Banco Central do Brasil. Paradoxalmente, os sistemas de controle se expandiram a outros segmentos das organizações, como já retratado neste trabalho, como, a exemplo, a Lei Anticorrupção.

A Lei Federal nº 13.303/2016, conhecida como a Lei das Estatais, por seu turno, estabelece a obrigação dos estatutos das empresas públicas, economias mistas (**Banco do Brasil S.A., Banco da Amazônia S.A., Banco do Nordeste S.A. etc**) e suas respectivas subsidiárias, *observar regras de governança corporativa, de transparência e de estruturas, práticas de gestão de riscos e de controle interno*, como destacado em seu artigo 6º. Já o artigo 9º é categórico:

Art. 9º A empresa pública e a sociedade de economia mista adotarão regras de estruturas e práticas de gestão de riscos e controle interno que abranjam: I - ação dos administradores e empregados, por meio da implementação cotidiana de práticas de controle interno;

II - área responsável pela verificação de cumprimento de obrigações e de gestão de riscos;

III - auditoria interna e Comitê de Auditoria Estatutário.

§ 1º Deverá ser elaborado e divulgado Código de Conduta e Integridade, que disponha sobre:

I - princípios, valores e missão da empresa pública e da sociedade de economia mista, bem como orientações sobre a prevenção de conflito de interesses e vedação de atos de corrupção e fraude;

II - instâncias internas responsáveis pela atualização e aplicação do Código de Conduta e Integridade;

III - canal de denúncias que possibilite o recebimento de denúncias internas e externas relativas ao descumprimento do Código de Conduta e Integridade e das demais normas internas de ética e obrigacionais;

IV - mecanismos de proteção que impeçam qualquer espécie de retaliação a pessoa que utilize o canal de denúncias;

V - sanções aplicáveis em caso de violação às regras do Código de Conduta e Integridade;

VI - previsão de treinamento periódico, no mínimo anual, sobre Código de Conduta e Integridade, a empregados e administradores, e sobre a política de gestão de riscos, a administradores. (GN) (BRASIL, 1998, p. 2).

Aos Bancos Públicos, portanto, a implantação de órgãos de controle interno, e Códigos de Conduta e Integridade, é compulsória, diante da Lei das Estatais.

A CVM – Comissão de Valores Mobiliários, importante autarquia federal, que tem a missão de disciplinar, fiscalizar e desenvolver o mercado de valores mobiliários no país, com fortíssima influência sobre as Instituições Financeiras, também prestigia o *compliance* em seus atos normativos. A Instrução CVM nº 586/2017, que alterou a redação da Instrução CVM nº 480/2009, a qual regula o registro de emissores de valores, prevê a obrigação de informar “*se o emissor possui regras, políticas, procedimentos ou práticas voltadas para a prevenção, a detecção e remediação de fraudes e ilícitos praticados contra a administração pública*” (COMISSÃO DE VALORES MOBILIÁRIOS, 2017, p. 24).

Já a Instrução CVM nº 558/2015 (alterada pela Instrução CVM nº 593/2017) impõe, no que tange ao exercício profissional de administração de carteiras de valores mobiliários, exigências acerca da implementação de programas de *compliance*.

Pois bem. Como se vê, o contexto normativo que entrelaça o *compliance* e as Instituições Financeiras é amplo, irrestrito, e navega por diversos atos normativos, desde leis até normas internas de entidades que regulam o setor. Desta forma, para se entender a real importância na gestão do *compliance*, necessário explicar ao leitor, mesmo de forma simplificada, a composição estrutural de um banco, sua gestão, a alta administração e os seus principais atores, e onde a conformidade se posiciona, e atua como elemento decisivo na garantia das boas práticas e do cumprimento das regras.

Para Senas (2013), uma estrutura de Governança, e isso aplicado a uma grande Instituição Financeira, deve conter (estar dividida): **a) Estrutura de suporte aos acionistas**, formada por: conselhos; comitê de auditoria; auditoria interna e auditoria externa; **b) Estrutura de suporte à gestão**, formada por: gerenciamento de risco, controles internos, *compliance* e jurídico.

A conformidade, portanto, tem assento como órgão de suporte à gestão do Banco, à Alta Administração.

O Instituto Brasileiro de Governança Corporativa – IBGC, organização sem fins lucrativos, referência nacional e internacional em governança e que contribui para o desempenho sustentável das organizações, em seu Código de Melhores Práticas (IBGC, 2009, p. 19), indica:

Governança Corporativa é o sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre proprietários, Conselho de Administração, Diretoria e **órgãos de controle**. As boas práticas de Governança Corporativa convertem princípios em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor da organização, facilitando seu acesso ao capital e contribuindo para sua longevidade.

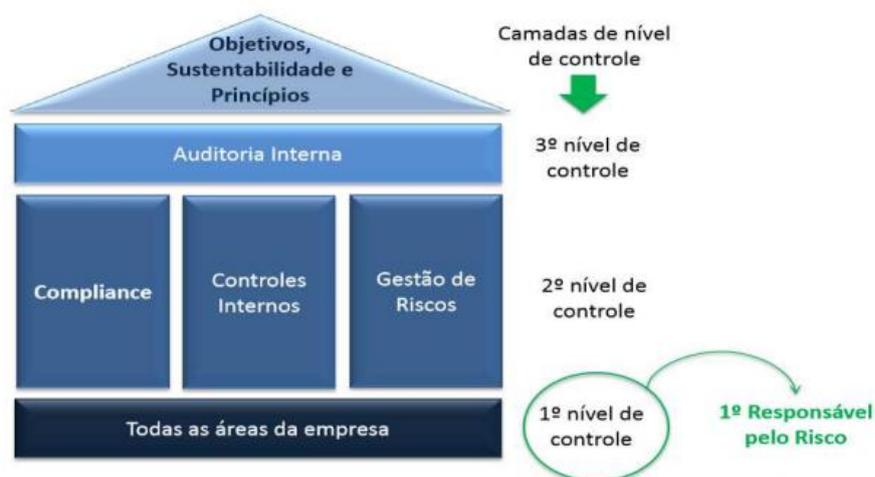
De acordo ainda com o IBGC (2009), os princípios básicos de Governança Corporativa são transparência (*disclosure*), equidade (*fairness*), prestação de contas (*accountability*) e, justamente, a **responsabilidade corporativa (*compliance*)**.

Ainda na fase embrionária, muitas organizações iniciaram a implantação de um modelo de *compliance* ligado às assessorias jurídicas, ante a ligação com atos normativos, regulamentos e as consequentes fiscalizações. Doravante, viu-se que, em verdade, tratava-se de um nítido modelo de gestão, a qual deveria estar inclusa nos processos. O gestor do *compliance*, muito além de editar normas e procedimentos, tem inúmeras outras atribuições, principalmente exigindo e cobrando responsabilidades aos gestores das diversas outras áreas da empresa.

Segundo Coimbra; Manzi (2010 *apud* SOUZA, 2013, p. 18):

[...] as responsabilidades do *compliance* são: assegurar, em conjunto com as demais áreas, a adequação, o fortalecimento e o funcionamento do sistema de controles internos, procurando mitigar riscos de acordo com a complexidade de seus negócios, bem como disseminar a cultura de controles para assegurar o cumprimento das leis e regulamentos existentes. Além disso, verifica e monitora as alterações no ambiente regulatório, tais como normas do órgão regulador, autorregulação, entre outras, bem como as alterações produzidas por novos produtos lançados, e informa às áreas envolvidas as alterações nas estruturas de controles internos.

**Figura 1 - O Compliance como Pilar da Governança em Mercados Regulados**



Fonte: (ALVES, 2013).

**Figura 2 - Tendências, Perspectivas e desafios de *Compliance***



Fonte: (SENAS, 2013).

As projeções dos organogramas, acima, indicam que, para a implantação, funcionamento, gerenciamento e obtenção de resultados de um programa de *compliance*, há a necessidade da interlocução deste com todas as demais áreas da Instituição Financeira. Não há programa eficaz sem o comprometimento da Alta Administração da empresa, em validar, acompanhar e fiscalizar um bom sistema de controle interno, e, principalmente, se submeter a ele.

Segundo Candeloro; Rizzo; Pinho (2012, p. 69 *apud* SOUZA, 2013, p. 22-23):

A Alta Administração deverá acompanhar periodicamente o programa de *Compliance* implementado na instituição que – juntamente com um sistema de Controles Internos adequado à estratégia de negócios adotada – maximizará o retorno do investimento, proporcionará segurança ao ambiente operacional e maior confiabilidade na instituição. Devido a esse suporte, a área de *Compliance*, ganha adequada estrutura administrativa de apoio, independência funcional e respeito para evitar conflitos de interesses e assegurar a isenta e atenta leitura dos fatos, buscando conformidade por meio de ações preventivas e corretivas.

Outro ponto fundamental é estabelecer e diferenciar a conformidade com a auditoria. O *compliance* fala com o setor de Auditoria Interna, e suas atividades são complementares. A Auditoria desempenha suas funções de forma aleatória e periódica, de forma amostral, e fiscaliza o cumprimento das normas internas e

externas instituídas pela empresa, e a eficácia dos controles. Já no *compliance*, a atuação é permanente, ao vigiar e monitorar todos os segmentos e departamentos da Instituição Financeira, e verifica a sua conformidade com as normas aplicáveis ao modelo de negócio desempenhado.

Essas áreas contribuem para a identificação de fragilidades nos controles internos e promovem uma cultura de correção dos pontos de não conformidade, por meio de reporte para a Alta Administração. O *compliance* engloba o acompanhamento dos pontos falhos identificados na auditoria até a sua regularização, configurando essa uma das interseções das duas áreas.

O *compliance* faz parte da cultura organizacional, podendo executar processos e implantar controles. Ao contrário da auditoria, responsável por avaliar a estrutura de controles internos, devendo, assim, não se envolver na execução de processos e na definição de controles. Portanto, a área de *compliance*, assim como as demais unidades da organização, devem ser objetos de avaliação da auditoria interna.

Por meio da auditoria do *compliance*, é possível avaliar se a função foi estruturada de acordo com o porte da organização, se há independência para que a área desenvolva um trabalho preventivo de identificação de possíveis não conformidades. E, principalmente, avaliar se as demais áreas da organização estão assumindo as suas responsabilidades em relação ao *compliance*. (GN) (SOUZA, 2013, p. 22-23).

O *compliance* tem ligação direta, também, com as áreas de Gestão de Riscos e Controles Internos, com o objetivo de reduzir perdas potenciais e melhorar o fluxo de processos internos, por exemplo. Tem estreita ligação com a área jurídica da Instituição, pois ambas têm como missão fazer com que a empresa cumpra os atos normativos, sejam internos ou externos. Todavia, a área de atuação do *compliance* é mais abrangente, visto que inclui a aplicação e fiscalização de normativos muitas vezes não direcionados às assessorias jurídicas, como por exemplo, do Código de Ética, os códigos de melhores práticas etc.

Além disso, ressalta Candeloro, Rizzo e Pinho (2012), as áreas (*compliance* e jurídico) podem muitas vezes ter visões antagônicas sobre o mesmo fato, e opinar divergentemente. Uma Instituição Financeira com missão no desenvolvimento sustentável pode, ao fim e ao cabo, deixar de financiar uma atividade potencialmente poluidora que, sob o aspecto jurídico seria viável, todavia, poderia se voltar em face dos valores éticos e morais da empresa, quando alertada pelo *compliance*.

Desta forma, é extremamente importante que estas áreas se complementem, todavia sempre com um destaque à independência e soberania da

área do *compliance*, a fim de garantir o efetivo cumprimento das normas e os objetivos da instituição.

Nas áreas comerciais e de recursos humanos, das Instituições Financeiras, também há forte impacto da atuação do *compliance*. Na venda dos produtos bancários, as decisões operacionais e as estratégias de atuação das unidades jurisdicionadas (agências) podem se valer de consultas, a fim de evitar aplicação de penalidades. Na formação do cadastro do cliente, a obtenção dos dados e origem dos recursos do mutuário é fundamental, para evitar o crime de lavagem de dinheiro previsto na Lei 12.846/2013, a qual sujeita o banco a pesadíssimas multas. Já na área de recursos humanos, a adesão de todos os empregados, terceirizados, e fornecedores, ao Código de Ética da empresa, faz parte da missão do *compliance*.

Como se vê, portanto, a conformidade tem ligação estreita com todos os demais atores dentro da Instituição, até em razão do controle e fiscalização exercidos, mesmo que em diferentes níveis. E, a verticalidade da atuação do *compliance* irá depender do quão longe quer chegar a empresa (do Banco, no caso), diante do cenário e objetivos delineados e frente a gestão e análise dos riscos do mercado.

### **6.3 Compliance e a Inovação**

Segundo o Manual de Oslo, inovação é a introdução de um bem ou serviço novo ou significativamente melhorado, no que se refere às suas características ou usos previstos, ou ainda, à implementação de métodos ou processos de produção, distribuição, marketing ou organizacionais novos ou significativamente melhorados (OCDE, 2004).

Inovar, oportunizar o crescimento da empresa, mas de forma organizada, sustentável e em conformidade. Este é o desafio das organizações, hodiernamente, e aqui o *compliance* e a inovação se entrelaçam. Para Doyle *et al*, 2019, a sustentabilidade é abordada no contexto amplamente definido, ou seja, baseia-se na capacidade de uma organização equilibrar as necessidades de curto e longo prazo das partes interessadas.

Como já registrado em linhas pretéritas, o *compliance*, no Brasil, ainda é embrionário. Iniciou-se, timidamente, nos anos 1990, com modelos estrangeiros. E, ao certo, para tomar fôlego e gerar resultados, depende de um processo crucial de

aculturação tanto das empresas quanto dos empregados nos tempos atuais. (SAMPAIO, 2019).

No cenário legal, normativo, a conformidade ganhou força com a edição da Lei Federal 12.846/2013, a qual dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, a chamada Lei anticorrupção. Referida norma trata da responsabilização administrativa e civil de pessoas jurídicas (empresas) pela prática de atos de corrupção contra a administração pública, nacional ou estrangeira, e atende ao pacto internacional firmado pelo Brasil. O objetivo é coibir a atuação de empresas em esquemas de corrupção e assim, evitar que grandes prejuízos sejam causados aos cofres públicos.

A lei em gênese prestigiou e incentivou as empresas a aplicarem mecanismos de conformidade em suas estruturas, eis que, caso existentes, tal particularidade será considerada em caso de aplicação de penalidade, conforme teor do artigo 7º:

Art. 7º Serão levados em consideração na aplicação das sanções:

[...]

VIII - a existência de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e a aplicação efetiva de códigos de ética e de conduta no âmbito da pessoa jurídica; (GN) (BRASIL, 2013, p. 2).

Crescer, inovar, mas com responsabilidade e em *conformidade*: esta é a pedra nevrálgica do sistema atual. Por isso, o *compliance* e toda sua rede é o assunto dominante, atualmente, no mundo corporativo. A gestão e o cumprimento das normas devem estar alinhados aos objetivos finalísticos da organização, e não ser enxergado, dentro e fora da empresa, como um fator inibidor da inovação ou até mesmo bloqueador no âmbito comercial em detrimentos do grau de cumprimento e exigências legais e normativas (GIOVANINI, 2014).

É inegável, d'outro turno, a expressiva valorização de uma organização que consegue aplicar o *compliance* em sua estrutura. Tanto a doutrina sobre a temática, como a própria regulação do mercado, é uníssona em afirmar tal particularidade. Estar em conformidade, como requisito de boa prática de mercado, bem como atender à fornecedores e parceiros comerciais que exigem este requisito

como condição para o relacionamento, favorecem o mercado atual a, cada vez mais, aderir a programas desta natureza.

Por outro lado, os riscos da empresa não estar em *compliance* é considerável. Como registram Isaac Danon Junior; Guizzo; Nogueira (2019) no artigo “*Compliance no Contexto de Inovação: uma revisão da literatura internacional*”:

Outro ponto relevante a mencionar é a questão do risco que empresas privadas podem estar sujeitas, quando da relação com parceiros comerciais e fornecedores, ou seja, risco de envolverem-se em situações de fraudes, ilicitudes etc., sem contar com a possibilidade da empresa ser arrolada em investigações e para tanto faz-se necessário conhecer e entender os tipos riscos de *compliance* que a empresa está exposta para mitigá-los, pois estes riscos podem impactar consideravelmente a sua reputação, imagem ou até mesmo a sua sustentabilidade no mercado. (ASSOCIAÇÃO BRASILEIRA DE BANCOS INTERNACIONAIS, 2009 *apud* DANON JUNIOR; GUIZZO; NOGUEIRA, 2019, p. 3).

Dito isso, registre-se que qualquer ato e/ou conduta não ética em todas às áreas da empresa pode sim contribuir para a lista de riscos de *compliance* a exemplificar e relacionados abaixo: corrupção ativa e passiva; assédio moral; assédio sexual; fraudes; desvio e lavagem de dinheiro; favorecimento em processos licitatórios; cultura organizacional; evasão fiscal: venda sem documentação fiscal; ausência de recolhimento de taxas/encargos trabalhistas; não pagar empregados "por fora" ou sem o contrato formal; não nomear empregados para cargos de gestão apenas por empatia, sem atentar aos requisitos técnicos para a função previstos no plano de cargos e salários da empresa; não se pôr em situação de conflitos de interesses; riscos de imagem etc. (GN) (DANON JUNIOR; GUIZZO; NOGUEIRA, 2019, p. 3).

Nesse contexto, como destacado, inovação e conformidade se entrelaçam. É propiciar o crescimento, com responsabilidade e dentro das normas, com sustentabilidade:

[...] um complexo ecossistema tecnológico demanda contínua inovação em conformidade um amplo regramento, que envolve, entre outras coisas, investimento em segurança e privacidade de dados. **Ao contrário do pensamento tradicional industrial, *compliance* hoje pode ser uma área extremamente inovadora e flexível em qualquer negócio, sem intenção de frear, impor ou dificultar processos, muito pelo contrário, é o olhar que corre juntamente com a inovação para garantir a sustentabilidade do que conquistamos até aqui e a segurança das coisas incríveis que ainda lançaremos** (GOMES, 2018, grifo nosso).

E os exemplos estão no mercado. No início de 2022, na Microsoft, a tentativa de venda da tecnologia holográfica ao exército barrou em uma séria de manifestações públicas, principalmente dos engenheiros e programadores da

empresa. Na ocasião, os profissionais assinaram um manifesto afirmando discordar que o fruto do seu trabalho fosse direcionado a fins bélicos. A comercialização, sob o prisma legal, era perfeita. Todavia, deixou de atender aos valores morais e éticos da organização, na visão dos engenheiros e programadores, talvez o maior ativo da empresa. Já em 2018, a Google refluíu de um contrato bilionário, face a uma situação análoga. Na ocasião, a empresa assinara um contrato de parceria com o Pentágono, conhecido como *Project Maven*, o qual utilizava a inteligência artificial, a partir da captação de imagens por drones, para identificar alvos inimigos com maior precisão e rapidez. À época, mais de três mil colaboradores da empresa assinaram uma carta exigindo a ruptura do contrato, o que, mais tarde, acabou ocorrendo. E, no Brasil, o caso envolvendo a Hering é emblemático, quando a empresa foi notificada para justificar e esclarecer sobre seu sistema de reconhecimento facial, sob pena de aplicação de multa que pode chegar a R\$ 9,7 milhões (SCHRAMM, 2019).

Em conclusão, é preciso inovar, mas em conformidade. Essa é a métrica.

#### **6.4 Compliance e a LGPD**

Como retratado em linhas volvidas, a cultura da conformidade no mundo das grandes corporações, no Brasil, ainda é incipiente. Nas Instituições Financeiras, dado ao regramento específico do BACEN, através de atos normativos próprios, o surgimento foi acelerado, todavia, no meio empresarial, a aplicação ainda cede diante da *pseudo* crença dos elevados custos.

A Lei Anticorrupção foi um importante marco legal, para a natureza obrigatória do *compliance*, e, agora, a Lei 13.709/2018 – a Lei Geral de Proteção de Dados, veio como um importante incentivo ao mercado para, definitivamente, a conformidade entrar na estrutura das organizações, como esteio ao seu funcionamento e propagador de resultados.

Todas as empresas, indistintamente, públicas ou privadas, passam a ter responsabilidade sob a governança das informações que detém, sobre os dados pessoais que guardam, e eventual vazamento, ou a espoliação destes, é punida com severidade. O objetivo da LGPD foi de proteger o cidadão contra o chamado uso disfuncional de seus dados, e lhes garante o poder de fiscalizar e controlar suas informações. A nova lei exige, outrossim, a autorização do proprietário para a divulgação e disponibilização de seus dados, de forma expressa, consciente e

inequívoca, o que exige um rígido, independente, adequado e estruturado setor, dentro da empresa.

Com efeito, a partir da vigência da lei, todo o sistema normativo interno da empresa, caso existente, deve, necessariamente, ser reestruturado. Novos códigos de conduta, as rotinas dos processos internos e tráfego dos dados, devem ser revistos e atualizados, de acordo com o tratamento dos dados exigidos pela norma. O compartilhamento e a eventual divulgação dos dados, agora, exige o máximo controle.

Comentam Ana Frazão, Milena Oliva e Vivianne Abilio:

Nesse cenário em que, por um lado, vislumbram-se profundas alterações na lógica até então vigente quanto ao tratamento de dados e, por outro, objetiva-se conferir papel primordial na efetividade dos direitos e na prevenção de danos, a adoção de mecanismos de *compliance* consubstancia valioso instrumento desse viés operacional e preventivo, auxiliando na promoção de condutas compatíveis com a regulamentação legal. (FRAZÃO; OLIVA; ABILIO, [2019], p. 682).

Nas Instituições Financeiras, o setor de cadastro é o responsável por arrecadar e armazenar todos os documentos do cliente. E, a partir de então, da análise destes, é que os negócios jurídicos são impulsionados. Daí a importância de se estabelecer um rigoroso aprimoramento na rotina do tratamento dos dados pessoais, posto que, a má gestão deste setor, poderá desaguar em um descumprimento legal em cascata, e consequências imprevisíveis à empresa.

A implantação de um rígido modelo de *compliance*, para tratar estes dados, e dar conformidade às normas editadas pela Lei 13.709/2018, é medida que se impõe, notadamente às Instituições Financeiras.

## **6.5 A Lei de Dados Pessoais em um panorama geral e no contexto histórico**

Importante registrar, inicialmente, que o sistema brasileiro de proteção de dados seguiu, em muito, o modelo europeu. As primeiras leis, ainda prematuras e sem verticalidade, surgiram na Alemanha e na Suécia, ainda nas décadas de 1960 e 1970. Passados os anos, e diante de um mercado avassalador, inúmeros países passaram a legislar sobre a matéria, até que a União Europeia promulgou a Diretiva 95/46/CE, em 1995. A norma foi um marco no campo da proteção de dados, e dispôs sobre o tratamento de dados e direitos dos usuários em todos os países membros do

bloco, colocando todos sob a mesma legislação (MONTEIRO *et al.*, [2019]; PARLAMENTO EUROPEU, 1995).

A referida Diretiva, à época, já trazia muitos dos direitos e proteções hoje projetadas nas legislações, como a forma e o tratamento dos dados, os princípios informadores da norma, a transparência, a intimidade, dentre outros. Esta norma vigorou até maio de 2018, quando entrou definitivamente em vigor o Regulamento nº 2016/679, de 27 abril de 2016, conhecido como *General Data Protection Regulation* (“GDPR”), a nova lei geral de proteção de dados da União Europeia.

A GDPR é reconhecidamente a lei de maior proteção de dados pessoais do mundo. A sua rede de proteção se estende para além das fronteiras da União Europeia, e atinge dados de qualquer país que, de alguma forma, possui contato com o mercado europeu.

Pois bem. A importância e o valor dos dados pessoais, a sua monetização, são assuntos que há tempos afligem o mercado. Ana Frazão, ao citar a revista *The Economist*, em manchete ainda de 2017, menciona:

A manchete da capa da revista *The Economist* de 06.05.2017<sup>7</sup> – *The world’s most valuable resource* –, **ao apontar os dados pessoais como os principais recursos econômicos da nossa época**, revela importante ponto de partida para a compreensão da necessidade de proteção dos dados pessoais.

**Vistos já como o novo petróleo**, os dados são hoje insumos essenciais para praticamente todas as atividades econômicas e tornaram-se, eles próprios, objeto de crescente e pujante mercado. Não é sem razão que se cunhou a expressão *data-driven economy*, ou seja, economia movida a dados, para designar o fato de que, como aponta Nick Srnicek, o capitalismo do século XXI passou a centra-se na extração e no uso de dados pessoais<sup>8</sup> (FRAZÃO, [2019a], p. 23, grifo nosso).

É fato que, no Brasil, diante de um novel e desconhecido cenário, a exemplo do resto do mundo, era premente a necessidade de uma legislação especial para tratamento e defesa deste novo *patrimônio*. A importância dos dados pessoais transcendeu ao aspecto meramente financeiro, dado à forma e a velocidade de como as informações passaram a circular, no mundo globalizado. E, assim, o contexto reclamou a edição de um novo arcabouço legal, que dessa efetiva proteção aos dados pessoais, e que passaram a integrar, de forma efetiva, os direitos da personalidade, e

---

<sup>7</sup> Cf. JOSSEN, Sam. The data economy demands a new approach to antitrust rules: The data economy demands a new approach to antitrust rules. *The Economist*, 6 maio 2017. Disponível em: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.

por isso, tornaram-se vetores das vidas e das liberdades individuais, assim como da sociedade e da própria democracia (FRAZÃO, [2019b]).

Vale ressaltar, também, outro fator importante neste cenário. A monetização dos dados pessoais criou um sistema nefasto, muito relacionado à coleta, circularização e comercialização destes junto à internet. Algoritmos são diariamente atualizados para rastrear dados e captar informações que, em sua grande maioria, são ignorados pelos usuários.

Neste panorama surgem também os governos e os denominados grandes *players* econômicos, como descrito por Frank Pasquale, notórios usurpadores dos dados pessoais. As autoridades do executivo desenvolvem sistemas de rastreamento, para um monitoramento e vigília constantes sobre cada passo da vida das pessoas, o que leva a um verdadeiro capitalismo de vigilância, cuja principal consequência é a constituição de uma sociedade também de vigilância (FRAZÃO, [2019b]; PASQUALE, 2015. p. 9).

Sob tal prisma, percebe-se, então, que os direitos relacionados aos dados não se relacionam, somente, com a com a propriedade do nome e as informações pessoais, mas são muito mais extensos. O direito à privacidade e à intimidade tem ligação intrínseca nessa seara, além dos direitos ligados à personalidade.

Pasquale (2015) afirma que os controladores de dados criaram um sistema desenhado não para tratar os titulares de dados decentemente, mas sim para maximizar seus lucros ou colocar a inovação acima de qualquer outro valor. E, nessa linha conceitual, Frazão ([2019b]) define que o objetivo central da LGPD é resgatar a dignidade dos titulares de dados e seus direitos básicos relacionados à autodeterminação informativa.

E é neste conturbado cenário, diante da mercantilização dos dados pessoais frente à extrema urgência de sua proteção, que surge, no ano de 2018, já com certo atraso, a Lei Federal 13.709.

Após 48 anos da existência da primeira lei de proteção de dados no mundo, o Brasil passa a ter a sua lei geral de proteção de dados. Com a aprovação da LGPD, há forte expectativa de uma promoção maior de direitos e garantias para os cidadãos, no meio online e offline, de forma a, espera-se, resguardar direitos individuais e fomentar a inovação por meio do estabelecimento de regras claras, harmônicas e transparentes. (MONTEIRO, *et al.*, [2019], p. 12).

---

<sup>8</sup> Cf. SRNICEK, Nick. Platform capitalism. Cambridge: Polity Press, 2018. p. 39.

E a Lei, já em seus artigos 1º e 2º, estabelece os direitos protegidos pela norma:

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, 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 e o livre desenvolvimento da personalidade da pessoa natural.

Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. [\(Incluído pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:  
I - o respeito à privacidade;  
II - a autodeterminação informativa;  
III - a liberdade de expressão, de informação, de comunicação e de opinião;  
IV - a inviolabilidade da intimidade, da honra e da imagem;  
V - o desenvolvimento econômico e tecnológico e a inovação;  
VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e  
VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, 2018, p. 59).

Percebe-se, claramente, a extensão dos direitos atingidos pela legislação, não resumidos, unicamente, à dados. Para muito além da simples propriedade do dado pessoal, a novel legislação trouxe a privacidade, a liberdade, a inviolabilidade da intimidade, entre outros, como vetores pragmáticos que informam a aplicação da lei, além do desenvolvimento econômico e tecnológico, e, claro, da inovação.

Os princípios que norteiam a aplicação da Lei também mereceram tratamento especial, no caso pelo artigo 6º, onde indica:

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. (GN) (BRASIL, 2018, p. 60, grifo nosso).

Observa-se que a Lei, de uma maneira geral, objetivou a proteção integral de todas as situações que envolvem tratamento de dados, assim definidas no art. 5º, X, da Lei 13.709/2018:

[...] 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; (BRASIL, 2018, p. 60).

Diante da amplitude das relações tratadas pela LGPD, e da extensão dos direitos por ela protegidos, é que na doutrina assentou-se ter sido acolhida a chamada *concepção convergente*, citado por Stefano Rodotá e por Ana Frazão, de que a proteção de dados consiste em verdadeiro direito fundamental autônomo, expressão da liberdade e da dignidade humana, que está intrinsecamente relacionada à impossibilidade de transformar os indivíduos em objeto de vigilância constante. (FRAZÃO, [2019b]; RODOTÁ, 2008).

A ideia de concepção convergente, enquanto protecionista de uma gama de direitos ligados ao nome e aos dados dos cidadãos vencem, ao menos por ora, uma visão minimalista ou chamada “proprietária”, dos dados pessoais, a qual enxerga somente uma análise míope e estritamente negocial deste universo.

Assim, a Lei 13.709/2018, após longos anos de debates, foi promulgada, venceu seu período de vacância e, após períodos de adiamentos, finalmente entrou em vigor, em 18 de setembro de 2021.

## 6.6 As exigências legais trazidas pela LGPD ao setor bancário

O contexto e a dinâmica do trabalho, aqui apresentado, são voltados ao setor bancário. A LGPD, todavia, não excepciona este segmento, ou o mercado financeiro, de maneira especial, o que lança as Instituições Financeiras na vala comum daquelas organizações que devem seguir os padrões de regulação geral da norma.

A Lei Geral de Proteção de Dados foi criada, em suma, para regradar a *coleta, o tratamento, o armazenamento e o compartilhamento* dos dados pessoais. Este é o sentido e o objetivo da norma. E o trabalho, aqui desenvolvido, é apontar quais as exigências reclamadas pela lei às Instituições Financeiras e, ao final, como o *compliance* pode auxiliar, como governança, a dar o efetivo cumprimento aos rigores da norma.

Para o bom entendimento quanto às exigências da lei, convém esclarecer o que são *dados*, na concepção legal. O conceito de dados, e suas diferenças, são estabelecidos pelo artigo 5º, da Lei 13.709/2018:

Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; (BRASIL, 2018, p. 60).

A lei criou três espécie de dados, e a sua diferenciação é vital para dar aplicabilidade prática à norma. De antemão, percebe-se que os dados bancários não são classificados como dados *sensíveis* (art. 5º, II), o que lhes retira de uma forma diferenciada de tratamento. Isso por que, os dados pessoais sensíveis mereceram, por parte do legislador, uma forma particular de gerenciamento, em especial e como requisito preponderante o consentimento do proprietário. Nenhum controlador<sup>9</sup> pode

---

<sup>9</sup> Cf. Art. 5º da lei 13.709/2018. (Para os fins desta Lei, considera-se: [...] VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais).

legalmente tratar um dado sensível sem o consentimento do titular, salvo as exceções legais trazidas no art. 11, II, da LGPD.

Em que pese alguma divergência, é assente na doutrina não estarem os dados bancários inseridos entre os dados pessoais sensíveis. Primeiro por que o rol descrito no artigo 5º, II, da Lei apresenta um *rol taxativo*, e, diante do recrudescimento da norma, com relação a estes, as obrigações não podem ser estendidas, sem prévia definição legal, tudo em homenagem ao princípio da legalidade e na boa prática da hermenêutica jurídica (normas restritivas de direitos devem, em princípio, sofrerem interpretação restritiva).

Sob outro ângulo, a do direito comparado, a *General Data Protection Regulation* (“*GDPR*”), em seu artigo 9º, encontra idêntica definição, indicando e classificando os mesmos dados como sensíveis, e excluindo os dados bancários desta definição.

Isso não retira, sobremaneira, a importância dos dados bancários no contexto legal, e as inúmeras exigências havidas nas diversas leis extravagantes, e que regulamentam e impõe à atividade bancária um grande conjunto de exigências ao tratamento de informações desta natureza. A Lei 4.595/64 (Lei do Mercado Financeiro), e a Lei Complementar 105/2001, conhecida como a Lei do Sigilo Bancário são, a despeito de inúmeras outras, exemplos das normas legais impostas ao setor bancário, e que protegem os dados dos clientes.

Todo este arcabouço legal se inclina, a exemplo da LGPD, ao tratamento e à proteção dos dados pessoais, e tem nestes – os dados bancários, como o principal objetivo da norma. Vale citar, ainda a título de exemplo, as normas de prevenção à lavagem de dinheiro e financiamento ao terrorismo, e de combate à corrupção, todas aplicáveis ao setor bancário.

Com efeito, ao fim e ao cabo, as Instituições Financeiras tratam dos dados pessoais, assim definidos aqueles insertos no artigo 5º, I, da LGPD.

No contexto do presente estudo, há que se diferenciar as exigências gerais, trazidas pela LGPD, e aplicadas indistintamente a todos os destinatários da norma, daquelas específicas, aplicadas ao setor bancário, e identificadas através da subsunção do texto legal aos contratos bancários e o tratamento de dados dos clientes. A LGPD, assim como uma parte considerável das leis, traz em seu bojo normas *regras gerais, normas programáticas e princípios*, os quais, em que pese um

alto grau de abstração, orientam a aplicação da lei e devem ser rigorosamente seguidos pelos destinatários.

As normas programáticas são:

[...] aquelas em que o constituinte não regula diretamente os interesses ou direitos nela consagrados, limitando-se a traçar princípios a serem cumpridos pelos Poderes Públicos (Legislativo, Executivo e Judiciário) como programas das respectivas atividades, pretendendo unicamente à consecução dos fins sociais pelo Estado (DINIZ, 1998, p. 371).

Veja que o artigo 1º, parágrafo único<sup>10</sup>, da Lei 13.709/2018, estabelece que “[...] As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios [...]” (BRASIL, 2019, p. 1). O legislador deixou claro que as exigências da lei devem ser cumpridas pelo Estado, e seus princípios orientam, inclusive, eventuais novas legislações que surgirem sobre a temática.

Já as regras e princípios tem conceitos diversos. Na doutrina de Luiz Flávio Gomes:

O Direito se expressa por meio de normas. As normas se exprimem por meio de regras ou princípios. **As regras disciplinam uma determinada situação; quando ocorre essa situação, a norma tem incidência; quando não ocorre, não tem incidência. Para as regras vale a lógica do tudo ou nada (Dworkin).** Quando duas regras colidem, fala-se em “conflito”, ao caso concreto uma só será aplicável, pois uma afasta a aplicação da outra. O conflito entre regras deve ser resolvido pelos meios clássicos de interpretação: a lei especial derroga a lei geral, a lei posterior afasta a anterior etc... **Princípios são as diretrizes gerais de um ordenamento jurídico, ou parte dele.** Seu aspecto de incidência é muito mais amplo que o das regras. Entre eles podem haver “colisão”, não conflito. Quando colidem, não se excluem. Como “mandados de otimização” que (Alexy), sempre podem ter incidência em casos concretos, às vezes concomitantemente dois ou mais deles (GOMES, 2005, [s.p], grifo nosso).

Como exposto pelo doutrinador, os princípios são as normas com o teor mais elevado de generalidade e abstração, não interagem com o caso concreto, mas devem ser seguidos fundamentalmente pelos destinatários da norma. A LGPD cuidou, em dois artigos específicos, dos fundamentos e *princípios* informadores da norma:

Art. 2º A disciplina da proteção de dados pessoais tem como **fundamentos**:

<sup>10</sup> Incluído pela Lei nº 13.853, de 2019.

- I - o respeito à privacidade;
- II - a autodeterminação informativa;
- III - a liberdade de expressão, de informação, de comunicação e de opinião;
- IV - a inviolabilidade da intimidade, da honra e da imagem;
- V - o desenvolvimento econômico e tecnológico e a inovação;
- VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
- VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (GN) (BRASIL, 2018, p 59)

E no artigo 6º:

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. (GN) (BRASIL, 2018, p 59-60).

Os fundamentos e princípios são, portanto, informadores da lei, e que devem ser seguidos por todos, independentemente do modelo de função ou gestão desenvolvido pelo controlador dos dados.

Superado o plano abstrato, e sob tal prisma legal, surge, então, no plano prático, a primeira grande exigência às Instituições Financeiras, que é a busca pela **base legal** específica, para o tratamento e gerenciamento dos dados pessoais. As bases legais são as hipóteses legais que autorizam alguém (no caso o controlador) a

realizar o tratamento do dado. A lei, no caso, criou condições determinadas para que seja possível fazer a coleta e o tratamento dos dados pessoais.

Na doutrina de Laura Schertel Mendes:

Para que um tratamento de dados pessoais seja considerado legítimo, é preciso que sejam atendidas as seguintes condições:

i) o tratamento de dados deve se amparar em uma das bases legais previstas no art. 7º ou no art. 23 da LGPD; e

ii) o tratamento de dados deve levar em conta os princípios previstos no art. 6º da LGPD, entre eles, a boa-fé objetiva, a finalidade e a necessidade. Pressuposto fundamental da lei é de que o tratamento de dados só poderá ser realizado se houver base legal que o autorize. Assim, os tratamentos de dados pessoais somente serão legítimos quando se enquadrem em ao menos uma das hipóteses previstas no art. 7º ou no art. 23 da LGPD, totalizando 11 hipóteses autorizativas para o tratamento de dados pessoais. (MENDES, 2019, p. 47).

Importante registrar, também, que as únicas hipóteses de exclusão (inexistência de base legal) estão previstas no art. 4º, da Lei. E, ainda, no caso das exceções do inciso III (para fins exclusivos de segurança pública; defesa nacional; segurança do Estado; ou atividades de investigação e repressão de infrações penais), há a previsão de lei específica para sua regulamentação, dada a importância da matéria.

E, assim, as bases legais (condições) estão estabelecidas no artigo 7º da norma:

### **Seção I**

#### **Dos Requisitos para o Tratamento de Dados Pessoais**

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 terceiro;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; [\(Redação dada pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, 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. (GN) (BRASIL, 2018, p 60, grifo nosso).

**Tabela 2 -Bases Legais da LGPD**

<b>HIPÓTESES DE TRATAMENTO DE DADOS</b>	<b>DEFINIÇÃO</b>	<b>BASE LEGAL</b>
Consentimento do titular	Consentimento para tratamento dos dados pessoais deverá ser livre e inequívoco	art 7, I, LGPD
Cumprimento de obrigação legal ou regulatória	Pode ocorrer por força de lei anterior ou para garantir a ordem e segurança social	art 7, II, LGPD
Uso compartilhado de dados pela administração pública	Feito com a finalidade específica da execução de política pública formalmente instituída por Lei ou Ato administrativo.	art 7, III, LGPD
Realização de estudos e pesquisas	Tratamento para pesquisas ou estudos para saúde pública ou programas de governo	art 7, IV, LGPD
Execução ou preparação de contrato	Fazer parte de contrato consentimento específico do titular para utilização de negócio jurídico em que seja parte	art 7, V, LGPD
Exercício de direitos em processos judicial, administrativo ou arbitral	Feito com a finalidade específica de lei anterior ou para garantir a ordem e segurança social	art 7, VI, LGPD
Proteção da vida ou da incolumidade física	Tratamento de dados em favor do titular do dado em casos de necessidade de tutela do bem maior da pessoa natural	Art. 7, VII, LGPD
Tutela da saúde do titular	Única hipótese de tratamento de dado manejado por agente exclusivo profissional de saúde, serviços de saúde ou autoridade sanitária	Art. 7, VIII, LGPD
Legítimo interesse	Previsão geral e subsidiária mediante previa e expressa motivação pelo controlador da finalidade e necessidade (legítimo interesse) do tratamento	Art 7. IX, LGPD
Proteção do crédito	Tratamento para proteção e manutenção do crédito	Art. 7. X, LGPD

Fonte: (10 BASES..., 2020).

Para o trabalho aqui retratado, serão olvidados os casos de tratamento previstos nos artigos 11 (tratamento de dados sensíveis) e 23 (tratamento de dados pessoais pelas pessoas jurídicas de direito público).

Tratando-se de Instituições Financeiras, há que se ter em mira a existência de um contrato jurídico preexistente, ou a ser firmado, entre o cliente/consumidor e a Instituição Financeira. A isso se aplica tanto aos contratos em andamento quanto aqueles a serem assinados, já no decorrer da vigência da Lei Geral de Proteção de Dados. O contrato bancário, conceitualmente, e de forma reduzida, é aquele que tem por objetivo a intermediação do crédito.

Nesse sentido, para que o agente financeiro analise, de forma ampla e irrestrita, a viabilidade de concessão do crédito/financiamento ao cliente, há, em

regra, *cláusulas contratuais* onde o cliente aporta e oferece ao banco toda a sua documentação pessoal (documentos pessoais em geral), além de sua documentação financeira (declarações de renda, patrimônio etc). E, para além disso, autoriza a Instituição Financeira a realizar uma ampla investigação, em todos os níveis possíveis, sobre sua vida pregressa.

Neste ponto, a base legal dos agentes financeiros surge em três níveis, a depender do caso concreto, conforme a previsão do art. 7º, da Lei 13.709/2018:

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - **mediante o fornecimento de consentimento pelo titular;**

[...]

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;**

[...]

X - **para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.** (GN) (BRASIL, 2018, p 60, grifo nosso).

#### 6.6.1 As bases legais. O consentimento. Artigo 7º, I, da LGPD

O Banco pode realizar o tratamento do dado pessoal do cliente, utilizando a inciso I, do artigo 7º, com base no **consentimento**, o qual recebeu cuidado e atuação destacada pela LGPD. Uma análise minuciosa dos princípios – que têm grande parte de seu centro gravitacional baseado no ser humano – revela a preocupação do legislador com a participação do indivíduo no fluxo de suas informações, o que reforça a ideia e importância deste tema (TEFFÉ; VIOLA, 2020).

Nos termos da Lei, o consentimento é conceituado a “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”. (BRASIL, 2018, p. 60, art. 5º, XII, da LGPD), conceito análogo a GDPR. Manifestação livre indica sem a existência dos chamados vícios do consentimento (erro, simulação, coação e fraude – artigo 8º, § 3º, da LGPD) e, ainda, a segurança da informação, ou seja, ter direito a todas as informações pertinentes aos dados geridos pelo controlador e o tempo e modo que serão utilizados. Por fim, não escapou do conceito a *finalidade*, ou seja, o titular

deve ser informado a razão da coleta e do tratamento do dado, tudo em homenagem ao *princípio* estabelecido no artigo 6º, I, da LGPD<sup>11</sup>.

No caso dos bancos, o consentimento assume, ainda, uma importância destacada, dado ao amplo e propagado direito à informação e às normas do Código de Defesa do Consumidor. Por isso, a doutrina já traz casos onde os dados entram sob condição do negócio, como são, efetivamente, os contratos bancários, onde a análise da questão pessoal e patrimonial são condições do negócio. (BIONI, 2019, p. 197).

E a lei não descuidou desta particularidade, quando mencionou, no artigo 9º, § 3º:

Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

[...]

§ 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei. (GN). (BRASIL, 2018, p. 60).

O artigo em referência tem vertical aplicação aos contratos bancários e, por isso, abre espaço para a aplicação do artigo 18, da LGPD, o qual assegura aos titulares dos dados a exercerem, em qualquer tempo e modo, a fiscalização de seus dados, com amplo acesso, correções, anonimização, entre outros, e até mesmo **a revogação do consentimento, se o caso**. Todavia, a revogação não pode ser analisada somente sob a ótica do titular. No caso dos contratos bancários, onde há previsão contratual para a coleta e tratamento, os agentes financeiros têm a garantia e o direito sobre os dados, até em razão de ser isso (gerenciamento sobre os dados) uma condição necessária para a existência do negócio. A revogação, neste caso, não poderá ser realizada por ato unilateral do titular, o qual deverá buscar uma declaração judicial, e desde que comprovada a infração contratual da Instituição Financeira.

Todavia, como traço distintivo marcante, ressalta-se que o titular dos dados não poderá revogar o seu fornecimento a qualquer momento, uma vez que a

---

<sup>11</sup> 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;

outra parte estará resguardada pela LGPD para poder manter os dados fornecidos pelo titular enquanto durar a execução do contrato (TEFFÉ; VIOLA, 2020, p. 25).

Nesse caso, como tratado acima, o tratamento a ser feito pelo agente financeiro depende da situação contratual. Se o contrato bancário já autoriza a Instituição Financeira a arrecadar e fazer o tratamento, entende-se estar suprido o **consentimento**. Caso contrário, a partir da vigência da norma, urge a necessidade da alteração contratual para que o banco busque o consentimento do titular dos dados, para realizar toda e qualquer análise cadastral, e a efetiva utilização destes dados para qualquer finalidade.

Como o consentimento, junto às Instituições Financeiras, em regra, são colhidos via contratual, e por isso **escrito**, cumpre-se o requisito do artigo 8º, caput, da LGPD. Todavia, o parágrafo primeiro do mesmo artigo ressalta e põe condição contratual, exigindo cláusula específica na avença: “§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais” (BRASIL, 2018, p. 60).

Esta exceção é deveras importante, eis que, em contratos bancários pretéritos, pode exigir aos agentes financeiros as modificações necessárias, sob pena de nulidades futuras, caso eventual má gestão dos dados descambe para a análise do Poder Judiciário, e a exigência da cláusula específica não estiver satisfeita.

#### 6.6.2 As bases legais. A execução de contrato. Artigo 7º, V, da LGPD

A **segunda base legal** aberta à utilização pelas Instituições Financeiras, e que surge como exigência para tratamento de dados, é a prevista no artigo 7º, V, da LGPD: “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” (BRASIL, 2018, p. 60).

Esta base legal se assemelha ao consentimento, na medida em que o proprietário já é contratante (cliente do Banco), ou pretende formalizar um contrato, onde será necessário o fornecimento de seus dados ao controlador. No caso, ambas as partes formalizam uma avença, onde o titular permite o uso dos dados pessoais, e, assim, o tratamento pode ser executado, até como condição do negócio.

São os típicos negócios jurídicos bancários, os quais exigem, fundamentalmente, o consentimento e seus requisitos, como tratado no tópico anterior.

Há os que defendem, inclusive, o direito do controlador em realizar a coleta e o tratamento, sem o consentimento, em razão da análise do dado ser necessário como condição de existência do negócio jurídico. Nesse contexto, Chiara TEFFÉ e Mario Viola revelam que:

A disposição em questão é mais ampla do que aquela prevista no art. 11, II, 'd', da LGPD, **podendo o agente tratar, sem consentimento**, os dados que são necessários para a contratação, bastando que o titular seja parte ou esteja em tratativas para um contrato. É possível trabalhar, aqui, dois exemplos: a) nas situações em que o titular adquira produtos ou serviços para entregá-los será preciso conhecer o nome completo, o endereço e outras informações de contato do consumidor; e b) **levantamentos realizados por instituições financeiras em relação a determinada pessoa, anteriormente à concessão de crédito a ela**. No campo dos seguros, essa base apresenta importância pois é necessário realizar análises preliminares para subsidiar a contratação (conhecimento do risco), como também para cumprir o contrato, como no caso da regulação de um sinistro, do fornecimento de assistência 24 horas, da inspeção de risco etc. (GN) (TEFFÉ; VIOLA, 2020, p. 24-25, grifo nosso).

Em que pese os Autores acima indiquem eventual possibilidade de coleta e tratamento de dados, no âmbito bancário, sem consentimento, mais seguro à Instituição Financeira é obter do cliente uma autorização prévia para formação do cadastro e uma análise dos dados, e patrimonial, como condição pré contratual, para posterior deferimento do crédito. Até por que a parte final do inciso V, do artigo 7º, da LGPD, faz expressa menção a existência de pedido do titular dos dados (*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*).

Em outras linhas, os dados financeiros, em que pese não sensíveis, são críticos e merecem análise e tratamento diferenciado, diante de uma ampla legislação extravagante.

### 6.6.3 As bases legais. A proteção do crédito. Artigo 7º, X, da LGPD

A **terceira base legal** aberta à utilização pelas Instituições Financeiras, e que surge como exigência para tratamento de dados, é a prevista no artigo 7º, X, da

LGPD: “para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente” (BRASIL, 2018, p. 60).

A previsão legal, em referência, é de conceito aberto. Afinal, a proteção do crédito deverá ser vista sob qual ótica, a do controlador, que eventualmente detém os dados, e quer tratá-los, ou do titular, que sequer conhece o controlador, e, se levado a conhecimento, quer eliminá-los (art. 5º, XIV, da LGPD)?

O sentido da norma, ao certo, foi ampliar e facilitar a concessão de créditos, aparelhar as instituições financeiras para melhorar a análise de riscos e impulsionar o consumo (TEFFÉ; VIOLA, 2020). O sentido é a proteção do crédito, de uma maneira geral, o que envolve considerar aspectos que ensejam as características de um bom pagador, de um superendividado ou de um devedor contumaz. Isso permite uma análise tanto da capacidade de pagamento como da probabilidade de inadimplência do indivíduo, de forma a mitigar os riscos da concessão de crédito aos quais o credor se sujeita (SEBBEN, 2020).

A análise sobre esta base legal é, ainda, rudimentar. Sustentar o tratamento dos dados nesta hipótese sem o consentimento, nos parece bastante ameaçador, principalmente aos agentes financeiros, diante das leis paralelas que protegem o consumidor, notadamente o CDC. Desde 2004, quando o Superior Tribunal de Justiça editou a Súmula 297<sup>12</sup>, não há mais discussão acerca da aplicação do Código de Defesa do Consumidor aos contratos bancários. E, nesta condição, qualquer cláusula é interpretada a favor da parte menos favorecida e hipossuficiente na avença, sempre, neste caso, o cliente.

Laura Schertel Mendes e Danilo Doneda, acerca do disposto no art. 7º, inciso X, lecionam:

Aqui, acena-se diretamente à tradição já estabelecida na legislação brasileira de prever especificamente regras para a proteção de dados no setor de crédito, **notadamente o Código de Defesa do Consumidor e a Lei 12.414/2011 (LGL\2011\1883) (conhecida como Lei do Cadastro Positivo)**. Considerando a natureza da atividade e da legislação pertinente, o dispositivo acena a uma leitura sistemática da LGPD juntamente com a legislação referente à proteção do crédito, cujas especificidades integram o regime que irá balizar o tratamento de dados no setor. Assim, elementos específicos como a inserção automática em cadastros de negativação (de acordo com o CDC (LGL\1990\40)) ou as regras previstas nos cadastros de adimplemento na Lei do Cadastro Positivo, específicas para o setor de crédito, continuarão a ser aplicadas e serão complementadas pelo conjunto de princípios e direitos da LGPD, fortalecendo a unidade sistêmica e

---

<sup>12</sup> O Código de Defesa do Consumidor é aplicável às **instituições financeiras**.

ampliando as garantias do titular dos dados nessas situações para além das previsões setoriais (MENDES; DONEDA, 2018, p. 473-474, grifo nosso).

Ainda nesta base legal, um dos pilares que sustenta a *proteção de crédito* e autoriza seu tratamento, até mesmo a despeito do consentimento, é a prevenção de fraudes. Permitir o acesso a dados, por parte das empresas que concedem crédito, ao certo aumentam os instrumentos de controle sobre possíveis fraudadores, mormente nos dias atuais, onde a indústria dos documentos falsos é alarmante.

Neste ponto, não há como dissociar o estudo desta base legal sem a integração com a Lei Complementar 166/2019, a qual alterou a Lei Complementar 105/2001, e a Lei 12.414/2011, conhecida como a “*Lei do Cadastro Positivo*”. A Lei do Cadastro Positivo surgiu para auxiliar os agentes financeiros nas tomadas de decisões relativas às concessões de crédito. Formou-se, então, um cadastro, à revelia do titular, para a criação do chamado *credit scoring* - sistema de pontuação. Este modelo foi considerado legal, pelo Superior Tribunal de Justiça, através do julgamento do Recurso Especial 1.419.697<sup>13</sup>, com base nos arts. 5º, IV, e pelo art. 7º, I, da Lei nº 12.414/11.

Não obstante, a autonomia do agente financeiro não é ilimitada. E os reiterados julgamentos do STJ culminaram na edição da Súmula 550:

A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo (BRASIL, 2015, segunda seção, julgado em 14/10/2015, DJe 19/10/2015).

Além do direito de eventual retificação, o titular poderá, também, solicitar a exclusão de dados desnecessários para a formação do *scoring*, e outros considerados sensíveis.

Conforme restou decidido no REsp 1.419.697, não podem ser valoradas pelo fornecedor do serviço de *credit scoring* informações sensíveis, ficando caracterizado abuso do direito pela utilização de informações sensíveis, excessivas, incorretas ou desatualizadas. Destaque-se que, no referido Recurso, o STJ entendeu

---

<sup>13</sup> STJ. REsp 1.419.697/RS (submetido ao regime dos recursos repetitivos), Rel. Min. Paulo de Tarso Sanseverino. DJe 17/11/2014.

que dentre as informações consideradas "excessivas" estão os referentes aos gostos pessoais e, até mesmo, filiação a clube de futebol (TEFFÉ; VIOLA, 2020).

Em conclusão, é praticamente assente entre os doutrinadores que se debruçam sobre a LGPD, as homenagens a esta base legal. A proteção do crédito é medida que se impõe, necessária ao crescimento econômico, mormente em economias emergentes como a brasileira. Medir o risco de crédito e eliminar os inadimplentes é crucial ao mercado, visto que a impontualidade prejudica indicadores relevantes para a economia. Análises de crédito com qualidade mais apurada permitem índices de perda esperada menores para respectivas linhas de crédito e geram externalidades positivas. Influenciam, sobretudo, o estabelecimento de taxas de juros e, também, um maior controle do risco de crédito (SEBBEN, 2020).

Por fim, a Lei do Cadastro Positivo não atenta contra o princípio da privacidade, mesmo que elevado a *status* de proteção constitucional como direito fundamental. A concessão de créditos, para sua realização e formatação, exige a formação de um negócio jurídico bilateral e sinalagmático (contrato), com obrigações recíprocas de ambas as partes. D'outro lado, o artigo 170 da CF/88, sobre a ordem econômica, também se eleva à condição de preceito constitucional, e o funcionamento adequado e equilibrado do mercado de crédito é fator relevante para a garantia desse preceito (SEBBEN, 2020).

Nesse sentido, a análise de crédito, para a proteção do mercado, não discrimina o indivíduo, mas sim serve como termômetro valioso aos riscos envolvidos no mercado. Para a Autora citada Sebben (2020), potenciais proibições ou limitações ao tratamento de dados para a finalidade de análise e concessão de crédito gerariam consequências desastrosas a todo sistema creditício e, conseqüentemente, a toda economia. Porquanto favoreceriam a assimetria informacional e inviabilizariam novas ofertas de linhas de crédito, em especial, para segmentos pouco favorecidos (como trabalhadores informais, por exemplo) até a promulgação do novo cadastro positivo.

E, para eventuais abusos há previsão legal rígida de punição, como destacam Danilo Doneda e Laura Mendes.

A utilização legítima e responsável dos dados pessoais proporciona ao cidadão a confiança necessária para compartilhá-los sempre que julgar cabível, bem como garante aos agentes de tratamento segurança jurídica para que possa utilizá-los de forma transparente em seus modelos de negócio. Para que se alcance tal finalidade, desenvolveu-se um sistema de

normas para proteção de dados, que envolve o estabelecimento de uma série de procedimentos, princípios e direitos que limitam o processamento de dados pessoais ao mesmo tempo que empoderam o cidadão para controlar o fluxo de seus dados. Nesse sentido, a sanção da LGPD foi, certamente, um enorme avanço no marco normativo brasileiro (MENDES; DONEDA, 2018, p. 480).

#### 6.6.4 As bases legais. Cumprimento de obrigação legal. Artigo 7º, II, da LGPD

A **quarta base legal** aberta à utilização pelas Instituições Financeiras, deve ser utilizada por ocasião de o agente financeiro ser compelido à prática de um ato, ou cumprimento de uma obrigação, decorrente de lei.

Esta base legal, desde que bem utilizada pelo controlador, não abre qualquer espaço para discussão. Para as Instituições Financeiras, a evolução das legislações de controle de capitais e evasão de divisas, criaram obrigações cujo descumprimento levam à graves sanções.

Cita-se, aqui, alguns exemplos. A Lei 9.613/1998 é o ato normativo que cria e disciplina os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras – COAF. Por obrigação legal, os Bancos devem notificar o COAF sempre que identificarem transações com indícios de lavagem de dinheiro, de financiamento de atividades terroristas ou de outras práticas ilícitas previstas em lei. (BRASIL, 1998).

Referida lei prevê, também, a chamada comunicação por Operação em Espécie (COE), que envolve movimentações em dinheiro acima do valor estabelecido em norma, atualmente fixado em R\$ 50 mil.

Nesse sentido, existindo uma obrigação legal, a base a ser utilizada é o artigo 7º, II, da LGPD, o qual, desde que detectada a irregularidade pelo agente financeiro, dispensa o consentimento do titular.

### **6.7 O Legítimo Interesse utilizado na atividade bancária. Uma base legal *questionada***

Como à sociedade exposto, a Lei Geral de Proteção de Dados foi criada para reger a *coleta, o tratamento, o armazenamento e o compartilhamento* dos dados

peçoais. E, para dar vazão a este tratamento, o controlador deve demonstrar a finalidade legítima do tratamento, sob pena de ilegalidade.

As Instituições de Crédito têm à disposição várias bases legais para coletar e tratar os dados dos clientes, como premissa a um contrato bancário e a existência de um consentimento formal e escrito, até a execução da evença, onde o próprio consentimento é afastado, em determinadas hipóteses. Utilizar uma base legal aberta, portanto, pode desaguar em notórios e graves problemas de enquadramento futuros, mormente se questionados pelo titular.

Referida base legal é prevista no art. 7º, IX<sup>14</sup>, e regulamentado pelo artigo 10, da LGPD:

Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I - apoio e promoção de atividades do controlador; e

II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial (BRASIL, 2018, p. 61-62).

O artigo 10 reclama, para a utilização desta base, para além da comprovação da justificativa legítima do controlador, a entrega ao titular de algum direito em seu benefício, ou ao menos, uma expectativa, além dos princípios da finalidade, da necessidade e da proporcionalidade na utilização dos dados. Quanto mais invasivo, inesperado ou genérico for o tratamento, menor será a probabilidade de que seja reconhecido o legítimo interesse. (TEFFÉ; VIOLA, 2020).

A prática doutrinária faz referência a aplicação prática do requisito do legítimo interesse, a fim de evitar problemas legais de ajustes. O chamado *legitimate interest assessment* (LIA) ou teste da ponderação, surgiu no Grupo de Trabalho do Artigo 29 (*Working party 29*), o qual serviu de base para o texto do GDPR. Neste modelo, pondera-se os direitos e os interesses do controlador, e se há um interesse

legítimo deste na coleta e tratamento dos dados e, noutro turno, se estão presentes os interesses e direitos, e as liberdades dos titulares.

Na visão de Souza; Viola; Padrão (2019, p. 120), o teste do legítimo interesse passa por quatro fases:

- (i) a avaliação dos interesses legítimos;
- (ii) o impacto sobre o titular do dado;
- (iii) o equilíbrio entre os interesses legítimos do controlador e o impacto sobre o titular; e
- (iv) salvaguardas desenvolvidas para proteger o titular dos dados e evitar qualquer impacto indesejado.

Nesse sentido, a Instituição Financeira poderá, à margem das outras bases legais, utilizar o legítimo interesse, desde que consiga, de forma segura, comprovar a legitimidade para a utilização e tratamento dos dados, e, paralelamente, cumprir a expectativa dos interesses do titular.

## **6.8 Os Procedimentos e as opções práticas de *compliance* disponíveis à implementação do tratamento de dados ao setor bancário. Os desafios**

O *compliance*, a conformidade e a integridade, é um órgão de governança obrigatório dentro de toda e qualquer Instituição Financeira, a rigor do artigo 2º, da Resolução 4.595/2017<sup>15</sup>, do Banco Central do Brasil. A criação, instituição e regular funcionamento do *compliance*, portanto, é compulsória.

Como já destacado, na legislação brasileira, não há, a rigor, obrigação das empresas criarem e instituírem um setor de conformidade, com poucas exceções, onde estão incluídos os agentes financeiros. O que há, de forma evidente, é o incentivo à tal prática, pois é assente que a conformidade desagua em boas práticas empresariais, previne a ocorrência de infrações ou minimiza seus danos, caso ocorridos.

A Lei Geral de Proteção de Dados trouxe uma grande leva de conceitos, normas abertas e de aplicação indefinida, um novo marco regulatório, que, inclusive, para fiscalização de eventuais desajustes e irregularidades, criou uma Agência

---

<sup>14</sup> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

<sup>15</sup> Cf. Art. 2º As instituições mencionadas no art. 1º devem implementar e manter política de conformidade compatível com a natureza, o porte, a complexidade, a estrutura, o perfil de risco e o modelo de negócio da instituição, de forma a assegurar o efetivo gerenciamento do seu risco de conformidade.

Reguladora, no caso a ANPD. Nesse contexto, um setor de regulação interno, nas veias da organização, que atue de forma concreta e efetiva, certamente minimiza as chances de ocorrência de ilícitos e a aplicação das severas penalidades existentes na norma. Sobre o tema:

Essa característica de complementaridade fica ainda mais evidente na proteção de dados, uma vez que a LGPD apresenta grande plasticidade, utilizando-se de diversos standards e conceitos abertos, que precisam ser necessariamente contextualizados diante da realidade de cada agente econômico, do contexto social e econômico e da evolução tecnológica do momento em que forem aplicados. Logo, é fundamental que, ao lado do papel regulamentador da autoridade nacional, os agentes econômicos possam também ter a iniciativa de dar concretude aos comandos legais, adaptando-os à sua realidade a partir dos incentivos e dos esclarecimentos que recebem do próprio Estado (FRAZÃO; OLIVA; ABILIO, [2019], p. 685).

E, continuando no tema, os autores retratam os procedimentos a serem adotados em um bom programa de *compliance*, e as vantagens advindas de sua aplicação:

(i) permitir a adequada gestão do risco da atividade – na medida em que identifica os pontos sensíveis em que há exposição ao descumprimento – e, por consequência, auxiliar na prevenção de ilícitos; (ii) viabilizar a pronta identificação de eventual descumprimento, bem como a remediação de danos daí decorrentes, auxiliando, assim, na minoração dos prejuízos; (iii) fomentar a criação de uma cultura corporativa de observância às normas legais; e (iv) servir potencialmente como atenuante no caso de punições administrativas na tutela de dados soma-se à vantagem adicional de adaptar e operacionalizar diversos dos comandos gerais e conceitos abertos da LGPD. Podem-se enumerar, ainda, benefícios, ainda que indiretos, concernentes ao desenvolvimento em qualidade e inovação, além de incrementos reputacionais (FRAZÃO; OLIVA; ABILIO, [2019], p. 686).

O programa de *compliance*, inicia, portanto, com identificação precisa dos riscos da atividade, e, com isso, mapear eventuais gargalos quanto a hipóteses de descumprimentos das normas. Identificado o descumprimento, através de mecanismos de gestão, e de forma pretérita, as chances de redução dos danos é infinitamente superior e, de consequência, a minoração dos prejuízos.

A identificação e o mapeamento de riscos, inclusive, devem ser feitos de forma linear e constante, posto que a empresa pode mudar o foco de atuação, girar seus investimentos, partir para novo segmento, e enfrentar outros ramos de atividade, sob o pálio de novas legislações, e estar exposta a novos riscos. Este requisito, inclusive, é fator crucial a distinguir o *compliance* do setor de auditoria. As

auditorias, em geral, são temporárias, sazonais e coletam dados por amostragem. A conformidade, ao contrário, atua permanentemente, sob forte vigilância sobre todos os segmentos da organização.

D'outro lado, um efetivo programa de *compliance*, com cursos periódicos compulsórios a todos os colaboradores, por exemplo, faz criar uma cultura dentro da organização, quanto à estrita observância das normas legais. Neste tópico, a elaboração de Códigos de Ética e de Conduta – “[...] documentos escritos que consubstanciam os valores e princípios da entidade, a serem observados por todos (inclusive terceiros), bem como orienta quais as condutas são aceitas e quais são vedadas)” (FRAZÃO; OLIVA; ABILIO, [2019], p. 689).

E, por fim, como citado pela doutrina, e previsto inclusive em legislações esparsas, a existência de programas de conformidade permite a redução de penas administrativas impostas às empresas, como é o caso da lei antiterrorismo.

No caso da LGPD, ainda, como abordado, face ao grande número de conceitos abertos e indeterminados, ter um setor de conformidade a ladear o de investimento, é salutar. E, neste ponto, o *compliance* se alia, também, à inovação. O sucesso e o crescimento empresarial, financeiro, é salutar, e ainda ganha maiores e melhores contornos se dentro da legislação, dentro das regras e evitando punições.

Segundo Frazão; Oliva; Abilio ([2019], o programa de *compliance* deve ter a estrutura de acordo e compatível com o risco e envergadura da empresa, que atue de forma independente e com recursos suficientes, além do comprometimento da Alta Administração da organização. Caso a alta cúpula atue de forma contrária com as diretrizes constantes no programa de *compliance*, certamente não se formará a cultura entre os colaboradores acerca da obrigatoriedade do programa.

A adaptação do setor de *compliance* às novas diretrizes e exigências criadas pela Lei Geral de Proteção de Dados passa, necessariamente, também, pelo aprimoramento, ou mesmo criação de um novo modelo de controle e gestão de processos. A Instituição Financeira é, verdadeiramente, um pulmão de dados: são dados de clientes, de colaboradores, de terceirizados, de fornecedores etc. Em que pese o trabalho aqui apresentado se concentre nos dados pessoais dos clientes bancários, é certo que o tratamento dos vários outros tipos de dados também merecerá especial atenção dos gestores.

O *compliance* terá novos paradigmas para, doravante aprimorar o controle dos processos internos. Seu desafio será estabelecer novas rotinas, novos modelos de

processos, para atender às Superintendências e agências, onde efetivamente os dados são coletados, armazenados, tratados e eventualmente compartilhados. Dessa forma, um monitoramento constante dos riscos é vital para o sucesso do modelo a ser empregado.

Por fim, a existência de seguros e eficientes canais de consultas/orientações, bem como uma rápida apuração e punição das condutas contrárias ao programa, são elementos essenciais para a boa gestão e funcionamento do *compliance* (FRAZÃO; OLIVA; ABILIO, [2019]).

## **6.9 O estudo de caso do Banco da Amazônia S.A.**

O Banco da Amazônia S.A. é uma Instituição Financeira Pública Federal, foi criado em 1942, exatamente no dia 9 de Julho, pelo Decreto-Lei n. 4.451. O contexto era a segunda Guerra Mundial, quando havia um esforço dos aliados para retomar a produção de borracha na Amazônia (BANCO DA AMAZÔNIA, 2019, p. [3]).

Após o encerramento deste importante ciclo econômico, o Banco foi repaginado pela Constituição Federal de 1946, que, entre outras coisas, possibilitou a criação de um órgão específico para o Desenvolvimento Regional. Com isso, ocorreu nova mudança da forma institucional do Banco que, por força da Lei n. 1.184 de 30 de agosto de 1950, passou a se chamar “Banco de Crédito da Amazônia” (BANCO DA AMAZÔNIA, 2019).

A partir de então, o Poder Público deu início à política de incentivos fiscais, onde o Banco passou a chamar-se “Banco da Amazônia”, e tornou-se o operador e gestor da carteira de incentivos fiscais por força da Lei n. 5.122 de 28 de setembro de 1966. Na década de 1970, abre-se o capital da Instituição Financeira, onde o Banco passa a ser o agente financeiro do Fundo de Investimento da Amazônia – FINAN, posteriormente renomeado para Fundo de Desenvolvimento da Amazônia – FDA.

Contudo, foi na Constituição de 1988, a Magna Carta Brasileira, que reservou-se e elevou-se o Banco da Amazônia a uma importante e singular atuação dentro do cenário financeiro e social, no Brasil. Este marcante espaço está ligado à gestão da aplicação dos recursos financeiros do Fundo Constitucional de Financiamento do Norte – FNO, o que marcou definitivamente a história do BASA em todo território nacional e especialmente na região norte.

O Art. 159 da Constituição Federal de 1988 criou os Fundos Constitucionais de Financiamentos e estabeleceu as condicionantes básicas dessa arquitetura institucional: a fonte dos recursos financeiros, os agentes operadores, e a norma diretriz.

Art. 159. A União entregará: [\(Vide Emenda Constitucional nº 55, de 2007\)](#)

I - do produto da arrecadação dos impostos sobre renda e proventos de qualquer natureza e sobre produtos industrializados, 50% (cinquenta por cento), da seguinte forma:

a) vinte e um inteiros e cinco décimos por cento ao Fundo de Participação dos Estados e do Distrito Federal;

b) vinte e dois inteiros e cinco décimos por cento ao Fundo de Participação dos Municípios;

c) **três por cento, para aplicação em programas de financiamento ao setor produtivo das Regiões Norte, Nordeste e Centro-Oeste, através de suas instituições financeiras de caráter regional**, de acordo com os planos regionais de desenvolvimento, ficando assegurada ao semi-árido [*sic*] do Nordeste a metade dos recursos destinados à Região, na forma que a lei estabelecer (BRASIL, 2016, p. 101).

Nesse contexto, percebe-se que a Constituição de 1988 ratificou a importância do Banco, e reorientou sua atuação, ligando-o diretamente à política de desenvolvimento regional. A PNDR,

[...] atualizada pelo [Decreto nº 9.810, de 2019](#), representa instrumento legal que baliza a ação em busca da redução das desigualdades econômicas e sociais, intra e inter-regionais, por meio da criação de oportunidades de desenvolvimento que resultem em crescimento econômico, geração de renda e melhoria da qualidade de vida da população (BRASIL, 2023).

E, para a execução destas metas, necessária a criação de uma gama de instrumentos econômico-financeiros, onde certamente os Fundos Constitucionais são importantes mecanismos de atuação. O FNO, assim como os demais fundos constitucionais, foi REGULAMENTADO pela Lei nº 7.827 de 1989<sup>16</sup>.

---

<sup>16</sup> Regulamenta o art. 159, inciso I, alínea c, da Constituição Federal, institui o Fundo Constitucional de Financiamento do Norte - FNO, o Fundo Constitucional de Financiamento do Nordeste - FNE e o Fundo Constitucional de Financiamento do Centro-Oeste - FCO, e dá outras providências.

**Figura 3 – Rota do FNO**



Fonte: (COSTA, 2017).

E o artigo 3º, da Lei 7.827/89, (BRASIL, 1989) logo define as diretrizes dos Fundos:

Art. 3º Respeitadas as disposições dos Planos Regionais de Desenvolvimento, serão observadas as seguintes diretrizes na formulação dos programas de financiamento de cada um dos Fundos:

I - concessão de financiamento aos setores produtivos das regiões beneficiadas

II - ação integrada com instituições federais sediadas nas regiões;

III - **tratamento preferencial às atividades produtivas de pequenos e miniprodutores rurais e pequenas e microempresas, às de uso intensivo de matérias-primas e mão-de-obra locais e as que produzam alimentos básicos para consumo da população**, bem como aos projetos de irrigação, quando pertencentes aos citados produtores, suas associações e cooperativas;

IV - **preservação do meio ambiente**;

V - **adoção de prazos e carência, limites de financiamento, juros e outros encargos diferenciados ou favorecidos, em função dos aspectos sociais, econômicos**, tecnológicos e espaciais dos empreendimentos;

Logo de plano verifica-se que os recursos originários dos Fundos Constitucionais, operados pelos Bancos Públicos, não se destinam à lucratividade ou rentabilidade. Está-se a falar em recursos destinados à sustentabilidade, **inovação**, distribuição de renda, apoio aos pequenos negócios e, notadamente, aos pequenos produtores.

O estudo (atualizado até 2018) revela a importância do FNO no cenário da região norte:

1. TOTAL GLOBAL APLICADO (TODAS AS FONTES) NA ECONOMIA DA REGIÃO DE A CRIAÇÃO DO FUNDO: 52,4 bilhões entre 01/01/1989 e 30/09/2018.

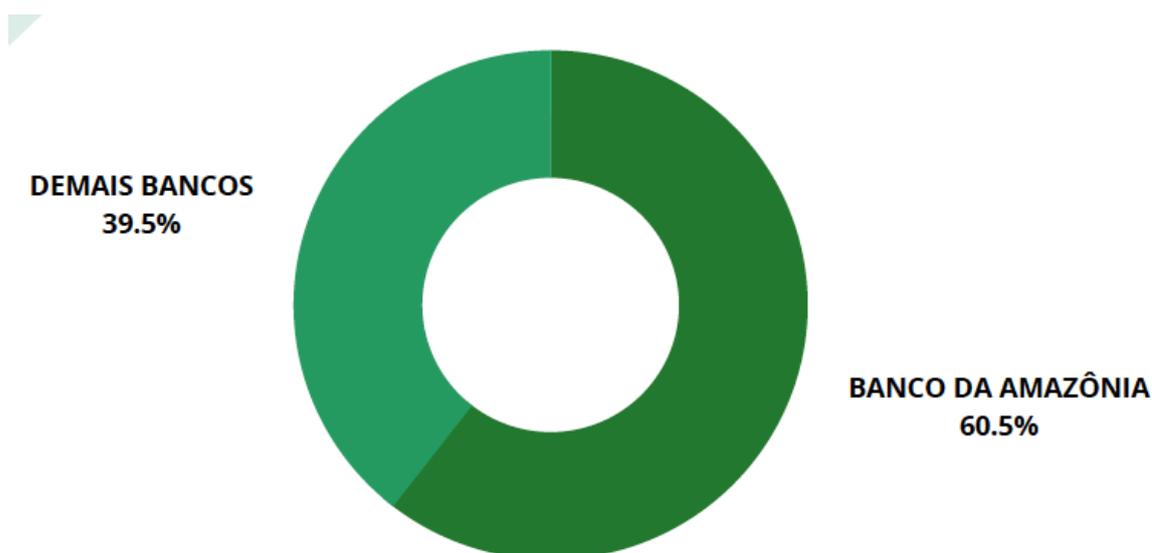
2. TOTAL DE OPERAÇÕES CONTRATADAS, TODAS AS FONTES DE A CRIAÇÃO DO FUNDO: 705,2 mil contratos entre 01/01/1989 e 30/09/2018.
3. A AGRICULTURA FAMILIAR (EXCLUÍDO O PROCERA): Mais de 509,6 mil contratos em um volume superior a 7,1 BI.
4. ESTIMATIVA DO NUMERO DE OCUPAÇÕES GERADAS: Estima-se que cada contrato gera em média 4 ocupações. Isso nos remete a quase 3 milhões de ocupações urbanas e rurais.
5. INOVAÇÕES EM QUE FOMOS PROTAGONISTAS: Banco tem sido indutor de tecnologia no campo e na cidade (BANCO DA AMAZÔNIA, 2019, p. [17]).

Ainda com base no mesmo estudo, o Banco da Amazônia é responsável por 36,35% do mercado de Crédito da Região Norte e por 62,52% do mercado de FOMENTO da Região Norte. “Trata-se de um número expressivo da importância do BASA para a Região Norte do Brasil” (BANCO DA AMAZÔNIA, 2019, p. [20]).

Desta forma, a atuação do Banco da Amazônia não é ligada, estritamente, à atividade bancária/financeira. Seu papel fundamental é ser o principal agente de indução das políticas públicas, das diretrizes políticas e estratégicas do estado brasileiro.

Atualmente, o Fundo Constitucional de Financiamento do Norte (FNO) é o principal instrumento de desenvolvimento da Amazônia, e junto com outras fontes de recursos do BASA, responderam por mais de 60% do crédito de fomento da Região Norte do país, em 2021.

**Gráfico 1 - Fundo Constitucional de Financiamento do Norte**



Fonte: (BANCO DA AMAZÔNIA, 2021, p, 9).

Desta forma, a atuação do Banco da Amazônia não é ligada, estritamente, à atividade bancária/financeira. Seu papel fundamental é ser o principal agente de indução das políticas públicas, das diretrizes políticas e estratégicas do estado brasileiro.

#### 6.9.1 O Banco da Amazônia e a LGPD

Como já destacado em linhas volvidas, os Bancos, há tempos, encontram legislações esparsas que lhes impõem o sigilo, a guarda, e a confidencialidade no processamento e armazenamento dos dados pessoais.

Inúmeras leis, resoluções, portarias etc., principalmente emanadas no Banco Central do Brasil – BACEN, órgão gestor dos Bancos, no Brasil, já regulamentavam a matéria, antes da edição da Lei 13.709/2018. No entanto, após a promulgação da referida norma jurídica, iniciou-se um novo ciclo tecnológico, dentro das Instituições Financeiras, na busca pelo cumprimento das obrigações legais, notadamente diante do cenário punitivo nela previsto.

Desta forma, a fim de fazer face à então novel legislação, o Banco da Amazônia cuidou de contratar profissionais renomados no setor, entre eles o escritório Peck Advogados<sup>17</sup>, o qual tem na sócia fundadora Patrícia Peck, renomada profissional do Direito Digital, sua principal atora.

E foi neste cenário que os profissionais cunhados pela própria Instituição Financeira, aprovados via concurso público, notadamente àqueles lotados na área de tecnologia da informação, e sob a assessoria das equipes externas, de apoio, deram início a um longo, incipiente e arrojado projeto para aplicação das normas da Lei Geral de Proteção de Dados junto ao Banco da Amazônia.

##### 6.9.1.1 A implantação da LGPD

Nas seções a seguir tratar-se-á das etapas da implantação da LGPD.

---

<sup>17</sup> <https://peckadv.com.br/>

#### 6.9.1.1.1 Primeira Etapa

O planejamento e a rotina de estudos, até final implementação, passando por novos mecanismos, naturalmente foi elaborado por etapas. Tudo iniciou com a sensibilização da equipe e a equalização de conhecimentos relacionados à proteção de dados pessoais. A ênfase em criar uma nova cultura de proteção de dados passa, primeiro, no convencimento daqueles que efetivamente serão responsáveis pela consecução do projeto.

A parte inicial do programa previu o levantamento de informações para dimensionamento e definição de cronograma, e o inventário dos dados pessoais atuais e mapeamento do fluxo de dados pessoais. Com todo o levantamento dos dados, o horizonte de aplicação, e os custos, seriam tangíveis. Em sequência, foram analisados os sistemas de informação que tratam de dados pessoais (próprios ou terceirizados), com alocação da equipe técnica para levantamento das informações técnicas.

Esta primeira etapa foi finalizada, com a análise de documentos (com o uso de indicadores), análise da lista de finalidades de uso de dados e composição da matriz de finalidades, com a apresentação do *framework*<sup>18</sup> geral de proteção a dados pessoais da empresa (árvore de governança de dados pessoais).

#### 6.9.1.1.2 Segunda Etapa

A segunda etapa inicia-se com a efetiva implementação do Plano de Ação Estruturante, no estabelecimento da Governança e Proteção dos Dados Pessoais. Nesta etapa, foi indicado o DPO<sup>19</sup> – encarregado da proteção dos dados pessoais, a estruturação a área e do Comitê de Privacidade e Proteção dos Dados pessoais, o mapeamento dos sistemas de informação e a execução do *Data Discovery*<sup>20</sup>.

---

<sup>18</sup> Na linguagem de programação, o framework é aquilo que está na base de um sistema, funcionando como um suporte. Ele permite compartilhar um conjunto de códigos entre aplicações e oferece algum tipo de funcionalidade.

(<https://www.cursospm3.com.br/glossario/framework/#:~:text=Na%20linguagem%20de%20programa%C3%A7%C3%A3o%2C%20o,oferece%20algum%20tipo%20de%20funcionalidade.>)

<sup>19</sup> Marcus Barreto Reis. Contato: [dpo@bancoamazonia.com.br](mailto:dpo@bancoamazonia.com.br)

<sup>20</sup> O Data Discovery é um processo utilizado para filtrar e otimizar a coleta de dados para análise corporativa. Essa abordagem permite a detecção ágil de padrões e ruídos no meio de um grande número de dados. Assim, rotinas como as de Business Intelligence e Big Data se tornam mais eficazes

Neste período, previa-se a elaboração e aprovação do Código de Conduta, essencial para as boas práticas de mercado e governança, e incentivado pela própria Lei, conforme art. 50, II, da Lei 13.709/2018:

## Seção II

### Das Boas Práticas e da Governança

Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

I - implementar programa de governança em privacidade que, no mínimo:

- a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
- b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
- c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
- d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
- e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
- f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
- g) conte com planos de resposta a incidentes e remediação; e
- h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por **promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei** (BRASIL, 2018c, p. 63).

Nesta etapa, estabeleceu-se a implantação da Política de Gestão de Dados Pessoais, incluindo preceitos de transferência internacional de dados pessoais e Gestão do Sistema de Governança da Privacidade, assim como a Política de Segurança da Informação, incluindo termos de RETICS (Recursos Computacionais Portáteis) e BYOD (Política de Segurança da Informação).

Estabeleceram-se os normativos de Gestão de Acessos, bem como as normas para classificação das informações com diretrizes de retenção e descarte seguro das mesmas, e procedimentos de dupla verificação para descarte de recursos. Ato contínuo, o Banco normatizou a utilização dos acessos remotos, e de **Segurança nas Contratações**, talvez uma das partes mais sensíveis de todo o processo de implantação.

A nova lei estabelece como coletar, armazenar e compartilhar os dados pessoais e sensíveis de clientes e consumidores, tanto por meios físicos quanto digitais. O início da vida contratual do cliente, como já à sociedade exposto neste trabalho, é o cadastro. Assim, a segurança das contratações, de plano, evidencia a primeira autorização para a coleta, o tratamento, o efetivo uso e o compartilhamento dos dados do consumidor. Esta é a etapa angular de todo o procedimento que dará, ou não, a segurança necessária ao Banco para todo o desenrolar da vida comercial do cliente.

#### 6.9.1.1.3. Terceira Etapa

A terceira etapa encerra o ciclo de aplicação efetiva de toda a plataforma alinhada pela equipe interna e a de apoio, contratada. A finalização dos termos de uso das Websites e APPs, os normativos finais, e a adequação dos produtos e serviços do Banco à nova modelagem legal.

Nesta etapa revisou, por exemplo, os cadastros já existentes, a fim de dar tratamento adequando aos dados pessoais vigentes e a criação dos canais de atendimento aos Titulares destes dados. Realizou-se a análise de eventuais vulnerabilidades, bem como aplicaram-se as Políticas de Anonimização e Pseudonimização dos Dados.

Os normativos de gestão, em caso de incidentes na Segurança das Informações foram criados, a fim de dar tratamento adequado à alguma situação de vulnerabilidade, tudo dentro do conceito, também normatizado, do **privacy by default** e do **privacy by design**<sup>21</sup>, os quais incorporam a ideia de que o produto ou serviço seja comercializado com todas as salvaguardas de privacidade concebidas durante o seu desenvolvimento, para a **proteção e a privacidade de dados pessoais em todas as etapas de desenvolvimento de uma solução**.

Com a normatização e aplicabilidade total nas plataformas, teve-se por encerrado o projeto, na etapa quatro. A Política de Privacidade do Banco da Amazônia

---

<sup>21</sup> <https://www.advogatech.com.br/blog/@HenriqueDantas/lcpd-o-que-e-privacy-by-design-e-privacy-by-default-vc4zyjv>

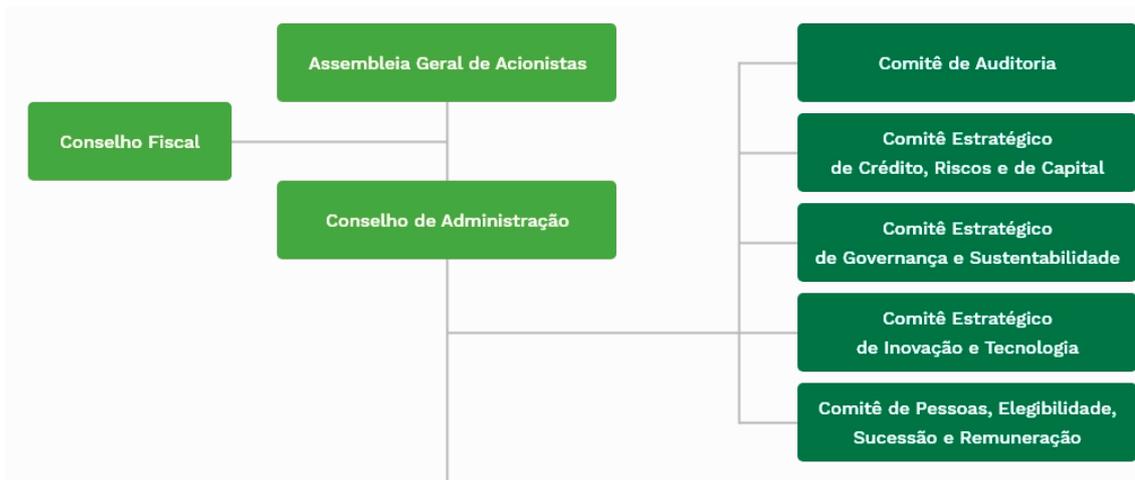
S.A. pode ser conferida no sítio, através do endereço <https://www.bancoamazonia.com.br/component/edocman/politica-de-privacidade-e-tratamento-de-dados-lgpd-2022/viewdocument/5201?Itemid=0>

### 6.9.2 O *compliance* dentro do Banco da Amazônia e a estrutura organizacional da Instituição

A estrutura de uma organização financeira é moldada, naturalmente, pela sua atividade finalística, com o objetivo final a ser por ela alcançado. Dentro do Banco da Amazônia S.A., banco público federal onde a União detém o controle acionário e os recursos manipulados são, basicamente, de ordem pública, é natural a existência de um sistema angularizado de amarras e freios, traduzidos em uma enorme gama de gerências e alçadas de competência, até uma decisão final, em sua maioria tomada de forma colegiada.

Como toda empresa integrada por ações (Sociedades Anônimas), com capital aberto, como é o BASA, o maior poder encontra-se nas mãos da Assembleia Geral, caso convocada, a qual tem o poder total de deliberação:

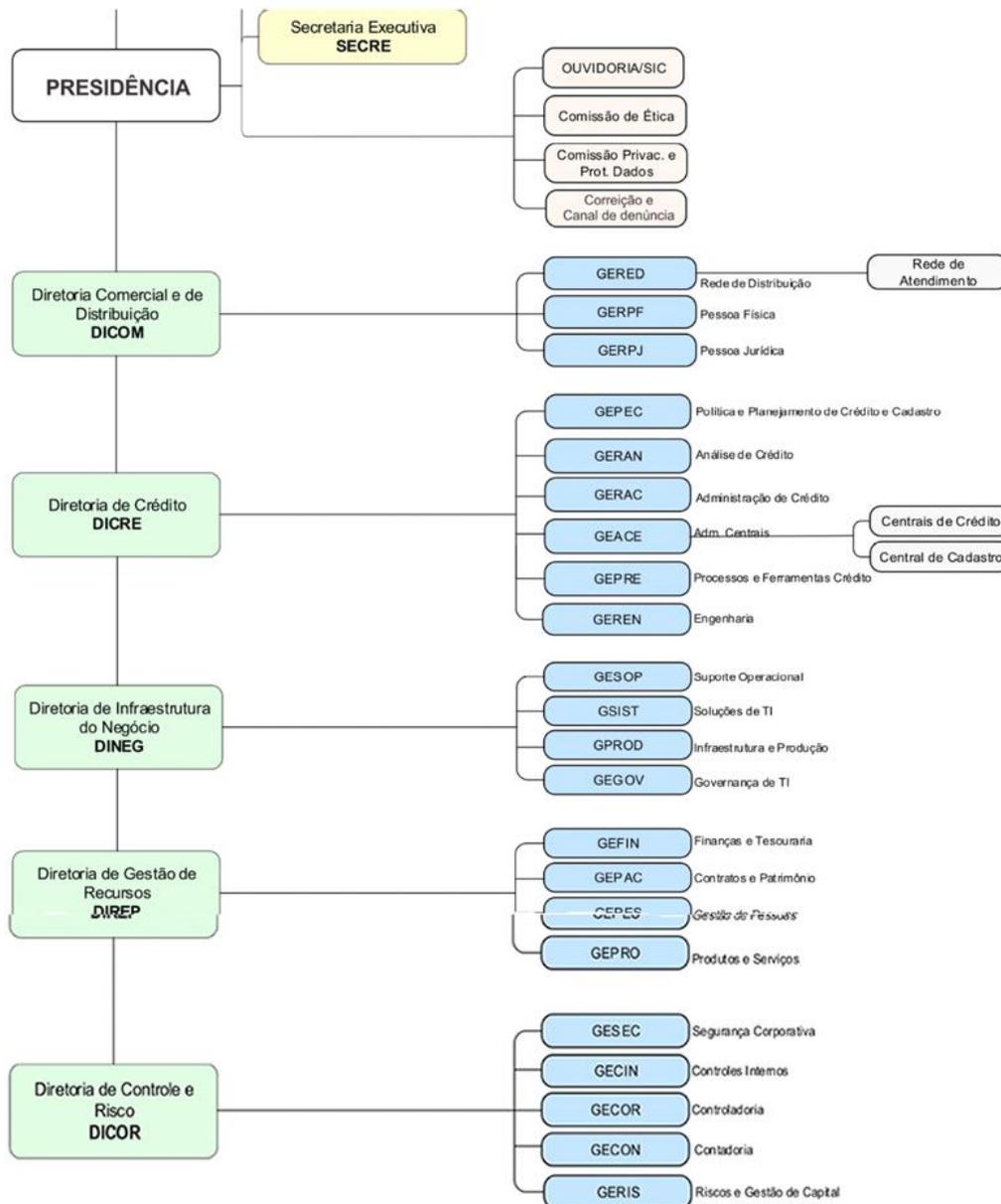
**Gráfico 2 – Organograma**



Fonte: (BANCO DA AMAZONIA, [S.d]).

Abaixo da AG, e do Conselho de Administração, de forma efetiva, encontra-se a Presidência da Instituição, com suas respectivas Diretorias Executivas:

Gráfico 3 – Estrutura Organizacional



Fonte: (BANCO DA AMAZONIA, [S.d]).

Assim, à Presidência do Banco cabe a responsabilidade de *coordenar o processo de planejamento estratégico de médio e longo prazo e seus desdobramentos; alinhar a atuação do Banco às políticas, planos e programas governamentais; coordenar e apoiar a atuação das Diretorias, para que trabalhem de forma harmônica, para cumprir suas finalidades específicas; gerir as ações do Banco voltadas à promoção do desenvolvimento regional em bases sustentáveis; acompanhar o desenvolvimento dos projetos corporativos; gerir a estrutura organizacional do Banco,*

*definindo processos e recursos necessários para concretizar o planejado; coordenar o trabalho de gestão da marca e da imagem do Banco fazendo transparecer ao público a sua atuação responsável na dinâmica econômica socioambiental; gerir as diretrizes da atuação jurídico-institucional da empresa; alinhar a forma de atuação da Ouvidoria/SIC, assegurando a estrita observância das normas legais e regulamentares afetas ao assunto; gerir o programa de integridade e a correição.*

A Presidência do Banco divide as responsabilidades e obrigações com 05 (cinco) Diretorias, que, juntas, foram a denominada Diretorias Executiva – DIREX (BANCO DA AMAZÔNIA, [2023?])<sup>22</sup>:

- **DIRETORIA DE INFRAESTRUTURA DO NEGÓCIO (DINEG):** promover a governança de TI, definido a arquitetura, o orçamento e o mapa de desenvolvimento tecnológico alinhando-os aos objetivos estratégicos da organização; prover de soluções e recursos de tecnologia da informação, realizando a gestão do desempenho de TI e garantindo a disponibilidade, qualidade, produtividade, competitividade, tempestividade economicidade; administrar os processos de suporte operacional necessários a formalização dos negócios do banco, gerindo os processos de pagamentos, arrecadação, compensação carteira de títulos de debêntures e ações dos fundos e recursos operados pelo banco.
- **DIRETORIA COMERCIAL E DE DISTRIBUIÇÃO (DICOM).** Finalidade: definir e aplicar a estratégia de atuação por segmento de cliente; elaborar e acompanhar a consecução das metas comerciais; maximizar o desempenho comercial da rede agências, gerir os canais de atendimento.
- **DIRETORIA DE CRÉDITO (DICRE):** Criar soluções de crédito para o cliente ter atendimento célere nas demandas de análise ou de reestruturação de dívidas compatibilizando com o perfil de risco cliente e sua capacidade de pagamento bem como acompanhamento das operações de crédito analisando os cenários e

---

<sup>22</sup> A Diretoria Executiva (DIREX) é o órgão responsável pela administração do Banco da Amazônia, cabendo-lhe cumprir as disposições do Estatuto Social e as deliberações do Conselho Administração, com poderes de administração e gestão dos interesses do Banco da Amazônia, sendo-lhe, porém, proibido prestar quaisquer garantias, constituir hipoteca ou gravar com qualquer ônus real os bens imóveis do Banco, bem como adquiri-los ou aliená-los sem prévia e expressa autorização do Conselho de Administração. No âmbito do sistema de governança corporativa do Banco da Amazônia, deve ser entendida como órgão de administração executiva, responsável por avaliar, direcionar e monitorar, internamente, o Banco da Amazônia. A Diretoria Executiva é composta por um Presidente e cinco Diretores, todos eleitos pelo Conselho de Administração. Os poderes conferidos pelo Estatuto ao Presidente e aos Diretores, conjunto ou de per si, são exercidos diretamente ou por intermédio dos órgãos integrantes da Estrutura Organizacional, cujas subordinações, atribuições e

antecipando ações que possam mitigar seu risco; definir as políticas, a metodologia, os modelos de crédito, em todas as suas linhas e origens de recursos e as diretrizes gerais que regem todas as etapas do ciclo de crédito (comercial e fomento) e cadastro, atentando para a necessária conformidade com a regulamentação aplicável; acompanhar as carteiras de crédito, minimizando o impacto de perdas no resultado do Banco; gerenciar as ações de cobrança e de renegociação e/ou recuperação de dívidas vencidas/compensadas; coordenar a gestão das centrais de crédito.

- **DIRETORIA DE GESTÃO DE RECURSOS (DIREP):** Formatar, desenvolver e oferecer aos canais de distribuição produtos e serviços que sejam adequados à necessidade dos clientes e ao mesmo tempo, possibilitar a geração de resultados para o Banco; gerir o portfólio de produtos e serviços; gerir os recursos financeiros à disposição do Banco, maximizando o retorno das operações de tesouraria, provendo o Banco de análise financeira para a tomada de decisão; gerir as estratégias de gestão de pessoas, o quadro funcional do Banco, selecionando, retendo e administrando talentos, desenvolvendo suas capacitações e planejando a progressão profissional dos empregados em linha com as estratégias da organização; gerir de forma estratégica os processos de patrimônio, compras e contratos.
- **DIRETORIA DE CONTROLE E RISCO (DICOR):** Atuar para o aprimoramento da governança corporativa, mitigando riscos, promovendo maior controle e conformidade na gestão do Banco, de maneira a possibilitar maior eficácia e eficiência e segurança ao processo decisório; administrar as atividades contábeis e tributárias, incluindo a formalização e execução orçamentária observando os requisitos legais e de controle; elaborar a Programação Orçamentária, controlando a sua execução e o desempenho econômico e financeiro do Banco, centralizando a difusão de informações gerenciais; conduzir de forma integrada a gestão riscos e de alocação de capital que possibilite a identificação, a mensuração, a avaliação, o monitoramento, o reporte, o controle e a mitigação dos efeitos adversos resultantes das interações entre os riscos; responder pelas ações institucionais de Relações com Investidores; desenvolver controles internos visando identificar desvios de padrão e riscos, assegurando níveis de adequados à legislação; desenvolver a segurança corporativa e de segurança da informação e de comunicações observando os requisitos legais, de controle e de segurança, estabelecendo processo de permanente avaliação e

adequação das medidas e procedimentos de segurança de forma a resguardar a integridade das pessoas, das informações, dos ativos físicos e financeiros e da imagem do Banco; realizar o controle das dotações e do passivo.

O *Compliance*, naturalmente, encontra-se dentro da **DICOR – Diretoria de Controle e Riscos**, na medida em que cabe a este órgão *cabe atuar para o aprimoramento da governança corporativa, mitigando riscos, promovendo maior controle e conformidade na gestão do Banco, de maneira a possibilitar maior eficácia e eficiência e segurança ao processo decisório.*

Cada Diretoria Executiva é dividida, dentre suas áreas de atuação, pelas respectivas **Gerências Executivas**. As Gerências Executivas são as subdivisões existentes, dentro da Diretoria, a fim de delimitar e pulverizar a sua área de atuação.

A **DICOR – Diretoria de Controle e Riscos**, no organograma do Banco da Amazônia, é subdividida em **04 (quatro) Gerências Executivas**, (BANCO DA AMAZÔNIA, [2023?]) a saber:

#### **8.1 GERÊNCIA EXECUTIVA DE CONTADORIA (GECOR)**

8.1.1 Finalidade: gerir a contabilidade, estruturando políticas e procedimentos contábeis, efetuando a conciliação contábil, elaborando e divulgando as demonstrações financeiras do banco fontes de recurso sob gestão, em conformidade com a legislação e normativos vigentes, além de realizar o planejamento tributário, gerenciar as obrigações tributárias, coordenar a regularidade fiscal e realizar o controle, registro e pagamento das fontes de repasse.

#### **8.2 GERÊNCIA EXECUTIVA DE CONTROLADORIA (GECOR)**

8.2.1 Finalidade: gerir a programação orçamentária, realizar a gestão estratégica de custos, das fontes de recursos e do desempenho, estruturando, analisando e disponibilizando informações econômico financeiras do banco, inclusive análise prospectiva de orçamentos e projeções de resultados.

#### **8.3 GERÊNCIA EXECUTIVA DE RISCOS CORPORATIVOS (GERIS)**

8.3.1 Finalidade: realizar a gestão integrada de riscos e de capital, administrando as ações de identificação e gerenciamento dos riscos, definindo os níveis de risco e de alocação de capital adequados às estratégias e estrutura do banco.

#### **8.4 GERÊNCIA EXECUTIVA DE CONTROLES INTERNOS (GECIN)**

8.4.1 Finalidade: atuar como segunda linha de defesa de controles internos, assegurando a conformidade regulamentar e operacional, garantindo a adequação e o funcionamento do sistema controles internos do banco, reportando às instâncias de governança e à alta administração as avaliações nos controles institucionais.

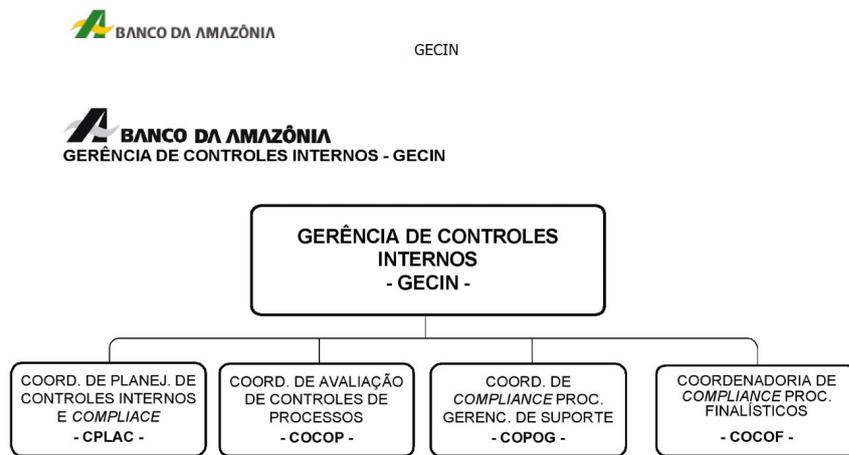
#### **8.5 GERÊNCIA EXECUTIVA DE SEGURANÇA CORPORATIVA (GESEC)**

8.5.1 Finalidade: gerir a segurança corporativa do banco observando os requisitos legais, de controle, buscando a prevenção e mitigação de ameaças com o objetivo de resguardar a integridade das pessoas, das informações, dos ativos físicos e financeiros e da imagem do banco.

A partir da criação das Gerências Executivas, as mesmas subdividem-se em **Coordenadorias**, guardando, neste caso, a mesma divisão de responsabilidades e obrigações dentro de uma mesma gerência.

Pois bem. A **GERÊNCIA EXECUTIVA DE CONTROLES INTERNOS (GECIN)**, é, por sua vez, subdividida em **04 (quatro) Coordenadorias**, assim disposta:

**Figura 4 – Gerencia de Controles Internos**



FUNÇÃO/CARGO	DOTAÇÃO
GERENTE EXECUTIVO	01
COORDENADOR	04
ANALISTA	16
OPERATIVO	04
<b>TOTAL</b>	<b>25</b>

CONTROLE, RISCO E SEGURANÇA (DICOR)	Atuar para o aprimoramento da governança corporativa, mitigando riscos, promovendo maior controle e conformidade na gestão do Banco, de maneira a possibilitar maior eficácia e eficiência e segurança ao processo decisório.	CONTABILIDADE	Gerir e controlar os registros contábeis para acompanhamento do patrimônio e dos ativos sob a gestão do Banco, em conformidade aos normativos legais.
		CONTROLADORIA	Organizar e controlar a gestão econômica do Banco, apoiando os gestores, mediante a geração de informações e indicadores para o auxílio nas tomadas de decisões.
		CONTROLE INTERNO E COMPLIANCE	Monitorar a eficiência dos mecanismos de controle através de testes contínuos de aferição, mapeamento e avaliação de processo e compliance nos negócios.
		CORREGEDORIA	Auxiliar a gestão no controle e acompanhamento de processos envolvendo denúncias de irregularidades, a fim de zelar pelas boas práticas de governança, relacionadas a integridade, ética e transparência.
		SEGURANÇA CORPORATIVA	Proteger o patrimônio do Banco e de seus clientes, bem como a integridade física de seus colaboradores através de ações de prevenção e controle de acessos, seja a dados e informações, ou a instalações físicas e ambientes virtuais. Combater ilícitos.
		RISCO E GESTÃO DE CAPITAL	Controlar e gerir os riscos (potenciais e efetivos), a fim de mitigar possíveis perdas e fazer a gestão dos níveis adequados de capital, que permitam ao Banco operar com segurança e assim contribuir para o atingimento dos objetivos estratégicos da Organização.
			<b>OBJETIVO</b>

Fonte: (BANCO DA AMAZÔNIA, [2023?]).

Com efeito, a área de *compliance* ficou afeta a **02 (duas) Coordenadorias do Banco**, junto GERÊNCIA EXECUTIVA DE CONTROLES INTERNOS (GECIN), dentro da **DICOR – Diretoria de Controle e Riscos**, (BANCO DA AMAZÔNIA, [2023?]). quais sejam:

### **3 COORDENADORIA DE COMPLIANCE EM PROCESSOS GERENCIAIS E DE SUPORTE - COPOG**

#### **3.1 Compliance regulamentar - Processos Gerenciais e de Suporte.**

- 3.1.1 Manter inventário atualizado de regulamentações externas.
- 3.1.2 Avaliar a eficácia dos controles na primeira linha em relação ao *compliance*.
- 3.1.3 Indicar necessidades de melhorias e mitigação do risco de *compliance*.
- 3.1.4 Receber, pesquisar e distribuir novas regulamentações externas e monitorar o seu cumprimento.
- 3.1.5 Analisar a aderência da instituição ao arcabouço legal, à regulamentação infralegal e às recomendações dos órgãos de supervisão, quando aplicáveis.
- 3.1.6 Coordenar as auto avaliações realizadas pela 1ª Linha relacionada a verificar a aderência dos seus processos e produtos às regulamentações externas.

#### **3.2 Compliance operacional - Processos Gerenciais e de Suporte.**

- 3.2.1 Efetuar a conformidade operacional dos processos relevantes, incluindo a criação e aprovação de novos produtos.
- 3.2.2 Definir, monitorar e manter atualizado o Rating de Conformidade.
- 3.2.3 Monitorar indicadores de *compliance*.
- 3.2.4 Monitorar as falhas em políticas, normas, procedimentos e controles que não garantam a conformidade do Banco aos normativos externos dos órgãos reguladores.
- 3.2.5 Emitir Recomendação Técnica de controle, Notas de Controle e Alertas de Controle a fim de minimizar deficiências identificadas, fragilidades ou não conformidades em processos, sistemas, produtos ou serviços.
- 3.2.6 Auxiliar as áreas na definição de controles necessários para atendimento das regulamentações.
- 3.2.7 Monitorar os processos críticos do Banco, visando manter o padrão de funcionamento.
- 3.2.8 Monitorar e analisar os impactos dos regulamentos e/ou normativos publicadas pelos órgãos reguladores afetos a controles internos e *compliance*.
- 3.2.9 Elaborar relatório contendo os resultados das atividades relacionadas à função de *compliance*.
- 3.2.10 Assessorar o Comitê de Elegibilidade, realizando avaliações de conformidade das indicações dos Conselheiros, diretores e presidente, na forma da legislação vigente.

#### **3.3 Administração do processo.**

- 3.3.1 Elaborar e manter atualizada, para os processos de responsabilidade da coordenadoria:
  - a) a política, as normas, os procedimentos, as delegações de responsabilidade e os fluxos de atividades;
  - b) os indicadores de desempenho, eficiência e qualidade;
  - c) os métodos, ferramentas e sistemas;
  - d) identificar as vulnerabilidades, a análise de risco do processo e medidas para mitigá-los.
- 3.3.2 Coordenar a execução orçamentária de todas as rubricas de responsabilidade da Coordenadoria.
- 3.3.3 Pesquisar e analisar regulamentos e/ou normativos publicadas pelos órgãos reguladores, afetos ao assunto, analisando impactos e efetuando os necessários ajustes nas políticas e demais normativos internos.

#### **4 COORDENADORIA DE COMPLIANCE EM PROCESSOS FINALÍSTICOS - COCOF**

##### **4.1 Compliance operacional de Processos Finalísticos.**

4.1.1 Efetuar a conformidade operacional dos processos de negócios, incluindo a criação e aprovação de novos produtos e serviços.

4.1.2 Avaliar a eficácia dos controles na primeira linha em relação ao compliance, inclusive na constituição de novos produtos, serviços e atividades de negócios.

4.1.3 Indicar necessidades de melhorias nos processos e mitigação de riscos.

4.1.4 Definir, monitorar e manter atualizado o Rating de Conformidade.

4.1.5 Monitorar os controles das agências (monitoramento contínuo).

4.1.6 Monitorar indicadores de compliance.

4.1.7 Emitir Recomendação Técnica de Controle, Notas de Controle e Alertas de Controle a fim de minimizar deficiências identificadas, fragilidades ou não conformidades em processos, sistemas, produtos ou serviços.

4.1.8 Auxiliar as unidades de 2ª Linha na definição de controles necessários para atendimento das normas e mitigação dos riscos.

4.1.9 Monitorar os negócios e produtos do Banco, visando supervisionar o padrão de funcionamento.

4.1.10 Elaborar relatório contendo os resultados das atividades relacionadas à função de compliance.

##### **4.2 Administração do processo.**

4.2.1 Elaborar e manter atualizada, para os processos de responsabilidade da coordenadoria:

a) a política, as normas, os procedimentos, as delegações de responsabilidade e os fluxos de atividades;

b) os indicadores de desempenho, eficiência e qualidade;

c) os métodos, ferramentas e sistemas;

d) identificar as vulnerabilidades, a análise de risco do processo e medidas para mitigá-los.

4.2.2 Coordenar a execução orçamentária de todas as rubricas de responsabilidade da Coordenadoria.

4.2.3 Pesquisar e analisar regulamentos e/ou normativos publicadas pelos órgãos reguladores, afetos ao assunto, analisando impactos e efetuando os necessários ajustes nas políticas e demais normativos internos.

Como se observa, o Banco da Amazônia dividiu sua área de *compliance* em ***Processos Gerenciais e de Suporte e em Processos Finalísticos***.

Na primeira, junto à **COORDENADORIA DE COMPLIANCE EM PROCESSOS GERENCIAIS E DE SUPORTE – COPOG**, o *compliance* atua junto aos procedimentos gerenciais do Banco e no Suporte às unidades: avalia os normativos internos e sugere melhorias e atualizações; verifica a aderência das normas junto às unidades e colaboradores; atua junto a processos relevantes, e junto à criação de novos produtos; monitora os próprios indicadores de compliance; monitora eventuais falhas na conformidade do Banco frente às normas impostas pelos órgãos externos e reguladores; emite recomendações técnicas e alertas de controle, a fim de minimizar deficiências e fragilidades em processos, produtos e serviços; elabora relatórios relacionados ao compliance entre outras responsabilidades.

Na segunda, junto à **COORDENADORIA DE COMPLIANCE EM PROCESSOS FINALÍSTICOS – COCOF**, o *compliance* atua junto aos processos finalísticos do Banco: faz a conformidade operacional em processos de negócio, incluindo a criação e aprovação de novos produtos; avalia a eficácia do *compliance* na primeira linha de atuação, feita pela **COPOG**; indica necessidade de melhorias; monitora o controle das agências e os indicadores de *compliance*; monitora os negócios e produtos do Banco, visando supervisionar o padrão de funcionamento; elabora relatório contendo os resultados das atividades relacionadas à função de *compliance*, entre outras responsabilidades.

As áreas de *compliance* do Banco da Amazônia funcionam de maneira efetiva. Prova disso são os índices de conformidade atingidos pela Instituição, seja em processos internos seja naqueles envolvendo terceiros, e, principalmente, na atuação junto ao público alvo, que é a venda de produtos e serviços.

Os índices de conformidade<sup>23</sup> podem ser medidos, por exemplo, em eventuais multas aplicadas pelos órgãos de controle, ou mesmo pelo *rating* das ações judiciais julgadas a favor ou contra a empresa, onde os números do Banco se mostram, sem positivos.

Com efeito, o Banco possui um sistema de controles internos adequados ao seu porte, perfil de risco e natureza dos seus negócios, adota como metodologia de controle interno, o modelo das Três Linhas de defesa, que assegura as competências e responsabilidades de todas as áreas da Instituição, por meio de uma estrutura integrada e coordenada, o que contribui para a efetividade dos controles internos e geração de resultados sustentáveis. Utiliza o framework COSO – Estrutura Integrada, considerando os seus componentes e princípios<sup>24</sup>.

O modelo de Três Linhas de Defesa foi instituído pelo Instituto de Auditores do Brasil (IIA Brasil), em janeiro de 2013, com a publicação da cartilha conhecida como "As Três Linhas de Defesa". Resumidamente pode se definir o modelo de Três Linhas de da seguinte forma (THE INSTITUTE OF INTERNAL AUDITORS, 2013):

- **Primeira linha de defesa:** representada pelas unidades operacionais, na qualidade de gestora de processos e proprietária dos riscos, será responsável pelo desenho, implementação e condução de seu processo e, conseqüentemente, por identificar,

---

<sup>23</sup> <https://www.bancoamazonia.com.br/index.php/relacoes-com-investidores/sobre-o-banco/ratings>

<sup>24</sup> <https://www.bancoamazonia.com.br/component/edocman/relatorio-anual-integrado-e-sustentabilidade-2021/viewdocument/5229?Itemid=0>

avaliar e mitigar riscos, além de definir e manter controles internos eficientes e implementar ações corretivas para resolver deficiências em processos e controles.

- **Segunda linha de defesa:** detém as funções de gerenciamento de risco e conformidade e neste sentido deve trabalhar em conjunto com a primeira linha de defesa para garantir identificação, avaliação e reporte as alçadas competentes. É de responsabilidade da segunda linha de defesa identificar regulamentações, estabelecer políticas, definir linguagem comum de riscos, mensurar os riscos e zelar pelo controle efetivo, de forma a assegurar que estejam sendo conduzidos de acordo com o nível de apetite definido, reportando resultados para os colegiados superiores. No Banco da Amazônia a segunda linha de defesa é composta, essencialmente, pelas equipes: controles internos e compliance (GECIN), riscos (GERIS), controles contábeis e financeiros (GECON), segurança (GESEC) e jurídica (GEJUR).
- **Terceira linha de defesa:** representada pela Auditoria Interna, deve revisar de modo sistemático e eficiente as atividades das duas primeiras linhas de defesa e contribuir aprimoramento.

**Figura 5 – Modelos de Três linhas de Defesa**



Fonte: (BANCO DA AMAZÔNIA, 2022, p. 60).

Tais estruturas asseguram um ambiente de integridade e confiança nas relações e possibilitam a promoção de ações educativas, preventivas e corretivas

concernentes à ética profissional, aos colaboradores e no tratamento com as pessoas e com o patrimônio público, onde todos os níveis hierárquicos terão papéis e responsabilidades em suas atividades objetivando a eficácia dos controles internos, cabendo ao Conselho de Administração, como instância máxima de controle interno do Banco, manter independência da gestão e exercer por meio das estruturas e processos que lhe dão suporte a supervisão sobre a administração da Instituição no desenho, implementação e aplicação dos controles.

Todavia, ao analisar o organograma da Instituição Financeira, principalmente junto à **GERÊNCIA EXECUTIVA DE CONTROLES INTERNOS (GECIN)**, e as 02 (duas) Coordenadorias (*COCOF e COPOG*), não há um órgão no Banco junto ao compliance responsável, especificamente, pelo controle e aplicação específica das normas da Lei 13.709/2018.

E, neste ponto, cinge-se o ponto nevrálgico do presente trabalho: pela envergadura e importância da LGPD, através das normas e obrigações previstas na Lei 13.709/2018, a proposição é a criação de uma **nova Coordenadoria no Banco da Amazônia**, junto à **GECIN – Gerência Executiva**, para análise, fiscalização e aplicabilidade da lei.

## **6.10 Proposta de aprimoramento do modelo de *compliance* junto ao Banco da Amazônia para adaptação à LGPD**

Neste capítulo apresenta-se os aspectos inovativos do trabalho, a importância de um modelo de compliance autônomo para cumprimento da Lei de Proteção de Dados e a criação de uma Coordenação independente para cumprimento e fiscalização da LGPD. Estrutura e organização.

### **6.10.1 Aspecto inovativo do trabalho**

Segundo o Manual de Oslo (OCDE, 2004), o conceito de inovação é definido como a implementação de um produto (bem ou serviço) novo ou significativamente melhorado, ou um processo, ou um novo método de marketing, ou um novo método organizacional nas práticas de negócios, na organização do local de trabalho ou nas relações externas.

Para a formação no mestrado Programa de Pós-Graduação em Propriedade Intelectual e Transferência de Tecnologia para a Inovação – PROFNIT, a natureza inovativa do trabalho e do produto a ser apresentado é essencial.

A proposta apresentada no projeto, originariamente, apresentou a proposta de desenvolvimento de 03 (três) objetivos específicos:

- a) Examinar as exigências legais trazidas pela LGPD ao setor bancário, por meio de uma revisão de literatura;
- b) Identificar os procedimentos e opções práticas de *compliance* à implementação do tratamento de dados ao setor bancário; e, finalmente,
- c) Aprimorar o sistema de *compliance* aplicado ao sistema bancário, o qual contemple as normas inovadoras da LGPD, e proteja as empresas de futuros dissabores, considerando as punições dela decorrentes

Na oportunidade da apresentação do projeto para a qualificação, apresentou-se os 02 (dois) primeiros objetivos específicos: o trabalho examinou e detalhou as exigências legais trazidas pela LGPD ao setor bancário, por meio de uma revisão de literatura, e; identificou os procedimentos e opções práticas de *compliance* à implementação do tratamento de dados ao setor bancário.

E, agora, com a entrega da Dissertação, encerra-se o terceiro e último objetivo específico. O projeto apresenta uma alteração do modelo de compliance do Banco da Amazônia, com a criação de uma Coordenadoria junto à **GECIN GERÊNCIA EXECUTIVA DE CONTROLES INTERNOS**, com o objetivo de *aprimorar o sistema de compliance aplicado ao Banco, o qual contemple as normas inovadoras da LGPD, e proteja a empresa de futuros dissabores, considerando as punições dela decorrentes.*

O projeto tem vinculação à inovação em processo e inovação organizacional, visto que objetiva propor o aprimoramento do sistema aplicado ao *compliance* da Instituição Financeira. A proposta de criação de uma nova Coordenadoria, com um novo arcabouço de normas/regras e o aprimoramento do sistema, desaguará em uma reestruturação da cadeia de processos hoje existente, tudo com o fito de proteger a empresa das punições decorrentes da norma legal. Insere-se, portanto, dentro do tema de Propriedade Intelectual (inovação em processo) e Transferência de Tecnologia.

Nesse sentido, a proposta desenvolvida, com a adaptação do modelo de *compliance*, centraliza a análise das obrigações legais criadas pela LGPD em um único setor, com uma nova plataforma. Os bancos terão que alterar significativamente suas

rotinas de trabalho, para identificar a forma como coletam os dados, a natureza destes, a base legal para tratá-los, eventual descarte, até a possibilidade final de compartilhamento. Isso é, conceitualmente, inovação em processo.

E, finalmente, a alteração do sistema de *compliance* encerra, também, natureza de inovação organizacional, que “é a implementação de um novo método organizacional nas práticas de negócios da empresa, na organização do seu local de trabalho ou em suas relações externas” (OCDE, 2004, p. 61).

Como outrora retratado, a implantação de um novo modelo de conformidade, ou sua alteração substancial, necessariamente caracteriza um novo método organizacional: novos conceitos e definições; atribuições de novas responsabilidades, aqueles que irão analisar os riscos e os dados pessoais existentes; aqueles que irão tratar os dados; aqueles que irão adaptar as novas rotinas e segmentá-las com todas as unidades da organização; aqueles que irão compartilhar os dados etc. Estas novas rotinas e responsabilidades se reveste em um novo modelo organizacional, e, por isso, inova neste segmento.

#### 6.10.2 A importância de um modelo de compliance independente para cumprimento da Lei de Proteção de Dados

Ao analisar todo o arcabouço documental, verificou-se que o Banco da Amazônia aplicou de forma sólida, efetiva e segura os comandos da Lei Geral de Proteção de Dados – 13.709/2018. Desde a contratação de uma renomada equipe de profissionais externos, até a capacitação dos empregados públicos internos, o Banco passou por um longo período de adaptação, dentro do lapso temporal de vacância da norma.

A concepção de um Plano de Implantação, criteriosamente elaborado pelas equipes, gerou o sucesso da empreitada. Atualmente, o Banco cumpre os requisitos objetivos e subjetivos da lei, o que dá conforto no planejamento dos negócios e, principalmente, segurança aos clientes, no que pertine à segurança dos dados pessoais mantidos e controlados pela Instituição Financeira.

Atualmente, o Banco tem um vasto e criterioso compêndio de normativos internos, todos ligados umbilicalmente à segurança dos dados e à conformidade e integridade dos negócios, tais como: um Código de Ética atualizado e em vigor; Normas Internas para descarte das informações; Comitês de Privacidade e Gestão Integrada;

órgão de Auditoria Interna independente e descentralizada; Normas Internas de Gestão de Conformidade, de Tratamento e Classificação das Informações; e normas internas criteriosas ligadas à Política de Gestão de Dados Pessoais, de Integridade e de Governança de Dados.

Todo este arcabouço de normativos internos, somados às demais normas editadas pelos órgãos de controle (BACEN, TCU, CGU etc), e as Leis Federais, asseguram ao cliente a convicção do estrito cumprimento na proteção e manipulação dos dados pessoais coletados e mantidos pela Instituição Financeira.

E o comprometimento da Alta Administração do Banco da Amazônia com as regras de compliance, e sua autonomia, essencial para o sucesso do sistema, vem definida nas diretrizes da POL 309 (BANCO DA AMAZÔNIA, [2023?]):

#### 6 DIRETRIZES

6.1 O Compliance será um dos pilares da governança corporativa que fortalecerá o ambiente de controles internos da Instituição, monitorando a conformidade com leis e regulamentos internos e externos, gerando a legitimidade e aumentando a transparência, o que favorecerá a vantagem competitiva e proporcionará a sustentabilidade da organização.

6.2 O Compliance deverá ser colocado em prática de modo contínuo pela estrutura de governança do Banco, alta administração, comitês e empregados conforme suas funções e responsabilidades. Todos os empregados deverão zelar pela integridade, ética e competência, responsabilidades, padrões de gerenciamento, organização e alocação de recursos.

6.3 O Banco incentivará seus empregados, terceirizados, dirigentes e conselheiros a prática de elevados padrões de comportamento ético e de governança, visando o fortalecimento da gestão do risco de compliance.

6.4 O Conselho de Administração (CONSAD), como instância máxima de controle interno do Banco, manterá independência da gestão e exercerá por meio das estruturas e processos que lhe dão suporte a supervisão sobre a administração da Instituição no desenho, implementação e aplicação dos controles internos.

6.5 A responsabilidade sobre o Compliance será de todos os empregados, permeará toda a estrutura organizacional do Banco e todos os níveis hierárquicos terão papéis e responsabilidades em suas atividades, objetivando a eficiência e eficácia dos controles internos.

6.8 A área responsável pelo Compliance deverá atuar de forma independente e autônoma das demais áreas da Instituição, para evitar os conflitos de interesses e assegurar a isenta leitura dos fatos, visando à busca da conformidade por meio de ações corretivas e preventivas. A unidade responsável pela função de conformidade e controles internos deverá ser integralmente segregada da atividade de auditoria interna.

6.9 A Instituição dará livre acesso aos responsáveis pelas atividades relacionadas à função de compliance às informações necessárias para o exercício de suas atribuições, incluindo o acesso a qualquer informação, colaborador ou administrador da Instituição.

Com efeito, a proposta apresentada neste projeto de pesquisa visa aprimorar o sistema de compliance, especificamente ligado à atividade de coleta e controle, e o

sigilo e a confidencialidade do processamento e armazenamento dos dados. E, neste ponto, acredita-se que a criação de uma Coordenadoria própria, e independente, unicamente ligada à proteção de dados (LGPD), será ponto fundamental para aprimorar o sistema de controle e mitigar os riscos, principalmente face às multas milionárias previstas na legislação.

Impende registrar, também, que com a publicação da [Lei 13.709/18](#) Lei Geral de Proteção de Dados Pessoais, para além do mero e simples controle na coleta e manipulação, estabeleceu-se como obrigação destes agentes de *tratamento* de dados pessoais a adoção de “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” (BRASIL, 2018, p. 63, art. 46).

Ainda no campo normativo, em 2020 foi publicada a nova versão da [IN 01 DSIC/GSIPR](#) que dispõe sobre a Estrutura de Gestão da Segurança da Informação e define diretrizes para a elaboração da Política de Segurança da Informação dos órgãos e entidades da administração pública federal<sup>25</sup>.

Desta forma, a criação de um órgão específico e individualizado, unicamente ligado à gestão e controle dos dados, poderá concentrar-se em atividades coordenadas para controlar e monitorar todos os processos da Instituição Financeira que envolvam a coleta e a segurança dos dados, objetivo maior da LGPD. Uma Coordenação de Compliance ligada à LGPD poderá criar mecanismos de gestão, com origem desde às agências da rede bancária, na ponta da Instituição, onde geralmente a coleta dos dados se inicia, até o destino final, com Operador e o Controlador dos dados.

A gestão dos dados pessoais e a própria gestão do compliance justificam referida criação, de uma área independente, na medida em que o risco das sanções legais, decorrentes da Lei 13.709/2018, vão muito além das perdas financeiras. Há o risco, iminente, das perdas reputacionais derivadas da falta de cumprimento das Leis e normas regulamentadoras, e a perda da credibilidade junto ao mercado.

Atualmente, o mercado, principalmente o financeiro, exige do Banco um cumprimento estrito de princípios e condutas éticas, e a política de integridade e conformidade nos negócios recebe um grau máximo de controle, o que, também, justifica ao nosso ver a criação da referida unidade independente.

---

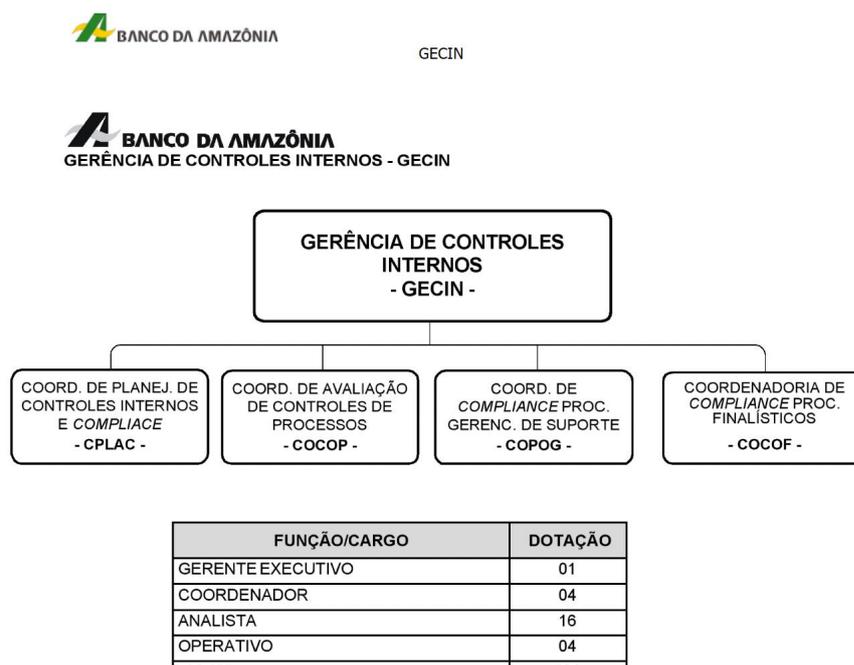
<sup>25</sup> POL 304 - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

### 6.10.3 Criação de uma Coordenação independente para cumprimento e fiscalização da LGPD. Estrutura e organização

Como exposto neste projeto, no organograma do Banco da Amazônia, junto à **GERÊNCIA EXECUTIVA DE CONTROLES INTERNOS (GECIN)**, há 02 (duas) Coordenadorias (*COCOF e COPOG*), sem que nenhuma delas tenha ligação umbilical pelo controle e aplicação específica das normas da Lei 13.709/2018.

Nesse sentido, o presente trabalho, pela envergadura e importância da LGPD, através das normas e obrigações previstas na Lei 13.709/2018, faz a proposição pela criação de uma **nova Coordenadoria no Banco da Amazônia**, junto à **GECIN – Gerência Executiva**, para análise, fiscalização e aplicabilidade da lei.

Figura 6 - GECIN



Fonte: (BANCO DA AMAZÔNIA, [2023?]).

A estrutura:

Propõem-se a criação da **Coordenação de Compliance no Gerenciamento e Acompanhamento de Processo de Dados Pessoais**, com designação/criação de 01 (um) cargo de Coordenador, 04 (quatro) analistas e 01 (um) operativo, tal qual os colaboradores já designados nas outras Coordenadorias.

A organização e responsabilidades:

Para propiciar o acompanhamento e gerenciamento dos dados pessoais, evidencia-se a necessidade de identificar-se a natureza e qualidade da informação, o que também deverá estar afetar à referida Coordenadoria. Desta forma, ficará afeto a este órgão classificar as informações, tais como de natureza **PÚBLICA** (*divulgada publicamente, sem restrição de acesso e cuja divulgação não cause qualquer dano à instituição.*), **INTERNA** (*pode ser divulgada a todos os empregados e prestadores de serviços, desde que estes estejam comprometidos com a confidencialidade das informações*), **RESTRITA** (*pode ser divulgada a determinadas áreas, grupos ou funções, cuja divulgação pode acarretar prejuízos ao Banco*) ou **SIGILOSA** (*Informação que requer um tratamento especial e cuja divulgação não autorizada ou acesso indevido pode gerar prejuízos financeiros, legais, normativos, contratuais ou de reputação, imagem ou estratégia do Banco*).

Para além disso, elencou-se, abaixo, uma prévia das áreas afetas à nova Coordenadoria, algumas já existentes no sistema da Instituição e agora proposto o seu deslocamento, e outras inéditas, objeto deste trabalho (BANCO DA AMAZÔNIA, [2023?]):

- a) Identificação de todo o normativo, interno e externo, sobre a LGPD e conformidade de dados, e manter inventário atualizado deste arcabouço legal;*
- b) Identificação e orientação às demais unidades do Banco acerca das bases legais da Lei 13.709/2018, que autorizam a coleta e tratamento dos dados por parte da Instituição Financeira;*
- c) Identificação das unidades internas do Banco que coletam dados pessoais;*
- d) Identificação das unidades internas do Banco que manipulam dados pessoais;*
- e) Identificação dos processos e/ou das atividades relevantes para empresa, levando em consideração tanto os aspectos da conformidade operacional, quanto regulatória;*
- f) Identificação dos processos de verificação obrigatória que contenham coleta e necessidade de tratamento de dados pessoais, tais como: cadastro; contrato de abertura de contas; todas as operações de crédito (contratos de mútuo etc); transações realizadas via canais de atendimento; contratos administrativos realizados pelo Banco, incluindo as licitações;*
- g) Identificação, análise e acompanhamento dos procedimentos junto ao setor de Recursos Humanos, contratação e demissão dos empregados e a coleta e tratamento dos dados dos empregados públicos e terceirizados;*
- h) Propor a divisão, dentro da Coordenadoria, de subgrupos de controle para gerenciamento no cumprimento das normas;*
- i) Controle periódico das agências/unidades responsáveis pelo cadastro dos clientes e coleta dos dados, principalmente com supervisão dos contratos de abertura de crédito e autorização dos terceiros para a coleta e tratamento dos dados pessoais;*

- j)** *Monitorar os procedimentos de controle de acesso às informações que contenham dados pessoais, com objetivo de garantir que somente pessoas autorizadas tenham acesso à determinada informação, recurso computacional ou ambiente físico.*
- k)** *Monitorar e acompanhar os contratos e procedimentos (relacionamentos) mantidos com todos os fornecedores de serviços, independentemente da natureza (notadamente a segurança dos dados, documentos e informações), de modo a mitigar riscos associados ao acesso dos fornecedores aos ativos do Banco.*
- l)** *Identificar, cadastrar, monitorar e relatar incidentes de segurança da informação relevante ou incidente cibernético, envolvendo dados pessoais, que afetem o Banco ou terceiros;*
- m)** *Considerando os dados pessoais já tomados pelo Banco, e após a implantação da LGPD, propor, periodicamente e assim que necessário, a classificação, reclassificação, anonimização e pseudonimização, manuseio, armazenamento, transporte e descarte dos dados, alertando a rede da utilização de forma transparente e apenas para a finalidade para a qual foi autorizada.*
- n)** *Acompanhar os procedimentos e forma de descarte dos dados;*
- o)** *Realizar teste de avaliação junto a todas as unidades identificadas, e verificar a aderência ao arcabouço legal, à regulamentação infralegal, às recomendações dos órgãos de supervisão e, quando aplicáveis, aos códigos de ética e de conduta do Banco;*
- p)** *Propor e encaminhar relatório sistemático dos resultados à DICOR (Diretoria de Controle e Risco), à GERIS (Gerência de Riscos Corporativos), à DIREX (Diretoria Executiva) e ao CONSAD (Conselho de Administração);*
- q)** *Promover a disseminação de valores, e programas de conscientização da segurança dos dados, via comunicados e comunicações internas de forma contínua, dos princípios e normas ligadas à LGPD e à necessidade de adaptação e cumprimento da lei de proteção de dados, propondo treinamentos obrigatórios, disseminação de artigos etc;*
- r)** *Atuar, juntamente com a Comissão de Privacidade e Proteção de Dados Pessoais (CPPD), na avaliação de contratos congêneres que envolvam tratamento de dados pessoais e nos incidentes de violação de dados pessoais no âmbito da LGPD.*
- s)** *Reportar imediatamente a identificação de qualquer fato relevante, deficiência, falha ou não cumprimento das normas de proteção de dados à autoridade superior.*
- t)** *Criar uma Política de Gestão e Acompanhamento dos Dados Pessoais, ligada à Lei 13.709/2018, bem como alinhada aos demais normativos congêneres;*
- u)** *As diretrizes relativas à gestão do Compliance dos dados pessoais deverão ser revistas periodicamente a fim de que os controles internos se mantenham adequados e a eles sejam incorporadas medidas relacionadas à mitigação de risco de Compliance, de acordo com a natureza e complexidade dos negócios do Banco da Amazônia.*

Com a criação desta nova unidade, dentro da Gerência de Controle de Riscos – GECIN, acredita-se que o controle dos processos será aferido de maneira mais incisiva, aprimorando os procedimentos e mitigando os riscos na aplicação dos comandos da LGPD.

## 7 CONCLUSÃO

Impende registrar, de início, que os estudos e trabalhos, pesquisas de campo, entre outros, foram iniciados durante o período pandêmico da COVID-19. Tal situação dificultou sobremaneira a obtenção tempestiva de informações, os estudos e a difusão do trabalho. Aulas *on line*, dificuldades de comunicação com os discentes (naturais, diante da circunstância), impossibilidade de visitas *in locu* aos locais a serem visitados pela busca de material foram alguns dos principais pontos negativos da caminhada.

D`outra banda, convém esclarecer que, durante a execução do trabalho, abriu a possibilidade de exploração de inúmeros outros dados e elementos de pesquisa, tais como os fluxos de processos existentes na gestão de *compliance*, a forma de tratamento, o tempo e a devolutiva, com a respectiva solução. Contudo, além de ser um dado extremamente sensível ao Banco, não houve tempo suficiente para estratificar as informações, o que poderá, certamente, ser alvo de um futuro trabalho, via artigo científico ou mesmo tese de doutoramento, dado ao seu ineditismo.

A Lei Geral de Proteção de Dados – Lei 13.709/2018 veio, em um cenário mais que tardio, proteger importantes direitos do cidadão. Os dados pessoais estão umbilicalmente ligados aos direitos da privacidade, da liberdade e do livre desenvolvimento da personalidade, todos de hospedagem constitucional.

Diz o artigo 5º, da CF/88:

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

[...]

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação (BRASIL, 2016, p. 13).

E o Código Civil Brasileiro vaticina, em seus artigos 12 e 21:

Art. 12. Pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo

[...]

Art. 21. ‘A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma’. o de outras sanções previstas em lei (BRASIL, 2002, p. 145; 146).

Como destaca Patrícia Peck Pinheiro, a LGPD foi criada com o objetivo principal de proteger os direitos fundamentais de liberdade e privacidade das pessoas, bem como promover o livre desenvolvimento de suas personalidades. Com isso, a lei estabelece uma série de princípios e medidas de controle técnico que devem ser seguidos para garantir a segurança e a privacidade dos dados pessoais identificáveis. E entre os principais impactos da LGPD está a garantia dos direitos dos titulares, que incluem o direito à portabilidade dos dados pessoais. Esses direitos são novos para o ordenamento jurídico e para empresas públicas e privadas, e devem ser respeitados dentro de um prazo razoável previsto pela lei brasileira. Em resumo, as instituições devem estar preparadas para cumprir com as exigências da lei e garantir a proteção dos dados pessoais dos titulares (PINHEIRO, 2023).

Cumprir a LGPD implica estar conforme e respeitar os Direitos Humanos, o que, atualmente, é fundamental para o crescimento de qualquer empresa ou organização. Os direitos ligados à privacidade e, principalmente, à propriedade e livre disposição dos dados, com a edição da nova lei, tomou uma nova dinâmica nesta era da Big Data, pois de nada adianta promover grandes avanços tecnológicos sem garantir essa prerrogativa às pessoas. “A partir dessa afirmação, depreende-se que organizações públicas e entidades privadas que não seguem a LGPD não respeitam os Direitos Humanos” (BALDISSERA, 2022).

Qualquer discussão sobre os cenários tecnológicos, na atualidade, perpassa por uma análise metódica dos impactos dos dados na sociedade, conceito dado à “*Data Driven Society*”<sup>26</sup>. E é nesta seara que o mercado, há muito, enxerga os dados, como um dos maiores ativos financeiros, e, por isso, a necessidade de uma legislação específica para tratar e regulamentar a matéria.

**Conforme relatou, em entrevista, o atual** diretor-presidente da ANPD (Autoridade Nacional de Proteção de Dados), Waldemar Gonçalves, em entrevista ao programa Brasil em Pauta, da TV Brasil. Na avaliação de Gonçalves, o cidadão é o elo mais fraco na cadeia de proteção dados. Segundo ele, a “riqueza” da atualidade é a proteção de informações pessoais e ANPD tem papel essencial na defesa dos dados de brasileiros. “Quando no passado, nós tínhamos o petróleo como a grande riqueza. **No**

---

<sup>26</sup> <https://medialab.espm.edu.br/data-driven-society/>

**século 21, hoje, os dados são o novo petróleo.** Exatamente porque a empresa viu quão precioso esses dados [são]” (BRASIL [...], 2021, 8 min 11 seg) e completa,

Com desenvolvimento tecnológico, inteligência artificial, a coisa hoje é de uma velocidade muito rápida. Quando faço uma pesquisa na Internet e olho um determinado produto, poucos segundos depois começa a surgir ‘do nada’ uma série de ofertas daquele produto. São empresas que comercializam essas informações e passam a ser extremamente valiosas. Esse que é nosso foco, essa proteção de dados. Até a criação da autoridade, ele não tinha a quem recorrer de forma mais pontual (BRASIL [...], 2021, 8 min 42 seg grifo nosso).

Com efeito, diante deste novo cenário criado pela Lei Geral de Proteção de Dados, e das consequências desastrosas àqueles que a descumprirem, iniciou-se, a partir da publicação da norma, em agosto de 2018, uma corrida frenética para sua análise e implantação, notadamente para as empresas que, de qualquer forma, coletassem e manipulassem dados pessoais.

E, nesse contexto, as Instituições Financeiras foram atingidas em cheio. Talvez poucas empresas mantenham, em seus cadastros, mais dados pessoais de clientes que os Bancos. Foi neste ambiente que se idealizou o presente trabalho: em que medida a LGPD impactou as Instituições Financeiras e, para além disso, de que forma o setor de compliance bancário poderia ajudar nesse cenário transformador, a fim de garantir o cumprimento da norma. O problema estava, então, apresentado<sup>27</sup>.

Para tanto, propôs-se os objetivos do trabalho (geral e específicos), onde, inicialmente, examinou-se as exigências legais trazidas pela LGPD às empresas do setor bancário. Assim, no capítulo 7 (sete), além de um contexto histórico da norma, fez-se uma longa estratificação das novas exigências legais aplicadas ao setor bancário, bem como os procedimentos e opções práticas de *compliance* possíveis à implementação do tratamento de dados na nova realidade.

Analisou-se, de forma criteriosa o artigo 7º, da Lei 13.709/2018 – as bases legais, e quais delas, ao entendimento deste trabalho, são aplicadas às Instituições Financeiras. Examinou-se o consentimento (art. 7º, I, da LGPD), certamente a base legal de maior importância dentro deste novo panorama. O titular dos dados, consentindo com a coleta e o tratamento deste, certamente não colocará em risco a

---

<sup>27</sup> De que forma é possível adaptar o sistema de *compliance* para o setor bancário, de modo que atenda as inovações criadas pela Lei Geral de Proteção de Dados, e, de consequência, reduza os riscos de danos administrativos e financeiros dela decorrentes?

empresa ou pessoa detentora (operador ou controlador), salvo exceções previstas na norma. A *execução de contrato*, a *proteção do crédito*, e o *cumprimento de obrigação legal*, previstas no mesmo art. 7º, incisos II, V, X, da LGPD, foram outras bases legais igualmente analisadas, e de que forma os agentes financeiros poderão utilizá-las.

O trabalho dedicou um espaço à parte para discutir o *legítimo interesse*, contida no art. 7º, IV, da Lei 13.709/2018, e a vertical discussão hoje existente no mundo jurídico sobre a utilização desta base legal, e os potenciais problemas futuros. E o item 7.8 trouxe os procedimentos de *compliance* disponíveis para, paralelamente a outros setores da Instituição, dar vazão ao cumprimento rigoroso da novel legislação.

Chegou-se, então, à parte final, onde o projeto apresenta um *estudo de caso*, de acordo com o setor de conformidade e *compliance* do Banco da Amazônia, importante Banco Público Federal, certamente o maior agente de fomento da região norte do Brasil, e ator principal e exclusivo na aplicação do FNO – Fundo Constitucional de Financiamento do Norte, criado pelo art. 159, da CF/88, e regulamentado pela Lei 7.897/1989.

A proposta apresenta, então, a criação de uma nova Coordenadoria de Trabalho, unicamente responsável pelo *compliance* ligado à Lei Geral de Proteção de Dados. A sugestão indicada não se trata de uma proposição exclusiva ao Banco da Amazônia, mas sim a todas as Instituições Financeiras, à rede bancária e agentes financeiros.

A criação de um setor/órgão de conformidade é obrigatório aos Bancos, conforme já destacado em linhas pretéritas, isso desde a Resolução BACEN 2554/1998 e hoje materializado pela Lei das Estatais.

É inconteste que a LGPD criou uma nova perspectiva, dentro do setor de conformidade, dado à quantidade de exigências criadas pela norma. Desta forma, a criação de um órgão específico e individualizado, unicamente ligado à gestão e controle dos dados, poderá concentrar, em local próprio, atividades coordenadas para controlar e monitorar todos os processos da Instituição Financeira que envolvam a coleta e a segurança dos dados, objetivo maior da LGPD.

Uma Coordenação de Compliance ligada à LGPD poderá criar e facilitar os mecanismos de gestão, com origem desde às agências da rede bancária, na ponta da Instituição, onde geralmente a coleta dos dados se inicia, até o destino final, com

Operador e o Controlador dos dados. Este novo panorama justifica a concepção de uma área independente, na medida em que o risco das sanções legais, decorrentes da Lei 13.709/2018, vão muito além das perdas financeiras. Há o risco, iminente, das perdas reputacionais derivadas da falta de cumprimento das Leis e normas regulamentadoras, e a perda da credibilidade junto ao mercado.

Como ao final exposto, o mercado, principalmente o financeiro, exige da Instituição Financeira um cumprimento estrito de princípios e condutas éticas, e a política de integridade e conformidade nos negócios recebe um grau máximo de controle, o que, também, justifica a criação da referida unidade independente.

A lei geral de proteção de dados não é apenas uma norma imperativa dotada de princípios e finalidades, **ela vem trazer uma cultura de compliance a qual não faz lei e não é lei, porém estabelece condutas éticas e morais que ajudaram a combater a corrupção sistemática.**

A LGPD obriga que todos os envolvidos no processo de tratamento de dados - *controladores/operadores e o encarregado* -, **sejam acobertados por códigos de condutas, termos de sigilo, políticas de privacidade e proteção**, além de uma análise sistemática quando do uso dos dados pessoais (TEIXEIRA, [2020], grifo nosso).

A Lei Geral de Proteção de Dados criou uma agência reguladora, a Autoridade Nacional de Proteção de Dados (ANPD). Desde o início da vigência da norma, referido órgão vem, paulatinamente, se estruturando, e, quando chegar ao seu ápice, de gestão e controle, as consequências legais do descumprimento da lei certamente baterão às portas das empresas, organizações, pessoas físicas, enfim, todos aqueles que manipulem dados sem o devido rigor.

E as multas, como à sociedade exposto neste trabalho, são milionárias, o que será determinante para a continuidade dos negócios. Os dados pessoais, como fator de geração de divisas, somente serão garantidos pela efetiva aplicação da LGPD, seja de forma coercitiva ou espontânea, a fim de ser o elo garantidor das riquezas do novo petróleo na atualidade (TEIXEIRA, [2020]).

Não há espaço para retrocesso!

## REFERÊNCIAS

10 BASES Legais da LGPD: [Tabela com todas as definições]. *In: Legalcloud Consultoria LTDA*, 5 nov. 2020. Disponível em: <https://legalcloud.com.br/bases-legais-lgpd-tabela/>. Acesso em: 11 mar. 2022.

ALVES, Jorge. *Compliance para Mercados Regulados*. *In: CONGRESSO DE COMPLIANCE*, 3., 2013. *Anais [...]*. São Paulo: IBC Brasil, 2013. (pelo Banco Votorantim).

AREAS, Patrícia de Oliveira; FREY, Irineu Afonso. O que é Permitido Fazer com a Tecnologia? *In: FREY, Irineu Afonso; TONHOLO, Josealdo; QUINTELLA, Cristina M. (org.). Transferência de tecnologia*. Salvador: IFBA, 2019. p. 44-102. (PROFNIT, Conceitos e aplicações de Transferência de Tecnologia; V. 1). ISBN: 978-85-67562-48-3. Disponível em: <https://www.profnit.org.br/wp-content/uploads/2019/10/PROFNIT-Serie-Transferencia-de-Tecnologia-Volume-I-WEB-2.pdf>. Acesso em: 11 mar. 2022.

BALDISSERA, Olívia. O objetivo da LGPD explicado por Patrícia Peck. *Pós PUCPR Digital Trends*, 2 jun. 2022. Direito. Disponível em: <https://posdigital.pucpr.br/blog/objetivo-lgpd>. Acesso em: 8 mar. 2023.

BANCO CENTRAL DO BRASIL. Resolução nº 2.554, de 24 de setembro de 1998. Dispõe sobre a implantação e implementação de sistema de controles internos. Brasília, DF, 1998. 5 p. Disponível em: [https://www.bcb.gov.br/pre/normativos/res/1998/pdf/res\\_2554\\_v3\\_P.pdf](https://www.bcb.gov.br/pre/normativos/res/1998/pdf/res_2554_v3_P.pdf). Acesso em: 11 mar. 2022.

BANCO CENTRAL DO BRASIL. Resolução nº 4.658, de 26 de abril de 2018. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. Brasília, DF, 2018. p. 1-11. Disponível em: [https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50581/Res\\_4658\\_v1\\_O.pdf](https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50581/Res_4658_v1_O.pdf). Acesso em: 15 maio 2021.

BANCO DA AMAZÔNIA. [Site]. Belém-Pará, [s. d]. Disponível em: <https://www.bancoamazonia.com.br/>. Acesso em: 11 jan. 2023.

BANCO DA AMAZÔNIA. **Carta anual de políticas públicas e governança corporativa**: exercício 2021. Belém-Pará, abr. 2021. Disponível em: <https://www.bancoamazonia.com.br/component/edocman/carta-anual-de-politicas-publicas-2021/viewdocument/5033>. Acesso em: 12 fev. 2023.

BANCO DA AMAZÔNIA. Estrutura Organizacional. [2023?]. Disponível em: <https://www.bancoamazonia.com.br/index.php/relacoes-com-investidores/sobre-o-banco/estrutura-organizacional>. Acesso em: 15 jan. 2023.

BANCO DA AMAZÔNIA. FNO Fundo Constitucional de Financiamento do Norte (LEIS Nº 7.827/1989, Nº 9.126/1995 e Nº 10.177/2001). Processo de Contas Ordinárias Exercício de 2017. Belém-Pará, abr. 2018. Disponível em: <https://antigo.mdr.gov.br/images/stories/acessoainformacao/relatoriodegestao/2017/fno-RelatorioGestao.pdf>. Acesso em: 12 fev. 2023.

BANCO DA AMAZÔNIA. O papel estratégico do BASA para o Desenvolvimento da Amazônia, incluindo os bancos do Brasil e do Nordeste, como operadores do Fundo Constitucional de Financiamento do Centro-Oeste (FCO) e do Fundo Constitucional de Financiamento do Nordeste (FNE). Brasília, DF, AEBA, 7 nov. 2019. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/cindra/arquivos/07-11-2019-2>. Acesso em: 15 jan. 2023.

BANCO DA AMAZÔNIA. **Relatório Anual Integrado e Sustentabilidade2021**. Belém-Pará, abr. 2022. Disponível em: <https://www.bancoamazonia.com.br/component/edocman/relatorio-anual-integrado-e-sustentabilidade-2021/viewdocument/5229?Itemid=0>. Acesso em: 12 fev. 2023.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

BLUM, Renato Opice; ZAMPERLIN, Emelyn. *Compliance*, responsabilidade empresarial e segurança da informação. **Revista brasileira de direito comercial**, Porto Alegre, v. 1, n. 6, p. 97–102, ago./set., 2015.

BRASIL em Pauta: Waldemar Gonçalves, diretor-presidente da Autoridade Nacional de Proteção de Dados. [S. l.: s. n.], 31 jan. 2021. 1 vídeo (27 min 37 seg). Publicado pelo canal TV Brasil. Disponível em: <https://www.youtube.com/watch?v=JhoTUy26nwo>. Acesso em: 1 mar. 2023.

BRASIL. [Código Civil (2002)]. **Código civil brasileiro e legislação correlata**. 2. ed. Brasília, DF: Senado Federal, Subsecretaria de Edições Técnicas, 2008. 616 p. Disponível em: <https://www2.senado.leg.br/bdsf/bitstream/handle/id/70327/C%C3%B3digo%20Civil%202020ed.pdf>. Acesso em: 11 jan. 2023.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**: texto constitucional promulgado em 5 de outubro de 1988, com as alterações determinadas pelas Emendas Constitucionais de Revisão nos 1 a 6/94, pelas Emendas Constitucionais nos 1/92 a 91/2016 e pelo Decreto Legislativo no 186/2008. Brasília, DF: Senado Federal, Coordenação de Edições Técnicas, 2016.496 p. ISBN: 978-85-7018-698-0. Disponível em: [https://www2.senado.leg.br/bdsf/bitstream/handle/id/518231/CF88\\_Livro\\_EC91\\_2016.pdf](https://www2.senado.leg.br/bdsf/bitstream/handle/id/518231/CF88_Livro_EC91_2016.pdf). Acesso em: 15 maio 2017.

BRASIL. Despachos do Presidente da República. Mensagem nº 451, de 14 de agosto de 2018. **Diário Oficial da União**: seção 1, Brasília, DF, ano 155, n. 157, p. 75-81, 15 ago. 2018a. ISSN 1677-7042. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_Ato2015-2018/2018/Msg/VEP/VEP-451.htm](http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Msg/VEP/VEP-451.htm). Acesso em: 4 mar. 2021.

BRASIL. Lei n. 13.303, de 30 de junho de 2016. Dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios. **Diário Oficial da União**: seção 1, Brasília, DF, ano 153, n. 125, p. 1-10, 1 jul. 2016. ISSN 1677-7042. Disponível em:

<https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=1&data=01/07/2016>. Acesso em: 15 mar. 2022.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

**Diário Oficial da União**: seção 1, Brasília, DF, ano 155, n. 157, p. 59-64, 15 ago. 2018b. ISSN 1677-7042. Disponível em:

<https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=515&pagina=59&data=15/08/2018>. Acesso em: 15 maio 2021.

BRASIL. Lei n. 9.613, de 3 de março de 1998. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores, a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências. **Diário Oficial da União**: seção 1, Brasília, DF, ano 136, n. 42, p. 1-3, 4 mar. 1998. ISSN 1677-7042.

Disponível em:

<https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=13&data=04/03/1998>. Acesso em: 15 mar. 2022.

BRASIL. Lei nº 12.846, de 1 de agosto de 2013. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. **Diário Oficial da União**: seção 1, Brasília, DF, ano 150, n. 148, p. 1-3, 2 ago. 2013. ISSN 1677-7042.

Disponível em:

<https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=02/08/2013&jornal=1&pagina=2&totalArquivos=128>. Acesso em: 4 mar. 2021.

BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. **Diário Oficial da União**: seção 1, Brasília, DF, ano 156, n. 130, p. 1-3, 9 jul. 2019. ISSN 1677-7042. Disponível em:

<https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=515&pagina=1&data=09/07/2019>. Acesso em: 12 mar. 2022.

BRASIL. Lei nº 7.827, de 27 de setembro de 1989. Regulamenta o art. 159, inciso I, alínea c, da Constituição Federal, institui o Fundo Constitucional de Financiamento do Norte - FNO, o Fundo Constitucional de Financiamento do Nordeste - FNE e o Fundo Constitucional de Financiamento do Centro-Oeste - FCO, e dá outras providências. Brasília, DF, 27 set. 1989.

Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/17827.htm](http://www.planalto.gov.br/ccivil_03/leis/17827.htm). Acesso em: 1 jan. 2023.

BRASIL. Medida Provisória nº 869, de 27 de dezembro de 2018. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências.

**Diário Oficial da União**: seção 1, Brasília, DF, ano 155, n. 149, p. 8-9, 28 dez.

2018c. ISSN 1677-7042. Disponível em:

<https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=515&pagina=59&data=15/08/2018>. Acesso em: 15 maio 2021.

BRASIL. Ministério da Integração e do Desenvolvimento Regional. Política Nacional de Desenvolvimento Regional. Brasília, DF, 6 mar 2023. Disponível em:

<https://www.gov.br/mdr/pt-br/assuntos/desenvolvimento-regional/pndr>. Acesso em: 15 mar. 2023.

BRASIL. Superior Tribunal de Justiça. **Súmula 550/STJ**. Recurso especial repetitivo. Consumidor. Credit scoring. Recurso especial representativo de controvérsia. Tema 710. Direito do consumidor. Banco de dados. Arquivos de crédito. Sistema credit scoring. Compatibilidade com o direito brasileiro. Brasília, DF: STJ, 19 out. 2015. Doc. LEGJUR 158.0515.0000.0000. Disponível em: <https://www.legjur.com/sumula/busca?tri=stj&num=550#:~:text=26.,dados%20considerados%20no%20respectivo%20c%C3%A1culo.%C2%BB>. Acesso em: 1 mar. 2022.

CANDELORO, Ana Paula P.; RIZZO, Maria B. M. de; PINHO, Vinícius. **Compliance 360°**: riscos, estratégias, conflitos e vaidades no mundo corporativo. São Paulo: Trevisan Editora Universitária, 2012.

COIMBRA, Marcelo de Aguiar; MANZI, Vanessa Alessi (Coord.). **Manual de Compliance**: preservando a boa governança e a integridade das organizações. São Paulo: Atlas, 2010.

COMISSÃO DE VALORES MOBILIÁRIOS. Instrução CVM nº 586, de 8 de junho de 2017. Altera e acrescenta dispositivos à Instrução CVM nº 480, de 7 de dezembro de 2009. In: BRASIL. **Diário Oficial da União**: seção 1, Brasília, DF, ano 154, n. 110, p. 23-28, 9 jun. 2017. ISSN 1677-7042. Disponível em: <https://conteudo.cvm.gov.br/export/sites/cvm/legislacao/instrucoes/anexos/500/inst586.pdf>. / <https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=23&data=09/06/2017>. Acesso em: 15 mar. 2022.

COSTA, Divino Placido da. BASA realiza palestra do Projeto Rota do FNO. In: GUARAÍ (Município). **Câmara Municipal de Guaraí**, Guaraí, TO, 31 maio 2017. Disponível em: <https://www.guarai.to.leg.br/institucional/noticias/basa-realiza-palestra-do-projeto-rota-do-fno>. Acesso em: 2 fev. 2023.

DANON JUNIOR, Isaac; GUIZZO, Camila de Sousa Pereira; NOGUEIRA, Tarso Barreto Rodrigues. *Compliance* no contexto de inovação: uma revisão da literatura internacional. **Blucher Engineering Proceedings**, São Paulo, v. 6, n. 5, p. 458-464, nov. 2019. ISSN 2357-7592. Disponível em: <http://pdf.blucher.com.br/s3-sa-east-1.amazonaws.com/engineeringproceedings/siintec2019/58.pdf>. Acesso em: 5 mar. 2022.

DINIZ, Maria Helena. **Dicionário Jurídico**. São Paulo: Saraiva, 1998, vol. 3.

DOYLE, Eleanor *et al.* *Compliance-innovation: a quality-based route to sustainability*. **Journal of the Cleaner Production**, [s.l.], v. 210, p. 266-275, 10 fev. 2019. ISSN 1879-1786.

EXECUTIVE REPORT: Negócios & TIC - Tecnologia da informação e comunicação. LGPD no setor financeiro, p. 1-12, [2019?]. Disponível em: [https://www.fortinet.com/content/dam/fortinet/assets/solutions/pt\\_br/lgpd-financial.pdf](https://www.fortinet.com/content/dam/fortinet/assets/solutions/pt_br/lgpd-financial.pdf). Acesso em: 15 maio 2021.

FEBRABAN. **Função de Compliance**. [s.n]: Grupo de Trabalho-ABBI-FEBRABAN, jul. 2009. Disponível em: [http://www.abbi.com.br/download/funcaoodecompliance\\_09.pdf](http://www.abbi.com.br/download/funcaoodecompliance_09.pdf). Acesso em: 29 mar. 2022.

FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais: noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (org.). **A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters / Revista dos Tribunais, [2019a]. p. 23-52. ISBN 978-85-5321-663-5. Disponível em: [https://www.academia.edu/40040787/Compliance\\_de\\_dados\\_pessoais](https://www.academia.edu/40040787/Compliance_de_dados_pessoais). Acesso em: 15 maio 2021.

FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (org.). **A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters / Revista dos Tribunais, [2019b]. p. 99-129. ISBN 978-85-5321-663-5. Disponível em: [https://www.academia.edu/40040787/Compliance\\_de\\_dados\\_pessoais](https://www.academia.edu/40040787/Compliance_de_dados_pessoais). Acesso em: 15 maio 2021.

FRAZÃO, Ana. Programas de *compliance* e critérios de responsabilização de pessoas jurídicas por ilícitos administrativos. *In*: ROSSETTI, Maristela Abla; PITTA, Andre Grunspun. **Governança corporativa: avanços e retrocessos**. São Paulo: Quartier Latin, 2007. p. 42.

FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. *Compliance de dados pessoais*. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (org.). **A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters / Revista dos Tribunais, [2019]. p. 677-715. Cap. 10. ISBN 978-85-5321-663-5. Disponível em: [https://www.academia.edu/40040787/Compliance\\_de\\_dados\\_pessoais](https://www.academia.edu/40040787/Compliance_de_dados_pessoais). Acesso em: 15 maio 2021.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2009.

GIOVANINI, Wagner. **Compliance a excelência na prática**. São Paulo, 2014.

GOMES, Jose. É possível ter/estar em *compliance* e inovar. **Compliance e Inovação: Será?**, 10 abr. 2018. Disponível em: <https://medium.com/compliance-e-inova%C3%A7%C3%A3o-ser%C3%A1-%C3%A9-poss%C3%ADvel-ter-estar-em-compliance-e-inovar-77774ed559ed>. Acesso em: 12 mar. 2022.

GOMES, Luiz Flávio. Normas, regras e princípios: conceitos e distinções. **Revista Jus Navigandi**, Teresina, ano 10, n. 851, 1 nov. 2005. ISSN 1518-4862. Disponível em: <https://jus.com.br/artigos/7527>. Acesso em: 2 abr. 2022.

HIJAZ, Tailine Fátima. A importância do *compliance* para a efetivação de medidas anticorrupção no contexto da sociedade de risco e do Direito Penal Econômico. **Boletim Científico ESMPU**, Brasília, DF, ano 15, n. 48, p. 155-190, jul./dez. 2016. ISSN 1676-4781. Disponível em: <https://escola.mpu.mp.br/publicacoescientificas/index.php/boletim/article/view/479>. Acesso em: 15 mar. 2022.

IBGC – Instituto Brasileiro de Governança Corporativa. **Código das Melhores Práticas de Governança Corporativa**. 4. ed. São Paulo: IBGC, 2009.

IBM Corporation. **The end of the beginning**: unleashing the transformational power of GDPR. New York: Institute for Business Value, 2018. Disponível em: <https://www.ibm.com/downloads/cas/JEMXN6LV>. Acesso em: 11 maio 2021.

INPI. **Resolução INPI/PR nº 199, de 07 de julho de 2017**. Dispõe sobre as Diretrizes de exame para averbação ou registro de contratos de licença de direito de propriedade industrial e de registro de topografia de circuito integrado, transferência de tecnologia e franquia. Rio de Janeiro, 7 jul. 2017. 20 p. Disponível em: <https://www.gov.br/inpi/pt-br/servicos/contratos-de-tecnologia-e-de-franquia/arquivos/legislacao-contratos/Resoluo1992017DiretrizesCGTEC.pdf>. Acesso em: 1 mar. 2022.

MAEDA, Bruno Carneiro. Programas de *Compliance* anticorrupção: importância e elementos essenciais. In: DEBBIO, Alessandra Del; MAEDA, Bruno Carneiro; AYRES, Carlos Henrique da Silva (Coord.). **Temas de anticorrupção e Compliance**. Rio de Janeiro: Elsevier, 2013. p. 167-201. Disponível em: [https://edisciplinas.usp.br/pluginfile.php/4282048/mod\\_resource/content/0/TEMAS%20DE%20ANTICORRUP%C3%87%C3%83O%20E%20COMPLIANCE%20-%20P.%20149-201.pdf](https://edisciplinas.usp.br/pluginfile.php/4282048/mod_resource/content/0/TEMAS%20DE%20ANTICORRUP%C3%87%C3%83O%20E%20COMPLIANCE%20-%20P.%20149-201.pdf). Acesso em: 15 mar. 2022.

MANZI, Vanessa Alessi. **Compliance no Brasil**: consolidação e perspectivas. São Paulo: Saint Paul, 2008.

MENDES, Laura Schertel. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. In: SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (coord.). **Lei Geral de Proteção de Dados**. São Paulo: Revista dos Tribunais, 2019. p. 35-46. (Caderno Especial, nov. 2019).

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova lei de proteção de dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. **Revista de Direito do Consumidor**, Brasília, DF, v. 120, ano 27, p. 469-483, nov/dez, 2018.

Disponível em:

<https://revistadireitodoconsumidor.emnuvens.com.br/rdc/article/view/1116>. Acesso em: 15 mar. 2022.

MONTEIRO, Renato Leite *et al.* **Lei Geral de Proteção de Dados e GDPR: histórico, análise e impactos**. São Paulo: Baptista Luz Advogados, [2019]. 37 p. Disponível em: <https://baptistaluz.com.br/wp-content/uploads/2019/01/RD-DataProtection-ProvF.pdf>. Acesso em: 2 mar. 2022.

MORAIS, Eslei José de. **Controles internos e estrutura de decisão organizacional: o caso da Contadoria do Banco do Brasil**. Dissertação (Mestrado em Administração) – Universidade Federal do Paraná, Curitiba, 2005.

OCDE. **Manual de Oslo**: proposta de diretrizes para coleta e interpretação de dados sobre inovação tecnológica. Traduzido das edições originais em inglês e francês pelo FINEP. [Rio de Janeiro]: FINEP, 2004. Disponível em: [http://www.finep.gov.br/images/a-finep/biblioteca/manual\\_de\\_oslo.pdf](http://www.finep.gov.br/images/a-finep/biblioteca/manual_de_oslo.pdf). Acesso em: 1 jan. 2022.

OLIVA, Milena Donato; SILVA, Rodrigo da Guia. Notas sobre o *compliance* no direito brasileiro. **REVISTA QUAESTIO IURIS**, Rio de Janeiro, v. 11, n. 4, p. 2708-2729, dez. 2018. ISSN 1516-0351. DOI: <https://doi.org/10.12957/rqi.2018.33843>. Disponível em: <https://www.e-publicacoes.uerj.br/index.php/quaestioiuris/article/view/33843>. Acesso em: 05 abr. 2022.

PARLAMENTO EUROPEU. Directiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de Outubro de 1995. Relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. **Jornal Oficial das Comunidades Europeias**, n. L 281, p. 0031 – 0050, 23 nov. 1995. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT>. Acesso em: 1 mar. 2022.

PASQUALE, Frank. **The black box society: the secret algorithms that control money and information**. Cambridge: Harvard University Press, 2015.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais: comentários à lei N 13709/2018 (LGPD)**. 4. ed. São Paulo: Saraiva Jur, 2023.

RODOTÁ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008.

SAMPAIO, Joelson. A evolução do programa de *compliance* no Brasil. *In*: Colunas do Nefin. **Valor Investe**. [s.l.], 20 jun. 2019. Disponível em: <https://valorinveste.globo.com/blogs/nefin/coluna/a-evolucao-dos-programas-de-compliance-no-brasil.ghtml>. Acesso em: 15 jul. 2019.

SCHRAMM, Fernanda. *Compliance* e inovação: é preciso acelerar sem medo. *Comunicação Menezes Niebuhr*, 25 out. 2019. Disponível em:

<https://www.mnadvocacia.com.br/compliance-e-inovacao-e-preciso-acelerar-sem-medo/>. Acesso em: 1 mar. 2022.

SEBBEN, Naiara Anna. **O direito à proteção de dados pessoais e o mercado de crédito no Brasil**: análise à luz da lei nº 13.709/2018 (LGPD) e da lei complementar nº 166/2019. Orientadora: Suelen Carls. 2020. 144 f. Dissertação (Mestrado em Direito) - Universidade de Marília, Marília, SP, 2020. Disponível em: <https://portal.unimar.br/site/public/pdf/dissertacoes/595A37243A61B8D7FCAD52829C604839.pdf>. Acesso em: 1 mar. 2022.

SENAS, Alexandre. Abertura de Capital: o fundamental papel do *compliance* para a transparência de processos e a valorização da sua empresa no mercado de ações nacionais e internacionais. In: CONGRESSO DE COMPLIANCE, 3., 2013. **Anais** [...]. São Paulo: IBC Brasil, 2013. (pela Deloitte Touche Tohmatsu).

SOUZA, Carlos Affonso Pereira de; VIOLA, Mario; PADRÃO, Vinicius. Considerações iniciais sobre os interesses legítimos do controlador na lei geral de proteção de dados pessoais. **RDP**: Revista Direito Público, Porto Alegre, v. 16, n. 90, p. 109-131, nov./dez, 2019. ISSN: 2236-1766. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3744>. Acesso em: 1 mar. 2022.

SOUZA, Jane Dias Gomes de. A importância da função de *compliance* em instituições financeiras. 2013. 46 p. MBA (Especialização em Finanças) - Ibmecc Business School, Rio de Janeiro, 2013. Disponível em: <https://web.bndes.gov.br/bib/jspui/handle/1408/7025>. Acesso em: 15 mar. 2022.

SZTAJN, Rachel; SILVA, Reinaldo Marques da. “*Compliance*” e LGPD. **Campo Grande News**: conteúdo de verdade, Campo Grande – MS, 18 out. 2020. Disponível em: <https://www.campograndenews.com.br/artigos/compliance-e-lgpd>. Acesso em: 15 abr. 2022.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica.com**: revista eletrônica de direito civil, Rio de Janeiro, v. 9, n. 1, p. 1-38, 9 maio 2020. E-ISSN 2316-8374. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/510>. Acesso em: 5 mar. 2022.

TEIXEIRA, Ilderlandio. A LGPD como fonte de riqueza!. **JusBrasil**, [2020]. Disponível em: <https://ilderlandio.jusbrasil.com.br/artigos/783994130/a-lgpd-como-fonte-de-riqueza>. Acesso em: 11 mar. 2023.

THE INSTITUTE OF INTERNAL AUDITORS. **Declaração de Posicionamento do IIA**: as três linhas de defesa no gerenciamento eficaz de riscos e controles. [s.l.], Jan. 2013.

WAINER, Jacques. Métodos de pesquisa quantitativa e qualitativa para a ciência computação. In: KOWALTOWSKI, Tomasz; BREITMAN, Karin (org.). **Atualização em informática**. Porto Alegre: SBC, 2007. p. 221-262.

### APÊNDICE A – CANVAS

<i>Como?</i>		<i>O que?</i>	<i>Para quem?</i>	
<b>Parcerias Chave</b> <ul style="list-style-type: none"> <li>• Instituições Financeiras, em geral</li> <li>• Agências de Fomento e agentes financeiros</li> <li>• Governo Federal, como mantenedores dos Bancos Públicos</li> <li>• Governo Estadual, como mantenedores de agências de fomento</li> <li>• Bancos do setor privado</li> </ul>	<b>Atividades Chave (o que você faz)</b> <ul style="list-style-type: none"> <li>• Interação com a atividade bancária, como Procurador Jurídico de um Banco Público</li> </ul>	<b>Proposta de Valor</b> <ul style="list-style-type: none"> <li>• Apresentação de um Relatório Final de Pesquisa, após o término do estudo, na forma do art. 7º, § 3º, da Portaria 17/2009 do ME, a qual poderá ser utilizada como fonte de pesquisa e na formulação de novos instrumentos legais;</li> <li>• Depósito de um Código de Conduta ou de Boas Práticas aplicadas ao Setor Bancário, a partir das inovações e exigências da LGPD, estímulo trazido pela Lei, no artigo 50, e seguintes, o qual poderá ser adotado pelo Banco (transferência de tecnologia), ser utilizado como fonte de pesquisa ou mesmo na formulação de novos instrumentos legais;</li> </ul>	<b>Relacionamento</b> <ul style="list-style-type: none"> <li>• Assistência pessoal</li> <li>• Parcerias junto aos agentes financeiros;</li> <li>• Relacionamento junto ao Banco empregador</li> </ul>	<b>Segmento de Clientes</b> <ul style="list-style-type: none"> <li>• Instituições Financeiras, em geral</li> <li>• Agências de Fomento e agentes financeiros</li> <li>• Governo Federal, como mantenedores dos Bancos Públicos</li> <li>• Governo Estadual, como mantenedores de agências de fomento</li> <li>• Bancos do setor privado</li> </ul>
	<b>Recursos Chave (o que você tem)</b> <ul style="list-style-type: none"> <li>• Humanos – auxiliares</li> <li>• Físico – espaço necessário para a construção da pesquisa</li> <li>• Lei Federal 13.709/2018</li> <li>• Proposta de relatórios de pesquisa e códigos de conduta, como produto final</li> </ul>		<b>Canais</b> <ul style="list-style-type: none"> <li>• Páginas do governo</li> <li>• Correios</li> <li>• Internet</li> <li>• <i>In loco</i> na Unidade depositária</li> </ul>	
<b>Estrutura de Custo</b> <ul style="list-style-type: none"> <li>• Custo físico – Salários</li> </ul>		<b>Fontes de Receita</b> <ul style="list-style-type: none"> <li>• Fomento das próprias Instituições Financeiras, diante da necessidade urgente da implementação das alterações exigidas pela LGPD;</li> <li>• Fontes internas;</li> </ul>		
<i>Quanto?</i>				

**APÊNDICE B - MATRIZ SWOT / FOFA**

	<b>PONTOS POSITIVOS</b>	<b>PONTOS NEGATIVOS</b>
<b>Fatores</b> internos	<p><b>Forças (strengths)</b></p> <ul style="list-style-type: none"> <li>• <i>Procurador Jurídico de um Banco Público, facilitador da pesquisa e desenvolvimento da temática</i></li> <li>• <i>Rotina dentro da Instituição Financeira.</i></li> <li>• <i>Baixo custo</i></li> <li>• <i>Grande projeção do mercado financeira sobre os dados pessoais, e a sua valorização destes como prospecção para novos negócios</i></li> <li>• <i>Incentivo da LGPD às empresas que adotam Códigos de Conduta</i></li> <li>• <i>Implantação e adaptação de novo modelo que, ao final, evita multas milionárias e impede o acesso à base de dados</i></li> <li>• <i>Implantação de sistema de compliance, no mercado atual, agrega valor à empresa</i></li> </ul>	<p><b>Fraquezas (weaknesses)</b></p> <ul style="list-style-type: none"> <li>• <i>Mercado incipiente</i></li> <li>• <i>Burocracia na implementação</i></li> <li>• <i>Grande número de normas externas que influenciam na matéria</i></li> <li>• <i>Pouca cultura dos colaboradores para cumprimento de novas condutas</i></li> </ul>
	<p><b>Oportunidades (opportunities)</b></p> <ul style="list-style-type: none"> <li>• <i>Às Instituições Financeiras, adaptar seus programas de conformidade, a fim de cumprir as determinações da LGPD;</i></li> <li>• <i>Evitar multas milionárias e outras punições, como a vedação ao acesso à base de dados, o que impede a realização de novos negócios, prejuízo imensurável ao Banco;</i></li> <li>• <i>Ganho de valor de mercado da empresa, com o selo de cumprimento da LGPD, fator preponderante para conquista de novos negócios;</i></li> <li>• <i>Fator decisivo para acultramento dos colaboradores frente às novas dinâmicas da LGPD, e o recrudescimento da legislação frente ao uso dos dados pessoais</i></li> </ul>	<p><b>Ameaças (threatens)</b></p> <ul style="list-style-type: none"> <li>• <i>Instabilidade gerencial</i></li> <li>• <i>Falta de apoio da Alta Administração da organização, frente ao custo e burocracia na implementação</i></li> <li>• <i>Falta de tecnologia (TI) para implementação do sistema de controle dos novos processos (inovação em processo), os quais terão rotinas necessariamente alteradas para adaptação e controle no trafego dos dados pessoais</i></li> <li>• <i>Falta de mão-de-obra especializada para o funcionamento do setor de compliance e Tecnologia da Informação</i></li> </ul>
<b>Fatores</b> externos		

## APÊNDICE C – RELATÓRIO TÉCNICO CONCLUSIVO

Seguindo a estrutura de Relatório Técnico e/ou Científico (ABNT NBR 10719) adaptada para o modelo de livro, segue o relatório técnico conclusivo que apresenta os resultados e conclusões da pesquisa “O compliance como fator decisivo de controle nas empresas do setor bancário para a adaptação à lei geral da proteção de dados”.

CORDENONZI, Mauricio; PORTO JUNIOR, Francisco Gilson Rebouças. **O compliance como fator decisivo de controle nas empresas do setor bancário para a adaptação à Lei Geral da Proteção de Dados**: relatório técnico conclusivo. Palmas, TO: [S.n], 2023. 57 p. *E-book*. ISBN 978-65-00-66778-3.



# **O COMPLIANCE COMO FATOR DECISIVO DE CONTROLE NAS EMPRESAS DO SETOR BANCÁRIO PARA A ADAPTAÇÃO À LEI GERAL DA PROTEÇÃO DE DADOS**

relatório técnico conclusivo

*PRODUTO DA DISSERTAÇÃO DE MESTRADO DO PROFNIT/UFT*  
**MAURICIO CORDENONZI**  
**GILSON PORTO**

---

# Mauricio Cordenonzi

DISCENTE DO MESTRADO PROFISSIONAL DO PROGRAMA DE PÓSGRADUAÇÃO EM PROPRIEDADE INTELECTUAL E TRANSFERÊNCIA DE TECNOLOGIA PARA A INOVAÇÃO/UFT

# Dr. Prof. Gilson Porto Jr.

DOCENTE DO MESTRADO PROFISSIONAL DO PROGRAMA DE PÓSGRADUAÇÃO EM PROPRIEDADE INTELECTUAL E TRANSFERÊNCIA DE TECNOLOGIA PARA A INOVAÇÃO/UFT

## O COMPLIANCE COMO FATOR DECISIVO DE CONTROLE NAS EMPRESAS DO SETOR BANCÁRIO PARA A ADAPTAÇÃO À LEI GERAL DA PROTEÇÃO DE DADOS





Creative Commons "by-nc-sa" licenses

O conteúdo deste trabalho, exceto quando houver ressalva, é publicado sob a licença CC Atribuição 4.0

Capa e contracapa criadas no Canva



Dados da Catalogação *Anglo-American Cataloguing Rules – AACR2*

---

**C794c**

Cordenonzi, Mauricio

O *compliance* como fator decisivo de controle nas empresas do setor bancário para a adaptação à Lei Geral da Proteção de Dados: relatório técnico conclusivo [recurso eletrônico]. / Mauricio Cordenonzi, Francisco Gilson Rebouças Porto Junior. -- Palmas, TO: [S.n], 2023. 57 f.; il. Color.

E-book com dados eletrônicos (PDF), tamanho original 10,4 MB.  
Material como produto da Dissertação de Mestrado do PROFNIT/UFT.  
ISBN 978-65-00-66778-3

1. Direito – proteção de dados. 2. *Compliance*. 3. Bancos - Clientes. 4. LGPD. I. Porto Junior, Francisco Gilson Rebouças Porto Junior. II. Título.

CDD 332.1068  
CDU 347.734: 342.721(81)  
LCC KF6449.

---

Ficha Catalográfica elaborada por *Marcelo Neves Diniz* - CRB 2/1533.

[Resolução CFB nº 184, de 29 de setembro de 2017.](#)

TODOS OS DIREITOS RESERVADOS - A reprodução total ou parcial de qualquer forma ou por qualquer meio deste documento é autorizado desde que citada a fonte. A violação dos direitos do autor ([Lei nº 9.610/98](#)) é crime estabelecido pelo artigo 184 do Código Penal.

# RESUMO

A Lei Geral de Proteção de Dados – Lei Federal 13.709/2018, trouxe extensas e significativas mudanças aos atores responsáveis pela coleta e tratamento de dados pessoais, entre elas as Instituições Financeiras. Nesse contexto, o setor de *compliance* (responsável, dentro da empresa, pelo estrito cumprimento das normas, internas e externas), foi profundamente afetado pela novel legislação, na medida e que precisou, em um curto espaço de tempo, adaptar-se aos inúmeros comandos na norma. Este projeto discorre sobre um estudo de caso, realizado no Banco da Amazônia, com o propósito de, sob a análise do novo conjunto de normativas, propor um novo modelo de compliance, ou seu aperfeiçoamento, para adaptação à Lei Geral da Proteção de Dados – LGPD. O objetivo do estudo é propor critérios sobre as exigências legais trazidas pela LGPD às empresas do setor bancário, de modo a identificar e especificar os procedimentos e opções práticas de compliance à implementação do tratamento de dados na nova realidade e inviabilizar, tanto possível, a aplicação de multas. O público alvo e sujeitos envolvidos na pesquisa foram pessoas da área jurídica, servidores e empregados públicos, principalmente ligados à rede bancária, profissionais de TI e auditores, todos do setor bancário. A metodologia aplicada na pesquisa, além do estudo de caso, adota também procedimentos de cunho bibliográfico e documental partindo de um processo de revisão de literatura para compreender as exigências legais trazidas pela LGPD ao setor bancário, onde além de documentos oriundos do setor bancário, utilizados para análise de dados, adotou-se artigos, teses e dissertações encontrados em bases de dados científicas. Já quanto à abordagem de análise de dados, a pesquisa caracteriza-se como qualitativa, baseando-se na observação e compreensão dos ambientes em que os sistemas de compliance são utilizados para assim promover uma compreensão dos fenômenos da pesquisa. Como solução, propôs-se, para o aperfeiçoamento do atual modelo de *compliance*, a criação de uma nova Coordenação, para controle e gerenciamento de processos internos e externos, unicamente ligados ao tratamento de dados pessoais, a fim de otimizar tramitação e fluxo dos procedimentos, e mitigar, tanto quanto possível, os danos/multas decorrentes da norma. O estudo culminou na elaboração de um modelo de negócios CANVAS para o setor bancário, uma matriz SWOT, a produção de um relatório final onde foi possível apontar os gargalos existentes para propor um material didático para o modelo de compliance em forma de Manual de Aplicação da LGPD em Bancos.

Palavras-chave: compliance; LGPD; Banco da Amazonia; Tocantins (Estado).

# ABSTRACT

The General Data Protection Law - Federal Law 13.709/2018 brought extensive and significant changes to the actors responsible for collecting and processing personal data, including Financial Institutions. In this context, the compliance sector (responsible, within the company, for strict compliance with internal and external norms) was deeply affected by the novel legislation, as it needed to adapt to the numerous commands in the norm within a short period of time. This project discusses a case study, carried out at Banco da Amazônia, with the purpose of proposing a new compliance model, or its improvement, for adaptation to the General Data Protection Law - LGPD under the analysis of the new set of regulations. The objective of the study is to propose criteria on the legal requirements brought by the LGPD to companies in the banking sector, in order to identify and specify the practical compliance procedures and options for data processing implementation in the new reality and to prevent, as much as possible, the application of fines. The target audience and subjects involved in the research were people from the legal area, public servants and employees, mainly related to the banking network, IT professionals and auditors, all from the banking sector. The methodology applied in the research, in addition to the case study, also adopts bibliographic and documentary procedures starting from a literature review process to understand the legal requirements brought by the LGPD to the banking sector, where, in addition to documents from the banking sector, used for data analysis, articles, theses and dissertations found in scientific databases were adopted. As for the data analysis approach, the research is characterized as qualitative, based on the observation and understanding of the environments in which compliance systems are used to promote an understanding of the research phenomena. As a solution, the creation of a new Coordination was proposed for the improvement of the current compliance model, for the control and management of internal and external processes, solely related to the processing of personal data, in order to optimize the procedures' flow and mitigate, as much as possible, the damages/fines resulting from the norm. The study culminated in the development of a CANVAS business model for the banking sector, a SWOT matrix, the production of a final report where it was possible to identify existing bottlenecks to propose didactic material for the compliance model in the form of an LGPD Application Manual in Banks.

Keywords: compliance; LGPD; Banco da Amazonia; Tocantins (State)

# SUMÁRIO

1	INTRODUÇÃO .....	7
2	METODOLOGIA .....	9
2.1	Etapas da pesquisa .....	9
3	RESULTADOS .....	12
3.1	<i>Compliance</i> – Um resumo .....	12
3.2	O <i>Compliance</i> a Inovação e a LGPD. Fatores para o desenvolvimento do produto final. 18	
3.3	As exigências legais trazidas pela LGPD ao setor bancário .....	21
3.3.1	As bases legais. O consentimento. Artigo 7º, I, da LGPD .....	25
3.3.2	As bases legais. A execução de contrato. Artigo 7º, V, da LGPD .....	26
3.3.3	As bases legais. A proteção do crédito. Artigo 7º, X, da LGPD .....	27
3.3.4	As bases legais. Cumprimento de obrigação legal. Artigo 7º, II, da LGPD .....	27
3.3.5	O Legítimo Interesse utilizado na atividade bancária. Uma base legal <i>questionada</i> 28	
3.4	Os Procedimentos e as opções práticas de <i>compliance</i> disponíveis à implementação do tratamento de dados ao setor bancário. Os desafios. ....	29
3.5	O estudo de caso do Banco da Amazônia S.A. ....	32
3.5.1	O Banco da Amazônia e a LGPD .....	35
3.5.2	O <i>compliance</i> dentro do Banco da Amazônia e a estrutura organizacional da Instituição.....	37
3.5.3	Proposta de aprimoramento do modelo de <i>compliance</i> junto ao Banco da Amazônia para adaptação à LGPD .....	45
3.5.4	Criação de uma Coordenação independente para cumprimento e fiscalização da LGPD. Estrutura e organização.....	46
4	CONSIDERAÇÕES FINAIS.....	50
	REFERÊNCIAS .....	53

# 1 INTRODUÇÃO

A Lei 13.709, de 14 de agosto de 2018, conhecida como LGPD – Lei Geral de Proteção de Dados, *dispõe sobre o tratamento de dados pessoais, 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 e o livre desenvolvimento da personalidade da pessoa natural.*

A referida norma legal trouxe mudanças poderosas às empresas que detém, em seu patrimônio, dados pessoais de pessoas físicas e jurídicas, e que, de alguma forma, utilizam destes dados em seu cotidiano. Doravante, com o término do período de vacância da norma, estes conglomerados (e aí se ligam boa parte da indústria, comércio e até o setor público), passaram a ter responsabilidade direta no tratamento dos dados pessoais, com implicações significativas para eventuais lesões causadas à terceiros.

Neste novo cenário de mudanças, a alteração do sistema de *compliance* dos Bancos é altamente recomendável. Como é cediço, o **compliance** tem a função de proporcionar segurança e minimizar riscos de instituições e empresas, garantindo o cumprimento dos atos, regimentos, normas e leis estabelecidos interna e externamente.

O conceito de *compliance*, na definição utilizada pelo Banco da Amazônia, na POL 309 – Política de Compliance, logo no preâmbulo, define:

## **1 INTRODUÇÃO**

*A atividade de Compliance busca aperfeiçoar resultados e mitigar os riscos de conformidade, implementando através de mecanismos de controle e conformidade às Normas, Leis, Regulamentos, bem como as políticas e diretrizes internas da empresa. Esta política estabelece conceitos e aplicações de forma preventiva, detectando e orientando, garantindo assim de forma efetiva a melhoria contínua dos padrões de atuação, com ética, transparência e eficiência na operacionalização das atividades no contexto das três linhas.*

## **2 OBJETIVO**

*Esta Política tem o objetivo de estabelecer diretrizes e procedimentos a serem seguidos por todos os colaboradores, dirigentes e conselheiros e prestadores de serviços terceirizados relevantes do Banco da Amazônia, quanto às regras de Compliance, zelando pelo cumprimento de leis, regulamentações, políticas, normas internas e externas, procedimentos e princípios corporativos que regem a atividade da empresa.*

A atividade de conformidade, cuja existência é obrigatória dentro de uma Instituição Financeira (desde a edição da Resolução BACEN 2554/1998), atua de

forma preventiva, e pró ativa, no sentido de certificar o cumprimento das normas internas e externas, e, com isso, evitar ou mitigar a possibilidade de infrações que possam causar danos financeiros ou reputacionais à empresa.

Nesse contexto, e agora voltado para o cerne do trabalho, dentro das Instituições Financeiras, é essencial que a área de *compliance* esteja organizada para adaptar-se às novas exigências da LGPD, seus requisitos e, principalmente, as implicações em vergar as regras estabelecidas, diante das multas, que podem alcançar cifras milionárias, além da suspensão do direito de acessar as bases de dados

Então, o objetivo deste relatório técnico é apresentar um estudo da LGPD sob o aspecto das Instituições Financeiras, no caso o Banco da Amazônia S.A., através de um estudo de caso. A pesquisa adota procedimentos de cunho bibliográfico e documental partindo de um processo de revisão de literatura para compreender as exigências legais trazidas pela LGPD ao setor bancário, onde, além de documentos oriundos da atividade bancária, adotou-se artigos, teses e dissertações encontrados em bases de dados científicas. A pesquisa tem natureza qualitativa, na medida em que baseia-se na observação e compreensão dos ambientes em que os sistemas de *compliance* são utilizados para, a partir daí, oferecer um modelo aperfeiçoado de *compliance* que possibilite a adequação dos Bancos às novas exigências da norma.

Como resultado final, portanto propôs-se o aperfeiçoamento do atual modelo de *compliance*, com a criação de uma nova Coordenação, para controle e gerenciamento de processos internos e externos, unicamente ligados ao tratamento de dados pessoais, a fim de otimizar tramitação e fluxo dos procedimentos, e mitigar, tanto quanto possível, os danos/multas decorrentes da norma.

## 2 METODOLOGIA

A metodologia pode ser compreendida por um conjunto de métodos e procedimentos utilizados para a realização de algo.

A pesquisa buscou resolver um problema do setor financeiro em face da introdução de um novo arcabouço legal e, dessa forma, caracteriza-se como uma pesquisa aplicada. Em relação aos objetivos, não se pretendeu explicar ou descrever um fenômeno, mas sim "proporcionar uma maior familiaridade com o problema, com vista a torná-lo mais explícito ou a constituir hipóteses" (GIL, 2009, p. 41) e, dessa forma, a pesquisa classificou-se como exploratória.

Em relação aos procedimentos adotados, caracterizou-se como bibliográfica e documental pois partiu-se de um processo de revisão de literatura para compreender as exigências legais trazidas pela LGPD ao setor bancário. Tal revisão ocorreu tanto em artigos científicos como em outros documentos como leis, normas e regulamentos relativos ao compliance.

Ainda, quanto aos procedimentos, caracterizou-se como estudo de caso pois visou retratar exhaustivamente os aspectos relativos à conformidade em uma instituição financeira, no caso o Banco da Amazônia S.A., e apresentar, ao final, uma nova ou aprimorada solução ao modelo de *compliance* hoje existente. Este aperfeiçoamento é materializado através da criação de um novo órgão, junto à Diretoria de Riscos do Banco da Amazônia, e que poderá ser desenvolvida em qualquer Instituição Financeira, exclusivamente responsável pela gestão de *compliance* ligada à Lei Geral de Proteção de Dados.

Por fim, quanto à abordagem de análise de dados, a pesquisa caracterizou-se como qualitativa pois baseou-se na observação e compreensão dos ambientes em que os sistemas de compliance são utilizados com a intenção de promover uma compreensão do fenômeno em sua totalidade (GIL, 2009; WAINER, 2017).

### 2.1 Etapas da pesquisa

A pesquisa para o desenvolvimento do estudo de caso ocorreu entre os meses de julho de 2021 a dezembro de 2022, e foi aplicada em uma Instituição Financeira, em

3 grandes fases: Revisão jurídica e bibliográfica, Coleta de dados na instituição financeira participante e Análise comparativa e proposição de solução.

Na primeira fase, foi realizada uma revisão de literatura para examinar tanto as exigências legais quanto as iniciativas presentes nos estudos científicos já realizados no sentido de aplicar no novo regramento da LGPD na prática. Para a revisão de estudos, foi realizado um mapeamento das referências em periódicos científicos responsáveis pela difusão de resultados de pesquisas e o registro dos avanços da produção acadêmica nas áreas de interesse do presente estudo. Tal revisão bibliográfica ocorreu em 4 (quatro) etapas, a saber: a) identificação e ajustes nas palavras-chave, b) coleta dos dados, c) leitura dos títulos e resumos para identificar os estudos mais relevantes, d) leitura integral e fichamento dos estudos.

Foram coletados artigos científicos publicados entre os anos de 2010 e 2021 nas coleções indexadas no portal de periódicos da Capes. Os estudos coletados forneceram subsídios para a resposta à pergunta da pesquisa. Dessa forma, para garantir uma recuperação ampla de artigos considerou-se as palavras-chaves mais significativas dentro do problema focalizado e seus termos correlatos em português e inglês, a saber: LGPD - "Lei geral de proteção de dados", Dados pessoais sensíveis, Compliance, Instituição Financeira. Após a etapa de ajuste a *string* de busca, foi aplicada na base de dados escolhida e os estudos recolhidos foram organizados em uma tabela para apoiar o processo de identificação dos estudos mais relevantes. Tal tabela foi formada pelos campos: autores, ano, título do estudo, resumo, decisão de inclusão e justificativa. Por fim, após a identificação dos estudos mais relevantes, procedeu-se a leitura e fichamento integral dos mesmos.

Após a revisão de literatura, a pesquisa voltou-se a compreender como a instituição financeira escolhida para análise realiza seu sistema de compliance. Nessa etapa foram realizadas a análise documental dos regimentos, regulamentos e demais documentos que normatizam os procedimentos dentro da instituição.

Por fim, foi realizada uma análise comparativa entre os regimentos e soluções apresentados na revisão bibliográfica e os dados coletados na instituição financeira e, com base nessa análise, foi apresentada uma solução/aprimoramento ao sistema de compliance, ajustado ao novo arcabouço legal.

O trabalho final é apresentado neste relatório técnico conclusivo. A área de conformidade é extremamente sensível dentro da Instituição Financeira, e tem a

responsabilidade em detectar possíveis gargalos existentes dentro da organização, saná-los e evitar ou minimizar prejuízos advindos. Nesse contexto, era presumível que o agente financeiro escolhido como base para o trabalho não autorizasse a reprodução de seu sistema de *compliance*, tampouco eventuais inconformidades existentes, o que limitou a extensão da pesquisa.

Desta forma, o relatório técnico teve a pretensão de apontar, de uma forma sistêmica, as exigências de um novo modelo de *compliance* frente às obrigações trazidas pela LGPD, de uma maneira geral.

### 3 RESULTADOS

#### 3.1 *Compliance* – Um resumo

A expressão *compliance* tem origem do verbo *to comply*, que, traduzido ao português, significa atuar de acordo com uma norma, uma lei, uma regra, uma ordem ou um pedido. No mundo empresarial e institucional, e no meio corporativo, *compliance* pode ser entendido como conjunto de ações que visam ao cumprimento das normas legais e regulamentares, das políticas e diretrizes do negócio e das atividades da instituição ou empresa, visando-se, sobretudo, a evitar, detectar e solucionar quaisquer desvios ou inconformidades que venham a acontecer (FEBRABAN, 2009; MORAIS, 2005; SZTAJN; SILVA, 2020).

“Estar em *compliance*” traduz, em suma, o dever de achar-se em conformidade e de fazer cumprir leis, regulamentos e diretrizes, em geral, “com o objetivo de mitigar o risco atrelado à reputação e o risco legal/regulatório” (COIMBRA; MANZI, 2010, p. 2).

De acordo com Manzi (2008), o *compliance* teve origem nas instituições financeiras, com a criação do Banco Central Americano (Board of Governors of the Federal Reserve), em 1913. Logo após a quebra da Bolsa de Nova York de 1929, foi criada a política intervencionista *New Deal*, em uma tentativa de intervir na economia para “corrigir as distorções naturais do capitalismo”<sup>28</sup>.

Com efeito, muito embora tenha origem no setor bancário, onde obteve progresso exponencial, é certo que o *compliance* é um modelo de gestão que se expandiu para muito além das fronteiras das Instituições Financeiras. Atualmente, existem inúmeros modelos e formatos de *compliance*, a depender da atividade desenvolvida, seja ligado a área empresarial, trabalhista, tributária, bancária, ambiental etc.

Com efeito, muito embora tenha origem no setor bancário, onde obteve progresso exponencial, é certo que o *compliance* é um modelo de gestão que se expandiu para muito além das fronteiras das Instituições Financeiras. Atualmente,

---

<sup>28</sup> A importância do *compliance* para a efetivação de medidas anticorrupção no contexto da sociedade de risco e do Direito Penal Econômico Tailine Fátima Hijaz Analista do Ministério Público da União (apoio jurídico/Direito). Pós-graduada pela Fundação Escola do Ministério Público do Paraná e pela Academia Brasileira de Direito Constitucional. Graduada em Direito pela Universidade do Extremo Sul Catarinense

existem inúmeros modelos e formatos de *compliance*, a depender da atividade desenvolvida, seja ligado a área empresarial, trabalhista, tributária, bancária, ambiental etc.

As Instituições Financeiras, notadamente após as deliberações do CMN – Conselho Monetário Nacional (a partir de 1994), e depois do Primeiro Acordo de Basiléia, de 1988, passaram a adotar procedimentos de controle rígidos a fim de minimizar impactos financeiros decorrentes de riscos operacionais. Já, neste período, entendia-se os riscos aplicados ao manuseio dos dados pessoais. Todavia, nos últimos anos, escândalos têm marcado a vida de grandes bancos, no Brasil e no exterior, com sérias consequências para as organizações, seus empregados e principalmente os clientes.

O caso envolvendo a Enron e a Lehman Brothers, que ocorreram no final do século XX e início do XXI, deixaram marcas profundas na credibilidade das Instituições Financeiras, tanto nos investidores quanto na sociedade em geral. No Brasil, pode-se citar os episódios do Banco Nacional, o qual desaguou em prejuízos superiores a US\$ 9 bilhões<sup>29</sup>, do Banco Marka, do Banestado e, por último, do Banco Rural, citado no caso do mensalão.

Escândalos atacam diretamente a reputação da empresa e, assim, o seu valor de mercado. E a reputação, como outrora exposto, é a linha frontal de defesa do *compliance*, com vista a minimizar diretamente o risco de descontinuidade dos negócios através da implantação de sistemas e métodos de controles que visam à observação das normas referentes ao mercado em que atuam e aos procedimentos internos (SOUZA, 2013).

Assim, tanto o mercado regulatório, quanto os órgãos de controle estatais entenderam a necessidade de implementação de instrumentos de governança e conformidade nas Instituições Financeiras, como órgãos obrigatórios, a fim de dinamizar os riscos ao setor, e minimizar os prejuízos, como nas fraudes outrora verificadas.

No ano de 1998, surge, então, a Resolução BACEN 2554/1998, cujo artigo primeiro, chancelou:

---

<sup>29</sup> Cf. ENTENDA o caso do Banco Nacional. In: FOLHA DE SÃO PAULO, São Paulo, domingo, 1 out. 2000. Brasil. Disponível em: <https://www1.folha.uol.com.br/fsp/brasil/fc0110200003.htm>. Acesso em: 15 mar. 2022.

Art. 1º **Determinar às instituições financeiras** e demais instituições autorizadas a funcionar pelo Banco Central do Brasil **a implantação e a implementação de controles internos** voltados para as atividades por elas desenvolvidas, seus sistemas de informações financeiras, operacionais e gerenciais e o cumprimento das normas legais e regulamentares a elas aplicáveis.

§ 1º Os controles internos, independentemente do porte da instituição, devem ser efetivos e consistentes com a natureza, complexidade e risco das operações por ela realizadas. (GN) (BANCO CENTRAL DO BRASIL, 1998, p. 1, grifo nosso).

Estava, na ocasião, definitivamente criado o sistema obrigatório de conformidade aos bancos, por expressa determinação do Banco Central do Brasil. Paradoxalmente, os sistemas de controle se expandiram a outros segmentos das organizações, como já retratado neste trabalho, como, a exemplo, a Lei Anticorrupção.

A Lei Federal nº 13.303/2016, conhecida como a Lei das Estatais, por seu turno, estabelece a obrigação dos estatutos das empresas públicas, economias mistas (**Banco do Brasil S.A., Banco da Amazônia S.A., Banco do Nordeste S.A. etc**) e suas respectivas subsidiárias, *observar regras de governança corporativa, de transparência e de estruturas, práticas de gestão de riscos e de controle interno*, como destacado em seu artigo 6º. Já o artigo 9º é categórico:

Art. 9º A empresa pública e a sociedade de economia mista adotarão regras de estruturas e práticas de gestão de riscos e controle interno que abranjam:  
I - ação dos administradores e empregados, por meio da implementação cotidiana de práticas de controle interno;

II - área responsável pela verificação de cumprimento de obrigações e de gestão de riscos;

III - auditoria interna e Comitê de Auditoria Estatutário.

§ 1º Deverá ser elaborado e divulgado Código de Conduta e Integridade, que disponha sobre:

I - princípios, valores e missão da empresa pública e da sociedade de economia mista, bem como orientações sobre a prevenção de conflito de interesses e vedação de atos de corrupção e fraude;

II - instâncias internas responsáveis pela atualização e aplicação do Código de Conduta e Integridade;

III - canal de denúncias que possibilite o recebimento de denúncias internas e externas relativas ao descumprimento do Código de Conduta e Integridade e das demais normas internas de ética e obrigacionais;

IV - mecanismos de proteção que impeçam qualquer espécie de retaliação a pessoa que utilize o canal de denúncias;

V - sanções aplicáveis em caso de violação às regras do Código de Conduta e Integridade;

VI - previsão de treinamento periódico, no mínimo anual, sobre Código de Conduta e Integridade, a empregados e administradores, e sobre a política de gestão de riscos, a administradores. (GN) (BRASIL, 1998, p. 2).

Aos Bancos Públicos, portanto, a implantação de órgãos de controle interno, e Códigos de Conduta e Integridade, é compulsória, diante da Lei das Estatais.

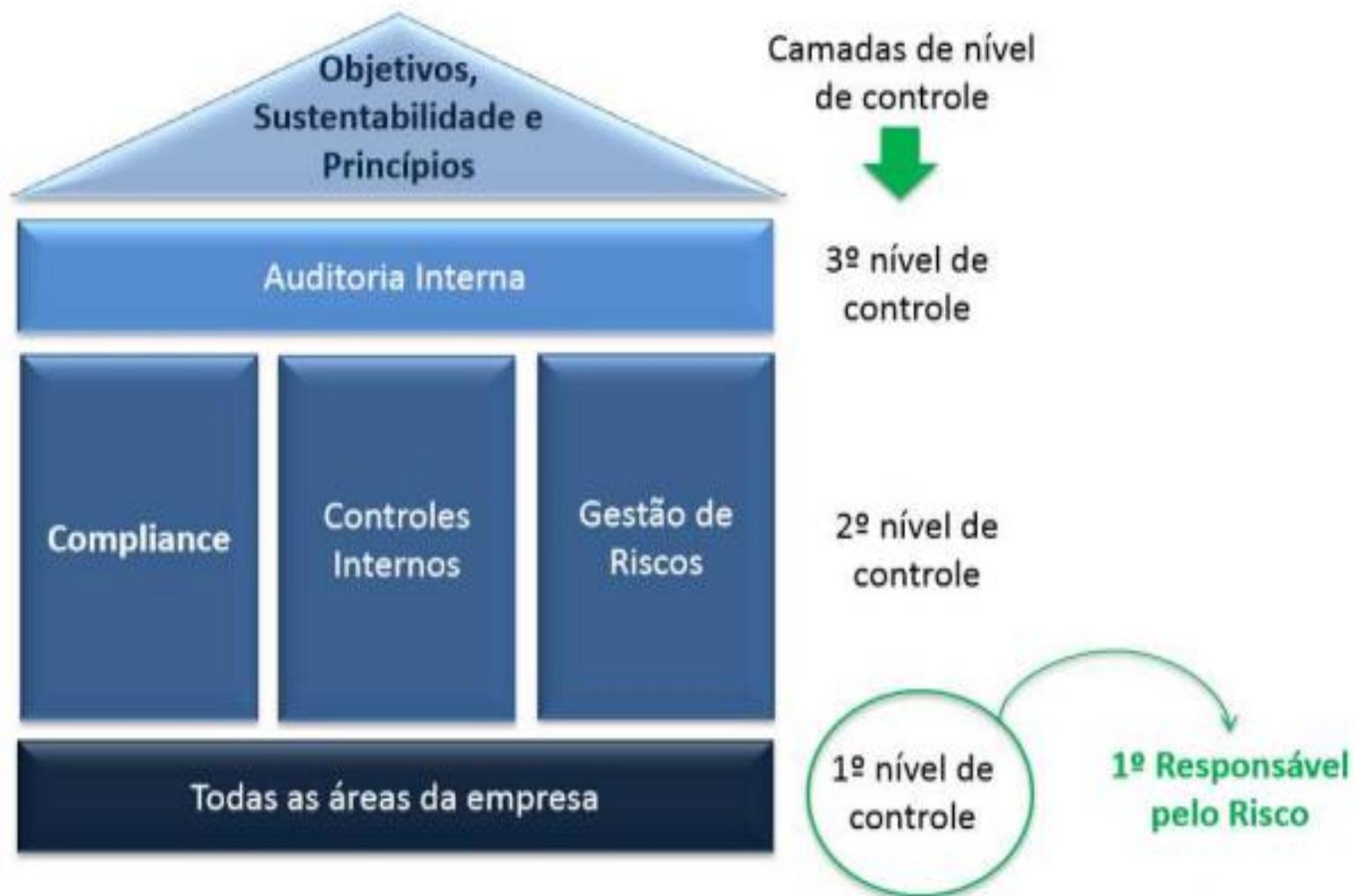
Ainda na fase embrionária, muitas organizações iniciaram a implantação de um modelo de *compliance* ligado às assessorias jurídicas, ante a ligação com atos normativos, regulamentos e as consequentes fiscalizações. Doravante, viu-se que, em verdade, tratava-se de um nítido modelo de gestão, a qual deveria estar inclusa nos processos.

O gestor do *compliance*, muito além de editar normas e procedimentos, tem inúmeras outras atribuições, principalmente exigindo e cobrando responsabilidades aos gestores das diversas outras áreas da empresa.

Segundo Coimbra; Manzi (2010 *apud* SOUZA, 2013, p. 18):

[...] as responsabilidades do *compliance* são: assegurar, em conjunto com as demais áreas, a adequação, o fortalecimento e o funcionamento do sistema de controles internos, procurando mitigar riscos de acordo com a complexidade de seus negócios, bem como disseminar a cultura de controles para assegurar o cumprimento das leis e regulamentos existentes. Além disso, verifica e monitora as alterações no ambiente regulatório, tais como normas do órgão regulador, autorregulação, entre outras, bem como as alterações produzidas por novos produtos lançados, e informa às áreas envolvidas as alterações nas estruturas de controles internos.

Figura 1 - O *Compliance* como Pilar da Governança em Mercados Regulados



Fonte: (ALVES, 2013).

**Figura 2 - Tendências, Perspectivas e desafios de *Compliance***



Fonte: (SENAS, 2013).

Como se vê, portanto, a conformidade tem ligação estreita com todos os demais atores dentro da Instituição, até em razão do controle e fiscalização exercidos, mesmo que em diferentes níveis. E, a verticalidade da atuação do *compliance* irá depender do quão longe quer chegar a empresa (do Banco, no caso), diante do cenário e objetivos delineados e frente a gestão e análise dos riscos do mercado.

### **3.2 O *Compliance* a Inovação e a LGPD. Fatores para o desenvolvimento do produto final.**

Segundo o Manual de Oslo, inovação é a introdução de um bem ou serviço novo ou significativamente melhorado, no que se refere às suas características ou usos previstos, ou ainda, à implementação de métodos ou processos de produção, distribuição, marketing ou organizacionais novos ou significativamente melhorados (OCDE, 2004).

Inovar, oportunizar o crescimento da empresa, mas de forma organizada, sustentável e em conformidade. Este é o desafio das organizações, hodiernamente, e aqui o *compliance* e a inovação se entrelaçam. Para Doyle (*et al*, 2019), a sustentabilidade é abordada no contexto amplamente definido, ou seja, baseia-se na capacidade de uma organização equilibrar as necessidades de curto e longo prazo das partes interessadas.

Como já registrado em linhas pretéritas, o *compliance*, no Brasil, ainda é embrionário. Iniciou-se, timidamente, nos anos 1990, com modelos estrangeiros. E, ao certo, para tomar fôlego e gerar resultados, depende de um processo crucial de aculturação tanto das empresas quanto dos empregados nos tempos atuais. (SAMPAIO, 2019).

No cenário legal, normativo, a conformidade ganhou força com a edição da Lei Federal 12.846/2013, a qual dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, a chamada Lei anticorrupção. Referida norma trata da responsabilização administrativa e civil de pessoas jurídicas (empresas) pela prática de atos de corrupção contra a administração pública, nacional ou estrangeira, e atende ao pacto internacional firmado pelo Brasil. O objetivo é coibir a atuação de

empresas em esquemas de corrupção e assim, evitar que grandes prejuízos sejam causados aos cofres públicos.

A lei em gênese prestigiou e incentivou as empresas a aplicarem mecanismos de conformidade em suas estruturas, eis que, caso existentes, tal particularidade será considerada em caso de aplicação de penalidade, conforme teor do artigo 7º:

Art. 7º Serão levados em consideração na aplicação das sanções:

[...]

VIII - a existência de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e a aplicação efetiva de códigos de ética e de conduta no âmbito da pessoa jurídica; (GN) (BRASIL, 2013, p. 2).

Crescer, inovar, mas com responsabilidade e em *conformidade*: esta é a pedra nevrálgica do sistema atual. Por isso, o *compliance* e toda sua rede é o assunto dominante, atualmente, no mundo corporativo. A gestão e o cumprimento das normas devem estar alinhados aos objetivos finalísticos da organização, e não ser enxergado, dentro e fora da empresa, como um fator inibidor da inovação ou até mesmo bloqueador no âmbito comercial em detrimentos do grau de cumprimento e exigências legais e normativas (GIOVANINI, 2014).

Nesse contexto, como destacado, inovação e conformidade se entrelaçam. É propiciar o crescimento, com responsabilidade e dentro das normas, com sustentabilidade:

[...] um complexo ecossistema tecnológico demanda contínua inovação em conformidade um amplo regramento, que envolve, entre outras coisas, investimento em segurança e privacidade de dados. **Ao contrário do pensamento tradicional industrial, *compliance* hoje pode ser uma área extremamente inovadora e flexível em qualquer negócio, sem intenção de frear, impor ou dificultar processos, muito pelo contrário, é o olhar que corre juntamente com a inovação para garantir a sustentabilidade do que conquistamos até aqui e a segurança das coisas incríveis que ainda lançaremos** (GOMES, 2018, grifo nosso).

Com efeito, a cultura da conformidade no mundo das grandes corporações, no Brasil, ainda é incipiente. Nas Instituições Financeiras, dado ao regramento específico do BACEN, através de atos normativos próprios, o surgimento foi acelerado, todavia, no meio empresarial, a aplicação ainda cede diante da *pseudo* crença dos elevados custos.

A Lei Anticorrupção, como exposto, foi um importante marco legal, para a natureza obrigatória do *compliance*, e, agora, a Lei 13.709/2018 – a Lei Geral de Proteção de Dados, veio como um importante incentivo ao mercado para, definitivamente, a conformidade entrar na estrutura das organizações, como esteio ao seu funcionamento e propagador de resultados.

Todas as empresas, indistintamente, públicas ou privadas, passam a ter responsabilidade sob a governança das informações que detém, sobre os dados pessoais que guardam, e eventual vazamento, ou a espoliação destes, é punida com severidade. O objetivo da LGPD foi de proteger o cidadão contra o chamado uso disfuncional de seus dados, e lhes garante o poder de fiscalizar e controlar suas informações. A nova lei exige, outrossim, a autorização do proprietário para a divulgação e disponibilização de seus dados, de forma expressa, consciente e inequívoca, o que exige um rígido, independente, adequado e estruturado setor, dentro da empresa.

Com efeito, a partir da vigência da lei, todo o sistema normativo interno da empresa, caso existente, deve, necessariamente, ser reestruturado. Novos códigos de conduta, as rotinas dos processos internos e tráfego dos dados, devem ser revistos e atualizados, de acordo com o tratamento dos dados exigidos pela norma. O compartilhamento e a eventual divulgação dos dados, agora, exige o máximo controle.

Comentam Ana Frazão, Milena Oliva e Vivianne Abilio:

Nesse cenário em que, por um lado, vislumbram-se profundas alterações na lógica até então vigente quanto ao tratamento de dados e, por outro, objetiva-se conferir papel primordial na efetividade dos direitos e na prevenção de danos, a adoção de mecanismos de *compliance* consubstancia valioso instrumento desse viés operacional e preventivo, auxiliando na promoção de condutas compatíveis com a regulamentação legal. (FRAZÃO; OLIVA; ABILIO, [2019], p. 682).

Nas Instituições Financeiras, o setor de cadastro é o responsável por arrecadar e armazenar todos os documentos do cliente. E, a partir de então, da análise destes, é que os negócios jurídicos são impulsionados. Daí a importância de se estabelecer um rigoroso aprimoramento na rotina do tratamento dos dados pessoais, posto que, a má gestão deste setor, poderá desaguar em um descumprimento legal em cascata, e consequências imprevisíveis à empresa.

A implantação de um rígido modelo de *compliance*, para tratar estes dados, e dar conformidade às normas editadas pela Lei 13.709/2018, é medida que se impõe, notadamente às Instituições Financeiras.

### 3.3 As exigências legais trazidas pela LGPD ao setor bancário

O contexto e a dinâmica do trabalho, aqui apresentado, são voltados ao setor bancário. A LGPD, todavia, não excepciona este segmento, ou o mercado financeiro, de maneira especial, o que lança as Instituições Financeiras na vala comum daquelas organizações que devem seguir os padrões de regulação geral da norma.

A Lei Geral de Proteção de Dados foi criada, em suma, para reger a *coleta, o tratamento, o armazenamento e o compartilhamento* dos dados pessoais. Este é o sentido e o objetivo da norma. E o trabalho, aqui desenvolvido, é apontar quais as exigências reclamadas pela lei às Instituições Financeiras e, ao final, como o *compliance* pode auxiliar, como governança, a dar o efetivo cumprimento aos rigores da norma.

Para o bom entendimento quanto às exigências da lei, convém esclarecer o que são *dados*, na concepção legal. O conceito de dados, e suas diferenças, são estabelecidos pelo artigo 5º, da Lei 13.709/2018:

Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; (BRASIL, 2018, p. 60).

A lei criou três espécie de dados, e a sua diferenciação é vital para dar aplicabilidade prática à norma. De antemão, percebe-se que os dados bancários não são classificados como dados *sensíveis* (art. 5º, II), o que lhes retira de uma forma diferenciada de tratamento. Isso por que, os dados pessoais sensíveis mereceram, por parte do legislador, uma forma particular de gerenciamento, em especial e como

requisito preponderante o consentimento do proprietário. Nenhum controlador<sup>30</sup> pode legalmente tratar um dado sensível sem o consentimento do titular, salvo as exceções legais trazidas no art. 11, II, da LGPD.

Em que pese alguma divergência, é assente na doutrina não estarem os dados bancários inseridos entre os dados pessoais sensíveis. Primeiro por que o rol descrito no artigo 5º, II, da Lei apresenta um *rol taxativo*, e, diante do recrudescimento da norma, com relação a estes, as obrigações não podem ser estendidas, sem prévia definição legal, tudo em homenagem ao princípio da legalidade e na boa prática da hermenêutica jurídica (normas restritivas de direitos devem, em princípio, sofrerem interpretação restritiva).

Com efeito, ao fim e ao cabo, as Instituições Financeiras tratam dos dados pessoais, assim definidos aqueles insertos no artigo 5º, I, da LGPD.

Sob tal prisma legal, surge, então, no plano prático, a primeira grande exigência às Instituições Financeiras, que é a busca pela **base legal** específica, para o tratamento e gerenciamento dos dados pessoais. As bases legais são as hipóteses legais que autorizam alguém (no caso o controlador) a realizar o tratamento do dado. A lei, no caso, criou condições determinadas para que seja possível fazer a coleta e o tratamento dos dados pessoais.

Na doutrina de Laura Schertel Mendes:

Para que um tratamento de dados pessoais seja considerado legítimo, é preciso que sejam atendidas as seguintes condições:

i) o tratamento de dados deve se amparar em uma das bases legais previstas no art. 7º ou no art. 23 da LGPD; e

ii) o tratamento de dados deve levar em conta os princípios previstos no art. 6º da LGPD, entre eles, a boa-fé objetiva, a finalidade e a necessidade. Pressuposto fundamental da lei é de que o tratamento de dados só poderá ser realizado se houver base legal que o autorize. Assim, os tratamentos de dados pessoais somente serão legítimos quando se enquadrem em ao menos uma das hipóteses previstas no art. 7º ou no art. 23 da LGPD, totalizando 11 hipóteses autorizativas para o tratamento de dados pessoais. (MENDES, 2019, p. 47).

Importante registrar, também, que as únicas hipóteses de exclusão (inexistência de base legal) estão previstas no art. 4º, da Lei. E, ainda, no caso das exceções do inciso III (para fins exclusivos de segurança pública; defesa nacional;

---

<sup>30</sup> Cf. Art. 5º da lei 13.709/2018. (Para os fins desta Lei, considera-se: [...] VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais).

segurança do Estado; ou atividades de investigação e repressão de infrações penais), há a previsão de lei específica para sua regulamentação, dada a importância da matéria.

E, assim, as bases legais (condições) estão estabelecidas no artigo 7º da norma:

### **Seção I**

#### **Dos Requisitos para o Tratamento de Dados Pessoais**

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 terceiro;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ([Redação dada pela Lei nº 13.853, de 2019](#)) [Vigência](#)

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, 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.** (GN) (BRASIL, 2018, p 60, grifo nosso).

**Tabela 2 -Bases Legais da LGPD**

<b>HIPÓTESES DE TRATAMENTO DE DADOS</b>	<b>DEFINIÇÃO</b>	<b>BASE LEGAL</b>
Consentimento do titular	Consentimento para tratamento dos dados pessoais deverá ser livre e inequívoco	art 7, I, LGPD
Cumprimento de obrigação legal ou regulatória	Pode ocorrer por força de lei anterior ou para garantir a ordem e segurança social	art 7, II, LGPD
Uso compartilhado de dados pela administração pública	Feito com a finalidade específica da execução de política pública formalmente instituída por Lei ou Ato administrativo.	art 7, III, LGPD
Realização de estudos e pesquisas	Tratamento para pesquisas ou estudos para saúde pública ou programas de governo	art 7, IV, LGPD
Execução ou preparação de contrato	Fazer parte de contrato consentimento específico do titular para utilização de negócio jurídico em que seja parte	art 7, V, LGPD
Exercício de direitos em processos judicial, administrativo ou arbitral	Feito com a finalidade específica de lei anterior ou para garantir a ordem e segurança social	art 7, VI, LGPD
Proteção da vida ou da incolumidade física	Tratamento de dados em favor do titular do dado em casos de necessidade de tutela do bem maior da pessoa natural	Art. 7, VII, LGPD
Tutela da saúde do titular	Única hipótese de tratamento de dado manejado por agente exclusivo profissional de saúde, serviços de saúde ou autoridade sanitária	Art. 7, VIII, LGPD
Legítimo interesse	Previsão geral e subsidiária mediante previa e expressa motivação pelo controlador da finalidade e necessidade (legítimo interesse) do tratamento	Art 7. IX, LGPD
Proteção do crédito	Tratamento para proteção e manutenção do crédito	Art. 7. X, LGPD

Fonte: (10 BASES..., 2020).

Para o trabalho aqui retratado, serão olvidados os casos de tratamento previstos nos artigos 11 (tratamento de dados sensíveis) e 23 (tratamento de dados pessoais pelas pessoas jurídicas de direito público).

Tratando-se de Instituições Financeiras, há que se ter em mira a existência de um contrato jurídico preexistente, ou a ser firmado, entre o cliente/consumidor e a Instituição Financeira. A isso se aplica tanto aos contratos em andamento quanto aqueles a serem assinados, já no decorrer da vigência da Lei Geral de Proteção de Dados. O contrato bancário, conceitualmente, e de forma reduzida, é aquele que tem por objetivo a intermediação do crédito.

Nesse sentido, para que o agente financeiro analise, de forma ampla e irrestrita, a viabilidade de concessão do crédito/financiamento ao cliente, há, em regra, *cláusulas contratuais* onde o cliente aporta e oferece ao banco toda a sua documentação pessoal (documentos pessoais em geral), além de sua documentação

financeira (declarações de renda, patrimônio etc). E, para além disso, autoriza a Instituição Financeira a realizar uma ampla investigação, em todos os níveis possíveis, sobre sua vida pregressa.

Neste ponto, a base legal dos agentes financeiros surge em três níveis, a depender do caso concreto, conforme a previsão do art. 7º, da Lei 13.709/2018:

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - **mediante o fornecimento de consentimento pelo titular;**

[...]

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;**

[...]

X - **para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.** (GN) (BRASIL, 2018, p 60, grifo nosso).

### 3.3.1 As bases legais. O consentimento. Artigo 7º, I, da LGPD

O Banco pode realizar o tratamento do dado pessoal do cliente, utilizando a inciso I, do artigo 7º, com base no **consentimento**, o qual recebeu cuidado e atuação destacada pela LGPD. Uma análise minuciosa dos princípios – que têm grande parte de seu centro gravitacional baseado no ser humano – revela a preocupação do legislador com a participação do indivíduo no fluxo de suas informações, o que reforça a ideia e importância deste tema (TEFFÉ; VIOLA, 2020).

Nos termos da Lei, o consentimento é conceituado a “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”. (BRASIL, 2018, p. 60, art. 5º, XII, da LGPD), conceito análogo a GDPR. Manifestação livre indica sem a existência dos chamados vícios do consentimento (erro, simulação, coação e fraude – artigo 8º, § 3º, da LGPD) e, ainda, a segurança da informação, ou seja, ter direito a todas as informações pertinentes aos dados geridos pelo controlador e o tempo e modo que serão utilizados. Por fim, não escapou do conceito a *finalidade*, ou seja, o titular deve ser informado a razão da coleta e do tratamento do dado, tudo em homenagem ao *princípio* estabelecido no artigo 6º, I, da LGPD<sup>31</sup>.

---

<sup>31</sup> 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;

No caso dos bancos, o consentimento assume, ainda, uma importância destacada, dado ao amplo e propagado direito à informação e às normas do Código de Defesa do Consumidor. Por isso, a doutrina já traz casos onde os dados entram sob condição do negócio, como são, efetivamente, os contratos bancários, onde a análise da questão pessoal e patrimonial são condições do negócio. (BIONI, 2019, p. 197).

O artigo em referência tem vertical aplicação aos contratos bancários e, por isso, abre espaço para a aplicação do artigo 18, da LGPD, o qual assegura aos titulares dos dados a exercerem, em qualquer tempo e modo, a fiscalização de seus dados, com amplo acesso, correções, anonimização, entre outros, e até mesmo **a revogação do consentimento, se o caso**. Todavia, a revogação não pode ser analisada somente sob a ótica do titular. No caso dos contratos bancários, onde há previsão contratual para a coleta e tratamento, os agentes financeiros têm a garantia e o direito sobre os dados, até em razão de ser isso (gerenciamento sobre os dados) uma condição necessária para a existência do negócio. A revogação, neste caso, não poderá ser realizada por ato unilateral do titular, o qual deverá buscar uma declaração judicial, e desde que comprovada a infração contratual da Instituição Financeira.

### **3.3.2 As bases legais. A execução de contrato. Artigo 7º, V, da LGPD**

A **segunda base legal** aberta à utilização pelas Instituições Financeiras, e que surge como exigência para tratamento de dados, é a prevista no artigo 7º, V, da LGPD: “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” (BRASIL, 2018, p. 60).

Esta base legal se assemelha ao consentimento, na medida em que o proprietário já é contratante (cliente do Banco), ou pretende formalizar um contrato, onde será necessário o fornecimento de seus dados ao controlador. No caso, ambas as partes formalizam uma avença, onde o titular permite o uso dos dados pessoais, e, assim, o tratamento pode ser executado, até como condição do negócio.

### **3.3.3 As bases legais. A proteção do crédito. Artigo 7º, X, da LGPD**

A **terceira base legal** aberta à utilização pelas Instituições Financeiras, e que surge como exigência para tratamento de dados, é a prevista no artigo 7º, X, da LGPD: “para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente” (BRASIL, 2018, p. 60).

A previsão legal, em referência, é de conceito aberto. Afinal, a proteção do crédito deverá ser vista sob qual ótica, a do controlador, que eventualmente detém os dados, e quer tratá-los, ou do titular, que sequer conhece o controlador, e, se levado a conhecimento, quer eliminá-los (art. 5º, XIV, da LGPD)?

O sentido da norma, ao certo, foi ampliar e facilitar a concessão de créditos, aparelhar as instituições financeiras para melhorar a análise de riscos e impulsionar o consumo (TEFFÉ; VIOLA, 2020). O sentido é a proteção do crédito, de uma maneira geral, o que envolve considerar aspectos que ensejam as características de um bom pagador, de um superendividado ou de um devedor contumaz. Isso permite uma análise tanto da capacidade de pagamento como da probabilidade de inadimplência do indivíduo, de forma a mitigar os riscos da concessão de crédito aos quais o credor se sujeita (SEBBEN, 2020).

### **3.3.4 As bases legais. Cumprimento de obrigação legal. Artigo 7º, II, da LGPD**

A **quarta base legal** aberta à utilização pelas Instituições Financeiras, deve ser utilizada por ocasião de o agente financeiro ser compelido à prática de um ato, ou cumprimento de uma obrigação, decorrente de lei.

Esta base legal, desde que bem utilizada pelo controlador, não abre qualquer espaço para discussão. Para as Instituições Financeiras, a evolução das legislações de controle de capitais e evasão de divisas, criaram obrigações cujo descumprimento levam à graves sanções.

Cita-se, aqui, alguns exemplos. A Lei 9.613/1998 é o ato normativo que cria e disciplina os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras – COAF. Por obrigação legal, os Bancos devem notificar o COAF sempre que identificarem transações com indícios

de lavagem de dinheiro, de financiamento de atividades terroristas ou de outras práticas ilícitas previstas em lei. (BRASIL, 1998).

### **3.3.5 O Legítimo Interesse utilizado na atividade bancária. Uma base legal questionada**

A Lei Geral de Proteção de Dados foi criada para regradar a *coleta, o tratamento, o armazenamento e o compartilhamento* dos dados pessoais. E, para dar vazão a este tratamento, o controlador deve demonstrar a finalidade legítima do tratamento, sob pena de ilegalidade.

As Instituições de Crédito têm à disposição várias bases legais para coletar e tratar os dados dos clientes, como premissa a um contrato bancário e a existência de um consentimento formal e escrito, até a execução da evença, onde o próprio consentimento é afastado, em determinadas hipóteses. Utilizar uma base legal aberta, portanto, pode desaguar em notórios e graves problemas de enquadramento futuros, mormente se questionados pelo titular.

Referida base legal é prevista no art. 7º, IX<sup>32</sup>, e regulamentado pelo artigo 10, da LGPD:

Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I - apoio e promoção de atividades do controlador; e

II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial (BRASIL, 2018, p. 61-62).

O artigo 10 reclama, para a utilização desta base, para além da comprovação da justificativa legítima do controlador, a entrega ao titular de algum

---

<sup>32</sup> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

direito em seu benefício, ou ao menos, uma expectativa, além dos princípios da finalidade, da necessidade e da proporcionalidade na utilização dos dados. Quanto mais invasivo, inesperado ou genérico for o tratamento, menor será a probabilidade de que seja reconhecido o legítimo interesse. (TEFFÉ; VIOLA, 2020).

A prática doutrinária faz referência a aplicação prática do requisito do legítimo interesse, a fim de evitar problemas legais de ajustes. O chamado *legitimate interest assessment* (LIA) ou teste da ponderação, surgiu no Grupo de Trabalho do Artigo 29 (*Working party 29*), o qual serviu de base para o texto do GDPR. Neste modelo, pondera-se os direitos e os interesses do controlador, e se há um interesse legítimo deste na coleta e tratamento dos dados e, noutro turno, se estão presentes os interesses e direitos, e as liberdades dos titulares.

Na visão de Souza; Viola; Padrão (2019, p. 120), o teste do legítimo interesse passa por quatro fases:

- (i) a avaliação dos interesses legítimos;
- (ii) o impacto sobre o titular do dado;
- (iii) o equilíbrio entre os interesses legítimos do controlador e o impacto sobre o titular; e
- (iv) salvaguardas desenvolvidas para proteger o titular dos dados e evitar qualquer impacto indesejado.

Nesse sentido, a Instituição Financeira poderá, à margem das outras bases legais, utilizar o legítimo interesse, desde que consiga, de forma segura, comprovar a legitimidade para a utilização e tratamento dos dados, e, paralelamente, cumprir a expectativa dos interesses do titular.

### **3.4 Os Procedimentos e as opções práticas de *compliance* disponíveis à implementação do tratamento de dados ao setor bancário. Os desafios.**

O *compliance*, a conformidade e a integridade, é um órgão de governança obrigatório dentro de toda e qualquer Instituição Financeira, a rigor do artigo 2º, da Resolução 4.595/2017<sup>33</sup>, do Banco Central do Brasil. A criação, instituição e regular funcionamento do *compliance*, portanto, é compulsória.

---

<sup>33</sup> Cf. Art. 2º As instituições mencionadas no art. 1º devem implementar e manter política de conformidade compatível com a natureza, o porte, a complexidade, a estrutura, o perfil de risco e o modelo de negócio da instituição, de forma a assegurar o efetivo gerenciamento do seu risco de conformidade.

Como já destacado, na legislação brasileira, não há, a rigor, obrigação das empresas criarem e instituírem um setor de conformidade, com poucas exceções, onde estão incluídos os agentes financeiros. O que há, de forma evidente, é o incentivo à tal prática, pois é assente que a conformidade desagua em boas práticas empresariais, previne a ocorrência de infrações ou minimiza seus danos, caso ocorridos.

A Lei Geral de Proteção de Dados trouxe uma grande leva de conceitos, normas abertas e de aplicação indefinida, um novo marco regulatório, que, inclusive, para fiscalização de eventuais desajustes e irregularidades, criou uma Agência Reguladora, no caso a ANPD. Nesse contexto, um setor de regulação interno, nas veias da organização, que atue de forma concreta e efetiva, certamente minimiza as chances de ocorrência de ilícitos e a aplicação das severas penalidades existentes na norma. Sobre o tema:

Essa característica de complementaridade fica ainda mais evidente na proteção de dados, uma vez que a LGPD apresenta grande plasticidade, utilizando-se de diversos standards e conceitos abertos, que precisam ser necessariamente contextualizados diante da realidade de cada agente econômico, do contexto social e econômico e da evolução tecnológica do momento em que forem aplicados. Logo, é fundamental que, ao lado do papel regulamentador da autoridade nacional, os agentes econômicos possam também ter a iniciativa de dar concretude aos comandos legais, adaptando-os à sua realidade a partir dos incentivos e dos esclarecimentos que recebem do próprio Estado (FRAZÃO; OLIVA; ABILIO, [2019], p. 685).

E, continuando no tema, os autores retratam os procedimentos a serem adotados em um bom programa de *compliance*, e as vantagens advindas de sua aplicação:

(i) permitir a adequada gestão do risco da atividade – na medida em que identifica os pontos sensíveis em que há exposição ao descumprimento – e, por consequência, auxiliar na prevenção de ilícitos; (ii) viabilizar a pronta identificação de eventual descumprimento, bem como a remediação de danos daí decorrentes, auxiliando, assim, na minoração dos prejuízos; (iii) fomentar a criação de uma cultura corporativa de observância às normas legais; e (iv) servir potencialmente como atenuante no caso de punições administrativas na tutela de dados soma-se à vantagem adicional de adaptar e operacionalizar diversos dos comandos gerais e conceitos abertos da LGPD. Podem-se enumerar, ainda, benefícios, ainda que indiretos, concernentes ao desenvolvimento em qualidade e inovação, além de incrementos reputacionais (FRAZÃO; OLIVA; ABILIO, [2019], p. 686).

O programa de *compliance*, inicia, portanto, com identificação precisa dos riscos da atividade, e, com isso, mapear eventuais gargalos quanto a hipóteses de descumprimentos das normas. Identificado o descumprimento, através de mecanismos de gestão, e de forma pretérita, as chances de redução dos danos é infinitamente superior e, de consequência, a minoração dos prejuízos.

A identificação e o mapeamento de riscos, inclusive, devem ser feitos de forma linear e constante, posto que a empresa pode mudar o foco de atuação, girar seus investimentos, partir para novo segmento, e enfrentar outros ramos de atividade, sob o pálio de novas legislações, e estar exposta a novos riscos. Este requisito, inclusive, é fator crucial a distinguir o *compliance* do setor de auditoria. As auditorias, em geral, são temporárias, sazonais e coletam dados por amostragem. A conformidade, ao contrário, atua permanentemente, sob forte vigilância sobre todos os segmentos da organização.

D’outro lado, um efetivo programa de *compliance*, com cursos periódicos compulsórios a todos os colaboradores, por exemplo, faz criar uma cultura dentro da organização, quanto à estrita observância das normas legais. Neste tópico, a elaboração de Códigos de Ética e de Conduta – “[...] documentos escritos que consubstanciam os valores e princípios da entidade, a serem observados por todos (inclusive terceiros), bem como orienta quais as condutas são aceitas e quais são vedadas)” (FRAZÃO; OLIVA; ABILIO, [2019], p. 689).

E, por fim, como citado pela doutrina, e previsto inclusive em legislações esparsas, a existência de programas de conformidade permite a redução de penas administrativas impostas às empresas, como é o caso da lei antiterrorismo.

No caso da LGPD, ainda, como abordado, face ao grande número de conceitos abertos e indeterminados, ter um setor de conformidade a ladear o de investimento, é salutar. E, neste ponto, o *compliance* se alia, também, à inovação. O sucesso e o crescimento empresarial, financeiro, é salutar, e ainda ganha maiores e melhores contornos se dentro da legislação, dentro das regras e evitando punições.

Segundo Frazão; Oliva; Abilio ([2019], o programa de *compliance* deve ter a estrutura de acordo e compatível com o risco e envergadura da empresa, que atue de forma independente e com recursos suficientes, além do comprometimento da Alta Administração da organização. Caso a alta cúpula atue de forma contrária com

as diretrizes constantes no programa de *compliance*, certamente não se formará a cultura entre os colaboradores acerca da obrigatoriedade do programa.

A adaptação do setor de *compliance* às novas diretrizes e exigências criadas pela Lei Geral de Proteção de Dados passa, necessariamente, também, pelo aprimoramento, ou mesmo criação de um novo modelo de controle e gestão de processos. A Instituição Financeira é, verdadeiramente, um pulmão de dados: são dados de clientes, de colaboradores, de terceirizados, de fornecedores etc. Em que pese o trabalho aqui apresentado se concentre nos dados pessoais dos clientes bancários, é certo que o tratamento dos vários outros tipos de dados também merecerá especial atenção dos gestores.

O *compliance* terá novos paradigmas para, doravante aprimorar o controle dos processos internos. Seu desafio será estabelecer novas rotinas, novos modelos de processos, para atender às Superintendências e agências, onde efetivamente os dados são coletados, armazenados, tratados e eventualmente compartilhados. Dessa forma, um monitoramento constante dos riscos é vital para o sucesso do modelo a ser empregado.

Por fim, a existência de seguros e eficientes canais de consultas/orientações, bem como uma rápida apuração e punição das condutas contrárias ao programa, são elementos essenciais para a boa gestão e funcionamento do *compliance* (FRAZÃO; OLIVA; ABILIO, [2019]).

### **3.5 O estudo de caso do Banco da Amazônia S.A.**

O Banco da Amazônia S.A. é uma Instituição Financeira Pública Federal, foi criado em 1942, exatamente no dia 9 de Julho, pelo Decreto-Lei n. 4.451. O contexto era a segunda Guerra Mundial, quando havia um esforço dos aliados para retomar a produção de borracha na Amazônia (BANCO DA AMAZÔNIA, 2019, p. [3]).

Contudo, foi na Constituição de 1988, a Magna Carta Brasileira, que reservou-se e elevou-se o Banco da Amazônia a uma importante e singular atuação dentro do cenário financeiro e social, no Brasil. Este marcante espaço está ligado à gestão da aplicação dos recursos financeiros do Fundo Constitucional de Financiamento do Norte – FNO, o que marcou definitivamente a história do BASA em todo território nacional e especialmente na região norte.

O Art. 159 da Constituição Federal de 1988 criou os Fundos Constitucionais de Financiamentos e estabeleceu as condicionantes básicas dessa arquitetura institucional: a fonte dos recursos financeiros, os agentes operadores, e a norma diretriz.

Art. 159. A União entregará: [\(Vide Emenda Constitucional nº 55, de 2007\)](#)

I - do produto da arrecadação dos impostos sobre renda e proventos de qualquer natureza e sobre produtos industrializados, 50% (cinquenta por cento), da seguinte forma:

a) vinte e um inteiros e cinco décimos por cento ao Fundo de Participação dos Estados e do Distrito Federal;

b) vinte e dois inteiros e cinco décimos por cento ao Fundo de Participação dos Municípios;

c) **três por cento, para aplicação em programas de financiamento ao setor produtivo das Regiões Norte, Nordeste e Centro-Oeste, através de suas instituições financeiras de caráter regional**, de acordo com os planos regionais de desenvolvimento, ficando assegurada ao semi-árido [*sic*] do Nordeste a metade dos recursos destinados à Região, na forma que a lei estabelecer (BRASIL, 2016, p. 101).

Nesse contexto, percebe-se que a Constituição de 1988 ratificou a importância do Banco, e reorientou sua atuação, ligando-o diretamente à política de desenvolvimento regional. A PNDR,

[...] atualizada pelo [Decreto nº 9.810, de 2019](#), representa instrumento legal que baliza a ação em busca da redução das desigualdades econômicas e sociais, intra e inter-regionais, por meio da criação de oportunidades de desenvolvimento que resultem em crescimento econômico, geração de renda e melhoria da qualidade de vida da população (BRASIL, 2023).

E, para a execução destas metas, necessária a criação de uma gama de instrumentos econômico-financeiros, onde certamente os Fundos Constitucionais são importantes mecanismos de atuação. O FNO, assim como os demais fundos constitucionais, foi REGULAMENTADO pela Lei nº 7.827 de 1989<sup>34</sup>.

---

<sup>34</sup> Regulamenta o art. 159, inciso I, alínea c, da Constituição Federal, institui o Fundo Constitucional de Financiamento do Norte - FNO, o Fundo Constitucional de Financiamento do Nordeste - FNE e o Fundo Constitucional de Financiamento do Centro-Oeste - FCO, e dá outras providências.

**Figura 3 – Rota do FNO**



Fonte: (COSTA, 2017).

E o artigo 3º, da Lei 7.827/89, (BRASIL, 1989) logo define as diretrizes dos Fundos:

Art. 3º Respeitadas as disposições dos Planos Regionais de Desenvolvimento, serão observadas as seguintes diretrizes na formulação dos programas de financiamento de cada um dos Fundos:

I - concessão de financiamento aos setores produtivos das regiões beneficiadas

II - ação integrada com instituições federais sediadas nas regiões;

III - **tratamento preferencial às atividades produtivas de pequenos e miniprodutores rurais e pequenas e microempresas, às de uso intensivo de matérias-primas e mão-de-obra locais e as que produzam alimentos básicos para consumo da população**, bem como aos projetos de irrigação, quando pertencentes aos citados produtores, suas associações e cooperativas;

IV - **preservação do meio ambiente**;

V - **adoção de prazos e carência, limites de financiamento, juros e outros encargos diferenciados ou favorecidos, em função dos aspectos sociais, econômicos**, tecnológicos e espaciais dos empreendimentos;

Logo de plano verifica-se que os recursos originários dos Fundos Constitucionais, operados pelos Bancos Públicos, não se destinam à lucratividade ou rentabilidade. Está-se a falar em recursos destinados à sustentabilidade, **inovação**, distribuição de renda, apoio aos pequenos negócios e, notadamente, aos pequenos produtores.

Atualmente, o Fundo Constitucional de Financiamento do Norte (FNO) é o principal instrumento de desenvolvimento da Amazônia, e junto com outras fontes de recursos do BASA, responderam por mais de 60% do crédito de fomento da Região Norte do país, em 2021.

**Gráfico 1 - Fundo Constitucional de Financiamento do Norte**



Fonte: (BANCO DA AMAZÔNIA, 2021, p, 9).

Desta forma, a atuação do Banco da Amazônia não é ligada, estritamente, à atividade bancária/financeira. Seu papel fundamental é ser o principal agente de indução das políticas públicas, das diretrizes políticas e estratégicas do estado brasileiro.

### **3.5.1 O Banco da Amazônia e a LGPD**

Como já destacado em linhas volvidas, os Bancos, há tempos, encontram legislações esparsas que lhes impõem o sigilo, a guarda, e a confidencialidade no processamento e armazenamento dos dados pessoais.

Inúmeras leis, resoluções, portarias etc., principalmente emanadas no Banco Central do Brasil – BACEN, órgão gestor dos Bancos, no Brasil, já regulamentavam a matéria, antes da edição da Lei 13.709/2018. No entanto, após a promulgação da referida norma jurídica, iniciou-se um novo ciclo tecnológico, dentro das Instituições Financeiras, na busca pelo cumprimento das obrigações legais, notadamente diante do cenário punitivo nela previsto.

Desta forma, a fim de fazer face à então novel legislação, o Banco da Amazônia cuidou de contratar profissionais renomados no setor, entre eles o escritório Peck Advogados<sup>35</sup>, o qual tem na sócia fundadora Patrícia Peck, renomada profissional do Direito Digital, sua principal atora.

<sup>35</sup> <https://peckadv.com.br/>

E foi neste cenário que os profissionais cunhados pela própria Instituição Financeira, aprovados via concurso público, notadamente àqueles lotados na área de tecnologia da informação, e sob a assessoria das equipes externas, de apoio, deram início a um longo, incipiente e arrojado projeto para aplicação das normas da Lei Geral de Proteção de Dados junto ao Banco da Amazônia.

As áreas de *compliance* do Banco da Amazônia funcionam de maneira efetiva. Prova disso são os índices de conformidade atingidos pela Instituição, seja em processos internos seja naqueles envolvendo terceiros, e, principalmente, na atuação junto ao público alvo, que é a venda de produtos e serviços.

Os índices de conformidade<sup>36</sup> podem ser medidos, por exemplo, em eventuais multas aplicadas pelos órgãos de controle, ou mesmo pelo *rating* das ações judiciais julgadas a favor ou contra a empresa, onde os números do Banco se mostram, sempre positivos.

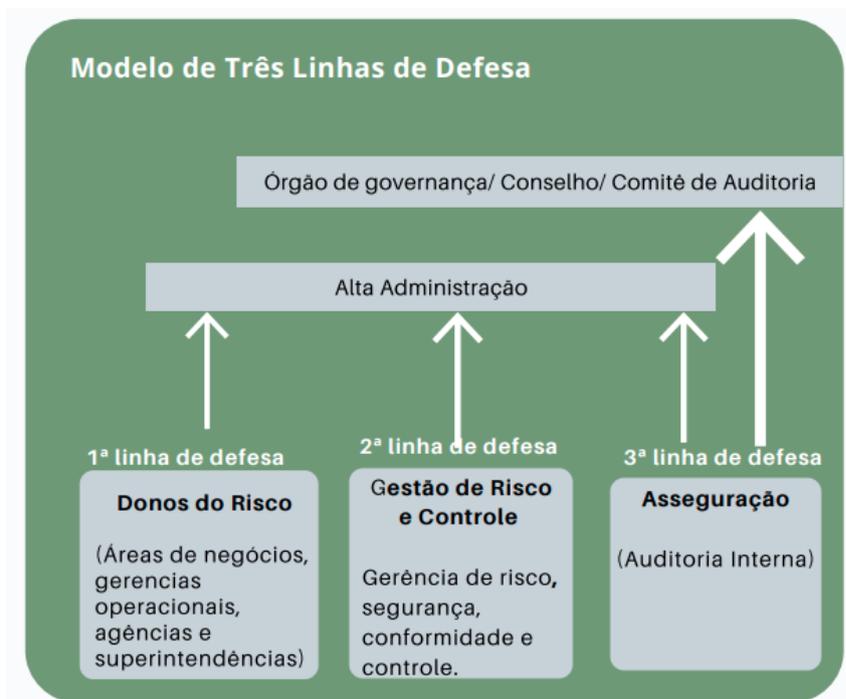
Com efeito, o Banco possui um sistema de controles internos adequados ao seu porte, perfil de risco e natureza dos seus negócios, adota como metodologia de controle interno, o modelo das Três Linhas de defesa, que assegura as competências e responsabilidades de todas as áreas da Instituição, por meio de uma estrutura integrada e coordenada, o que contribui para a efetividade dos controles internos e geração de resultados sustentáveis. Utiliza o framework COSO – Estrutura Integrada, considerando os seus componentes e princípios<sup>37</sup>.

---

<sup>36</sup> <https://www.bancoamazonia.com.br/index.php/relacoes-com-investidores/sobre-o-banco/ratings>

<sup>37</sup> <https://www.bancoamazonia.com.br/component/edocman/relatorio-anual-integrado-e-sustentabilidade-2021/viewdocument/5229?Itemid=0>

**Figura 5 – Modelos de Três linhas de Defesa**



Fonte: (BANCO DA AMAZÔNIA, 2022, p. 60).

Tais estruturas asseguram um ambiente de integridade e confiança nas relações e possibilitam a promoção de ações educativas, preventivas e corretivas concernentes à ética profissional, aos colaboradores e no tratamento com as pessoas e com o patrimônio público, onde todos os níveis hierárquicos terão papéis e responsabilidades em suas atividades objetivando a eficácia dos controles internos, cabendo ao Conselho de Administração, como instância máxima de controle interno do Banco, manter independência da gestão e exercer por meio das estruturas e processos que lhe dão suporte a supervisão sobre a administração da Instituição no desenho, implementação e aplicação dos controles.

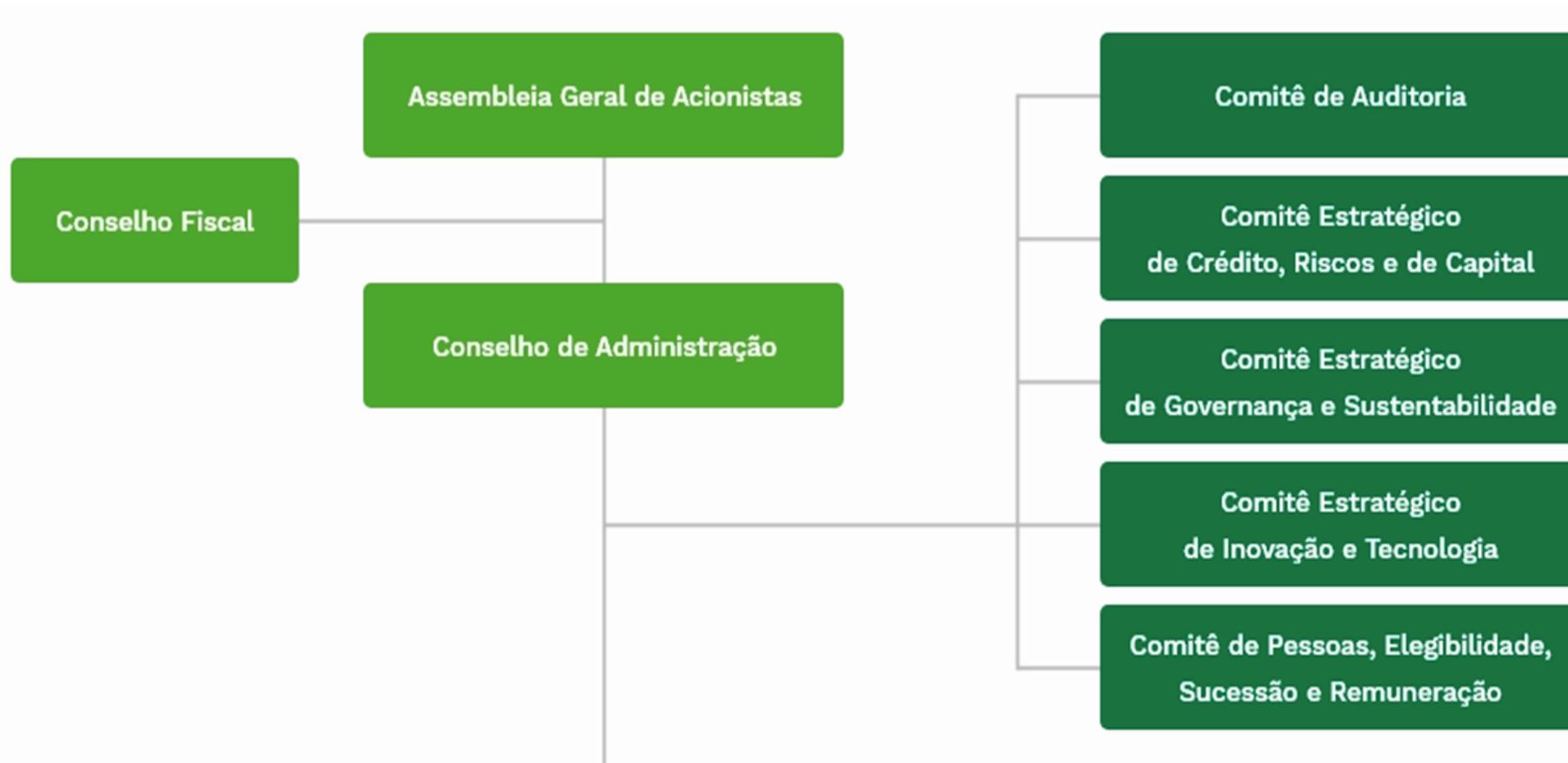
### **3.5.2 O *compliance* dentro do Banco da Amazônia e a estrutura organizacional da Instituição**

A estrutura de uma organização financeira é moldada, naturalmente, pela sua atividade finalística, com o objetivo final a ser por ela alcançado. Dentro do Banco da Amazônia S.A., banco público federal onde a União detém o controle acionário e os recursos manipulados são, basicamente, de ordem pública, é natural a existência de um

sistema angularizado de amarras e freios, traduzidos em uma enorme gama de gerências e alçadas de competência, até uma decisão final, em sua maioria tomada de forma colegiada.

Como toda empresa integrada por ações (Sociedades Anônimas), com capital aberto, como é o BASA, o maior poder encontra-se nas mãos da Assembleia Geral, caso convocada, a qual tem o poder total de deliberação:

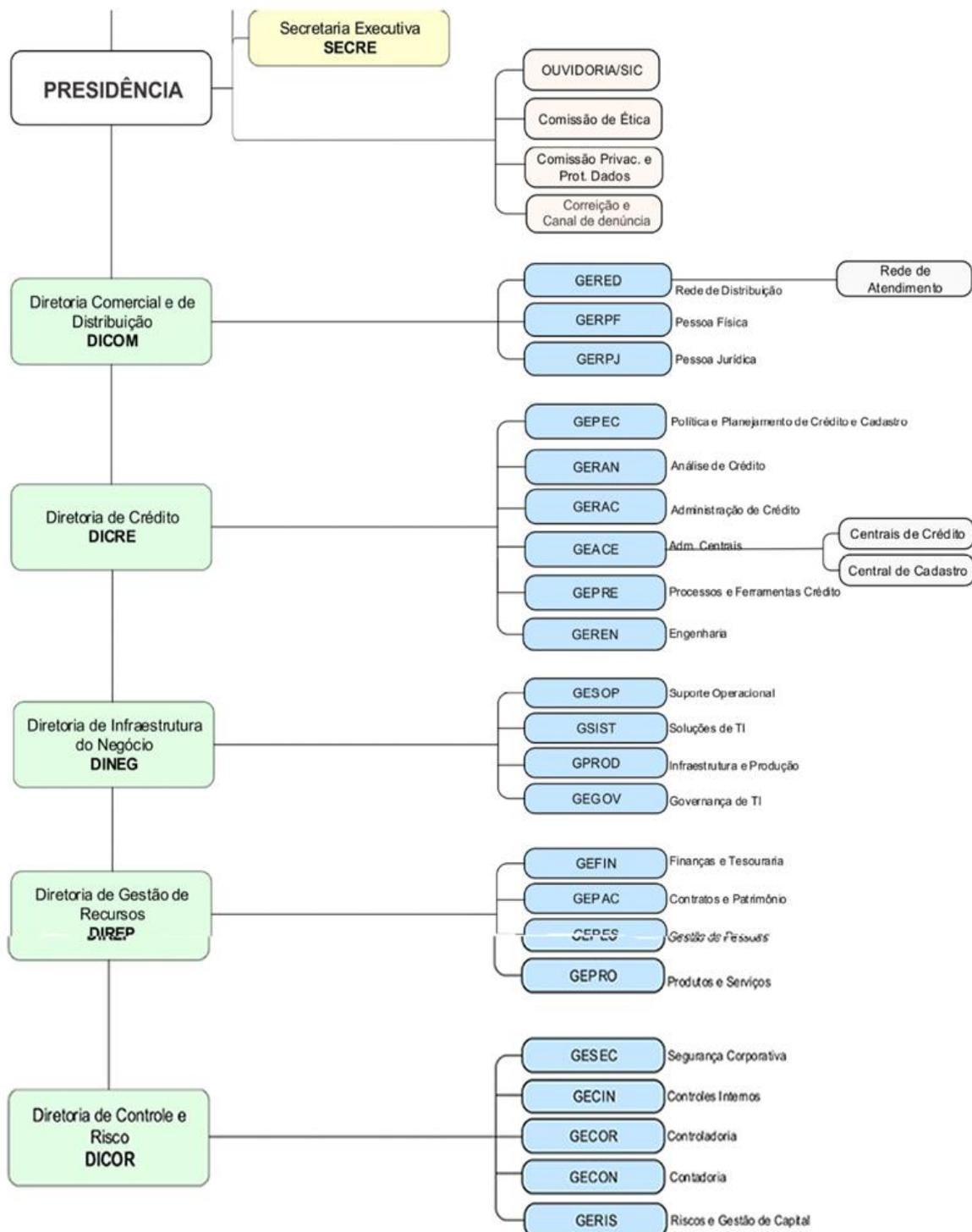
Gráfico 2 – Organograma



Fonte: (BANCO DA AMAZONIA, [S.d]).

Abaixo da AG, e do Conselho de Administração, de forma efetiva, encontra-se a Presidência da Instituição, com suas respectivas Diretorias Executivas:

**Gráfico 3 – Estrutura Organizacional**



Fonte: (BANCO DA AMAZONIA, [S.d]).

Assim, à Presidência do Banco cabe a responsabilidade de *coordenar o processo de planejamento estratégico de médio e longo prazo e seus desdobramentos; alinhar a atuação do Banco às políticas, planos e programas governamentais; coordenar e apoiar a atuação das Diretorias, para que trabalhem de forma harmônica, para cumprir suas finalidades específicas; gerir as ações do Banco voltadas à promoção do desenvolvimento regional em bases sustentáveis; acompanhar o desenvolvimento dos projetos corporativos; gerir a estrutura organizacional do Banco, definindo processos e recursos necessários para concretizar o planejado; coordenar o trabalho de gestão da marca e da imagem do Banco fazendo transparecer ao público a sua atuação responsável na dinâmica econômica socioambiental; gerir as diretrizes da atuação jurídico-institucional da empresa; alinhar a forma de atuação da Ouvidoria/SIC, assegurando a estrita observância das normas legais e regulamentares afetas ao assunto; gerir o programa de integridade e a correição.*

A Presidência do Banco divide as responsabilidades e obrigações com 05 (cinco) Diretorias, que, juntas, foram a denominada Diretorias Executiva – DIREX (BANCO DA AMAZÔNIA, [2023?])<sup>38</sup>: a) **DIRETORIA DE INFRAESTRUTURA DO NEGÓCIO (DINEG)**; b) **DIRETORIA COMERCIAL E DE DISTRIBUIÇÃO (DICOM)**; c) **DIRETORIA DE CRÉDITO (DICRE)**; d) **DIRETORIA DE GESTÃO DE RECURSOS (DIREP)**; e, finalmente, a e) **DIRETORIA DE CONTROLE E RISCO (DICOR)**.

E, cabe à DICOR - ***DIRETORIA DE CONTROLE E RISCO (DICOR)***.

Atuar para o aprimoramento da governança corporativa, mitigando riscos, promovendo maior controle e conformidade na gestão do Banco, de maneira a possibilitar maior eficácia e eficiência e segurança ao processo decisório; administrar as atividades contábeis e tributárias, incluindo a formalização e execução orçamentária observando os requisitos legais e de controle; elaborar

---

<sup>38</sup> A Diretoria Executiva (DIREX) é o órgão responsável pela administração do Banco da Amazônia, cabendo-lhe cumprir as disposições do Estatuto Social e as deliberações do Conselho Administração, com poderes de administração e gestão dos interesses do Banco da Amazônia, sendo-lhe, porém, proibido prestar quaisquer garantias, constituir hipoteca ou gravar com qualquer ônus real os bens imóveis do Banco, bem como adquiri-los ou aliená-los sem prévia e expressa autorização do Conselho de Administração. No âmbito do sistema de governança corporativa do Banco da Amazônia, deve ser entendida como órgão de administração executiva, responsável por avaliar, direcionar e monitorar, internamente, o Banco da Amazônia. A Diretoria Executiva é composta por um Presidente e cinco Diretores, todos eleitos pelo Conselho de Administração. Os poderes conferidos pelo Estatuto ao Presidente e aos Diretores, conjunto ou de per si, são exercidos diretamente ou por intermédio dos órgãos integrantes da Estrutura Organizacional, cujas subordinações, atribuições e responsabilidade estão definidas nesse Manual de Organização e no [Regimento Interno da Diretoria Executiva](#).

a Programação Orçamentária, controlando a sua execução e o desempenho econômico e financeiro do Banco, centralizando a difusão de informações gerenciais; conduzir de forma integrada a gestão riscos e de alocação de capital que possibilite a identificação, a mensuração, a avaliação, o monitoramento, o reporte, o controle e a mitigação dos efeitos adversos resultantes das interações entre os riscos; responder pelas ações institucionais de Relações com Investidores; desenvolver controles internos visando identificar desvios de padrão e riscos, assegurando níveis de adequados à legislação; desenvolver a segurança corporativa e de segurança da informação e de comunicações observando os requisitos legais, de controle e de segurança, estabelecendo processo de permanente avaliação e adequação das medidas e procedimentos de segurança de forma a resguardar a integridade das pessoas, das informações, dos ativos físicos e financeiros e da imagem do Banco; realizar o controle das dotações e do passivo.

O *Compliance*, naturalmente, encontra-se dentro da **DICOR – Diretoria de Controle e Riscos**, na medida em que cabe a este órgão *cabe atuar para o aprimoramento da governança corporativa, mitigando riscos, promovendo maior controle e conformidade na gestão do Banco, de maneira a possibilitar maior eficácia e eficiência e segurança ao processo decisório.*

Cada Diretoria Executiva é dividida, dentre suas áreas de atuação, pelas respectivas **Gerências Executivas**. As Gerências Executivas são as subdivisões existentes, dentro da Diretoria, a fim de delimitar e pulverizar a sua área de atuação.

A **DICOR – Diretoria de Controle e Riscos**, no organograma do Banco da Amazônia, é subdividida em **04 (quatro) Gerências Executivas**, (BANCO DA AMAZÔNIA, [2023?]) a saber: **8.1 GERÊNCIA EXECUTIVA DE CONTADORIA (GECON); 8.2 GERÊNCIA EXECUTIVA DE CONTROLADORIA (GECOR); 8.3 GERÊNCIA EXECUTIVA DE RISCOS CORPORATIVOS (GERIS); 8.4 GERÊNCIA EXECUTIVA DE CONTROLES INTERNOS (GECIN); 8.5 GERÊNCIA EXECUTIVA DE SEGURANÇA CORPORATIVA (GESEC).**

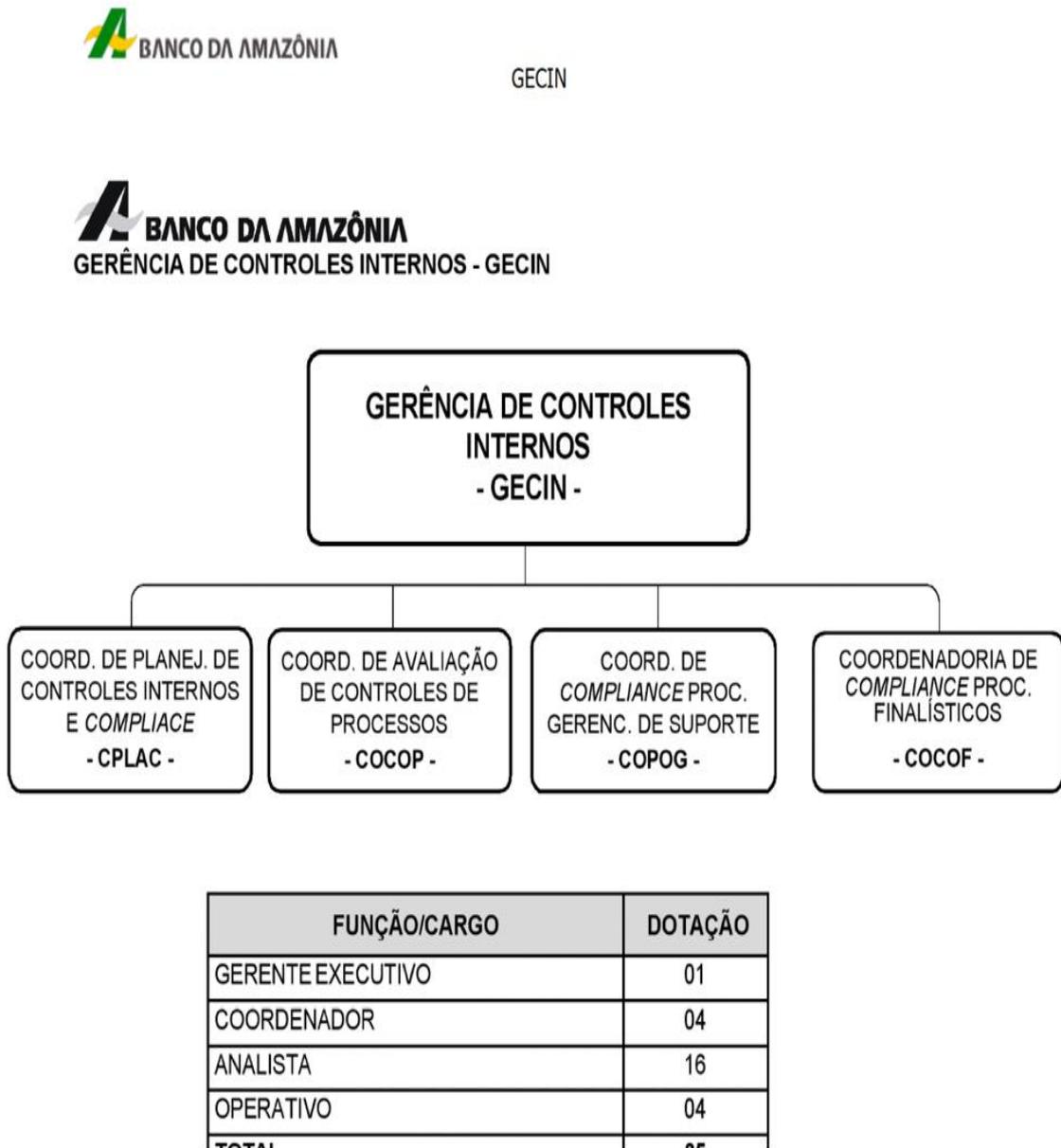
À GECIN – Gerência Executiva de Controles Internos, cabe:

8.4.1 Finalidade: atuar como segunda linha de defesa de controles internos, assegurando a conformidade regulamentar e operacional, garantindo a adequação e o funcionamento do sistema controles internos do banco, reportando às instâncias de governança e à alta administração as avaliações nos controles institucionais.

A partir da criação das Gerências Executivas, as mesmas subdividem-se em **Coordenadorias**, guardando, neste caso, a mesma divisão de responsabilidades e obrigações dentro de uma mesma gerência. Pois bem. A **GERÊNCIA EXECUTIVA**

DE CONTROLES INTERNOS (GECIN), é, por sua vez, subdividida em **04 (quatro) Coordenadorias**, assim disposta:

Figura 4 – Gerencia de Controles Internos



Fonte: (BANCO DA AMAZÔNIA, [2023?]).

Com efeito, a área de *compliance* ficou afeta a **02 (duas) Coordenadorias do Banco**, junto GERÊNCIA EXECUTIVA DE CONTROLES INTERNOS (GECIN), dentro da DICOR – Diretoria de Controle e Riscos, (BANCO DA AMAZÔNIA, [2023?]). quais sejam:

### **3 COORDENADORIA DE COMPLIANCE EM PROCESSOS GERENCIAIS E DE SUPORTE - COPOG**

#### **3.1 Compliance regulamentar - Processos Gerenciais e de Suporte.**

### **4 COORDENADORIA DE COMPLIANCE EM PROCESSOS FINALÍSTICOS - COCOF**

#### **4.1 Compliance operacional de Processos Finalísticos.**

Como se observa, o Banco da Amazônia dividiu sua área de *compliance* em ***Processos Gerenciais e de Suporte e em Processos Finalísticos***.

Na primeira, junto à **COORDENADORIA DE COMPLIANCE EM PROCESSOS GERENCIAIS E DE SUPORTE – COPOG**, o *compliance* atua junto aos procedimentos gerenciais do Banco e no Suporte às unidades: avalia os normativos internos e sugere melhorias e atualizações; verifica a aderência das normas junto às unidades e colaboradores; atua junto a processos relevantes, e junto à criação de novos produtos; monitora os próprios indicadores de *compliance*; monitora eventuais falhas na conformidade do Banco frente às normas impostas pelos órgãos externos e reguladores; emite recomendações técnicas e alertas de controle, a fim de minimizar deficiências e fragilidades em processos, produtos e serviços; elabora relatórios relacionados ao *compliance* entre outras responsabilidades.

Na segunda, junto à **COORDENADORIA DE COMPLIANCE EM PROCESSOS FINALÍSTICOS – COCOF**, o *compliance* atua junto aos processos finalísticos do Banco: faz a conformidade operacional em processos de negócio, incluindo a criação e aprovação de novos produtos; avalia a eficácia do *compliance* na primeira linha de atuação, feita pela **COPOG**; indica necessidade de melhorias; monitora o controle das agências e os indicadores de *compliance*; monitora os negócios e produtos do Banco, visando supervisionar o padrão de funcionamento; elabora relatório contendo os resultados das atividades relacionadas à função de *compliance*, entre outras responsabilidades.

Todavia, ao analisar o organograma da Instituição Financeira, principalmente junto à **GERÊNCIA EXECUTIVA DE CONTROLES INTERNOS (GECIN)**, e as 02 (duas) Coordenadorias (**COCOF e COPOG**), não há um órgão no Banco junto ao *compliance* responsável, especificamente, pelo controle e aplicação específica das normas da Lei 13.709/2018.

E, neste ponto, cinge-se o ponto nevrálgico deste Relatório Técnico: pela envergadura e importância da LGPD, através das normas e obrigações previstas na Lei 13.709/2018, a proposição é a criação de uma **nova Coordenadoria no Banco da Amazônia**, junto à **GECIN – Gerência Executiva**, para análise, fiscalização e aplicabilidade da lei.

### **3.5.3 Proposta de aprimoramento do modelo de *compliance* junto ao Banco da Amazônia para adaptação à LGPD**

Assaz ressaltar, inicialmente, o aspecto inovativo do Relatório. O projeto final apresenta uma alteração do modelo de *compliance* do Banco da Amazônia, com a criação de uma Coordenadoria junto à **GECIN – GERÊNCIA EXECUTIVA DE CONTROLES INTERNOS**, com o objetivo de *aprimorar o sistema de compliance aplicado ao Banco, o qual contemple as normas inovadoras da LGPD, e proteja a empresa de futuros dissabores, considerando as punições dela decorrentes*.

O projeto tem vinculação à inovação em processo e inovação organizacional, visto que objetiva propor o aprimoramento do sistema aplicado ao *compliance* da Instituição Financeira. A proposta de criação de uma nova Coordenadoria, com um novo arcabouço de normas/regras e o aprimoramento do sistema, desaguará em uma reestruturação da cadeia de processos hoje existente, tudo com o fito de proteger a empresa das punições decorrentes da norma legal. Insere-se, portanto, dentro do tema de Propriedade Intelectual (inovação em processo) e Transferência de Tecnologia.

Nesse sentido, a proposta desenvolvida, com a adaptação do modelo de *compliance*, centraliza a análise das obrigações legais criadas pela LGPD em um único setor, com uma nova plataforma. Os bancos terão que alterar significativamente suas rotinas de trabalho, para identificar a forma como coletam os dados, a natureza destes, a base legal para tratá-los, eventual descarte, até a possibilidade final de compartilhamento. Isso é, conceitualmente, inovação em processo.

E, finalmente, a alteração do sistema de *compliance* encerra, também, natureza de inovação organizacional, que “é a implementação de um novo método organizacional nas práticas de negócios da empresa, na organização do seu local de trabalho ou em suas relações externas” (OCDE, 2004, p. 61).

Com efeito, a proposta apresentada neste Relatório Técnico visa aprimorar o sistema de compliance, especificamente ligado à atividade de coleta e controle, e o sigilo e a confidencialidade do processamento e armazenamento dos dados. E, neste ponto, acredita-se que a criação de uma Coordenadoria própria, e independente, unicamente ligada à proteção de dados (LGPD), será ponto fundamental para aprimorar o sistema de controle e mitigar os riscos, principalmente face às multas milionárias previstas na legislação.

Desta forma, a criação de um órgão específico e individualizado, unicamente ligado à gestão e controle dos dados, poderá concentrar-se em atividades coordenadas para controlar e monitorar todos os processos da Instituição Financeira que envolvam a coleta e a segurança dos dados, objetivo maior da LGPD. Uma Coordenação de Compliance ligada à LGPD poderá criar mecanismos de gestão, com origem desde às agências da rede bancária, na ponta da Instituição, onde geralmente a coleta dos dados se inicia, até o destino final, com Operador e o Controlador dos dados.

A gestão dos dados pessoais e a própria gestão do compliance justificam referida criação, de uma área independente, na medida em que o risco das sanções legais, decorrentes da Lei 13.709/2018, vão muito além das perdas financeiras. Há o risco, iminente, das perdas reputacionais derivadas da falta de cumprimento das Leis e normas regulamentadoras, e a perda da credibilidade junto ao mercado.

Atualmente, o mercado, principalmente o financeiro, exige do Banco um cumprimento estrito de princípios e condutas éticas, e a política de integridade e conformidade nos negócios recebe um grau máximo de controle, o que, também, justifica ao nosso ver a criação da referida unidade independente.

#### **3.5.4 Criação de uma Coordenação independente para cumprimento e fiscalização da LGPD. Estrutura e organização**

Como retratado anteriormente, no organograma do Banco da Amazônia, junto à **GERÊNCIA EXECUTIVA DE CONTROLES INTERNOS (GECIN)**, há 02 (duas) Coordenadorias (*COCOF e COPOG*), sem que nenhuma delas tenha ligação umbilical pelo controle e aplicação específica das normas da Lei 13.709/2018.

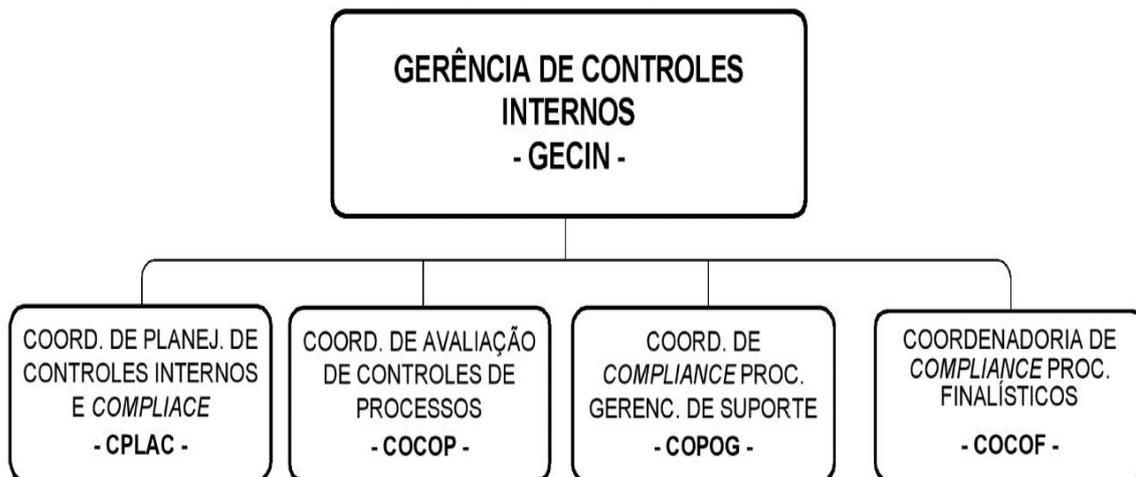
Nesse sentido, o presente trabalho, pela envergadura e importância da LGPD, através das normas e obrigações previstas na Lei 13.709/2018, faz a proposição pela

criação de uma **nova Coordenadoria no Banco da Amazônia**, junto à **GECIN – Gerência Executiva**, para análise, fiscalização e aplicabilidade da lei.

Figura 6 - GECIN



GECIN



FUNÇÃO/CARGO	DOTAÇÃO
GERENTE EXECUTIVO	01
COORDENADOR	04
ANALISTA	16
OPERATIVO	04
<b>TOTAL</b>	<b>25</b>

Fonte: (BANCO DA AMAZÔNIA, [2023?]).

A estrutura:

Propõem-se a criação da **Coordenação de Compliance no Gerenciamento e Acompanhamento de Processo de Dados Pessoais**, com designação/criação de 01 (um)

cargo de Coordenador, 04 (quatro) analistas e 01 (um) operativo, tal qual os colaboradores já designados nas outras Coordenadorias.

**A organização e responsabilidades:**

Para propiciar o acompanhamento e gerenciamento dos dados pessoais, evidencia-se a necessidade de identificar-se a natureza e qualidade da informação, o que também deverá estar afetar à referida Coordenadoria. Desta forma, ficará afeto a este órgão classificar as informações, tais como de natureza **PÚBLICA** (*divulgada publicamente, sem restrição de acesso e cuja divulgação não cause qualquer dano à instituição.*), **INTERNA** (*pode ser divulgada a todos os empregados e prestadores de serviços, desde que estes estejam comprometidos com a confidencialidade das informações*), **RESTRITA** (*pode ser divulgada a determinadas áreas, grupos ou funções, cuja divulgação pode acarretar prejuízos ao Banco*) ou **SIGILOSA** (*Informação que requer um tratamento especial e cuja divulgação não autorizada ou acesso indevido pode gerar prejuízos financeiros, legais, normativos, contratuais ou de reputação, imagem ou estratégia do Banco*).

Para além disso, elencou-se, abaixo, uma prévia das áreas afetas à nova Coordenadoria, algumas já existentes no sistema da Instituição e agora proposto o seu deslocamento, e outras inéditas, objeto deste trabalho (BANCO DA AMAZÔNIA, [2023?]):

- v)** *Identificação de todo o normativo, interno e externo, sobre a LGPD e conformidade de dados, e manter inventário atualizado deste arcabouço legal;*
- w)** *Identificação e orientação às demais unidades do Banco acerca das bases legais da Lei 13.709/2018, que autorizam a coleta e tratamento dos dados por parte da Instituição Financeira;*
- x)** *Identificação das unidades internas do Banco que coletam dados pessoais;*
- y)** *Identificação das unidades internas do Banco que manipulam dados pessoais;*
- z)** *Identificação dos processos e/ou das atividades relevantes para empresa, levando em consideração tanto os aspectos da conformidade operacional, quanto regulatória;*
- aa)** *Identificação dos processos de verificação obrigatória que contenham coleta e necessidade de tratamento de dados pessoais, tais como: cadastro; contrato de abertura de contas; todas as operações de crédito (contratos de mútuo etc); transações realizadas via canais de atendimento; contratos administrativos realizados pelo Banco, incluindo as licitações;*
- bb)** *Identificação, análise e acompanhamento dos procedimentos junto ao setor de Recursos Humanos, contratação e demissão dos empregados e a coleta e tratamento dos dados dos empregados públicos e terceirizados;*
- cc)** *Propor a divisão, dentro da Coordenadoria, de subgrupos de controle para gerenciamento no cumprimento das normas;*

**dd)** *Controle periódico das agências/unidades responsáveis pelo cadastro dos clientes e coleta dos dados, principalmente com supervisão dos contratos de abertura de crédito e autorização dos terceiros para a coleta e tratamento dos dados pessoais;*

**ee)** *Monitorar os procedimentos de controle de acesso às informações que contenham dados pessoais, com objetivo de garantir que somente pessoas autorizadas tenham acesso à determinada informação, recurso computacional ou ambiente físico.*

**ff)** *Monitorar e acompanhar os contratos e procedimentos (relacionamentos) mantidos com todos os fornecedores de serviços, independentemente da natureza (notadamente a segurança dos dados, documentos e informações), de modo a mitigar riscos associados ao acesso dos fornecedores aos ativos do Banco.*

**gg)** *Identificar, cadastrar, monitorar e relatar incidentes de segurança da informação relevante ou incidente cibernético, envolvendo dados pessoais, que afetem o Banco ou terceiros;*

**hh)** *Considerando os dados pessoais já tomados pelo Banco, e após a implantação da LGPD, propor, periodicamente e assim que necessário, a classificação, reclassificação, anonimização e pseudonimização, manuseio, armazenamento, transporte e descarte dos dados, alertando a rede da utilização de forma transparente e apenas para a finalidade para a qual foi autorizada.*

**ii)** *Acompanhar os procedimentos e forma de descarte dos dados;*

**jj)** *Realizar teste de avaliação junto a todas as unidades identificadas, e verificar a aderência ao arcabouço legal, à regulamentação infralegal, às recomendações dos órgãos de supervisão e, quando aplicáveis, aos códigos de ética e de conduta do Banco;*

**kk)** *Propor e encaminhar relatório sistemático dos resultados à DICOR (Diretoria de Controle e Risco), à GERIS (Gerência de Riscos Corporativos), à DIREX (Diretoria Executiva) e ao CONSAD (Conselho de Administração);*

**ll)** *Promover a disseminação de valores, e programas de conscientização da segurança dos dados, via comunicados e comunicações internas de forma contínua, dos princípios e normas ligadas à LGPD e à necessidade de adaptação e cumprimento da lei de proteção de dados, propondo treinamentos obrigatórios, disseminação de artigos etc;*

**mm)** *Atuar, juntamente com a Comissão de Privacidade e Proteção de Dados Pessoais (CPPD), na avaliação de contratos congêneres que envolvam tratamento de dados pessoais e nos incidentes de violação de dados pessoais no âmbito da LGPD.*

**nn)** *Reportar imediatamente a identificação de qualquer fato relevante, deficiência, falha ou não cumprimento das normas de proteção de dados à autoridade superior.*

**oo)** *Criar uma Política de Gestão e Acompanhamento dos Dados Pessoais, ligada à Lei 13.709/2018, bem como alinhada aos demais normativos congêneres;*

**pp)** *As diretrizes relativas à gestão do Compliance dos dados pessoais deverão ser revistas periodicamente a fim de que os controles internos se mantenham adequados e a eles sejam incorporadas medidas relacionadas à mitigação de risco de Compliance, de acordo com a natureza e complexidade dos negócios do Banco da Amazônia.*

Com a criação desta nova unidade, dentro da Gerência de Controle de Riscos – GECIN, acredita-se que o controle dos processos será aferido de maneira mais incisiva, aprimorando os procedimentos e mitigando os riscos na aplicação dos comandos da LGPD.

#### 4 CONSIDERAÇÕES FINAIS

A Lei Geral de Proteção de Dados – Lei 13.709/2018 veio, em um cenário mais que tardio, proteger importantes direitos do cidadão. Os dados pessoais estão umbilicalmente ligados aos direitos da privacidade, da liberdade e do livre desenvolvimento da personalidade, todos de hospedagem constitucional.

Como destaca Patrícia Peck Pinheiro, a LGPD foi criada com o objetivo principal de proteger os direitos fundamentais de liberdade e privacidade das pessoas, bem como promover o livre desenvolvimento de suas personalidades. Com isso, a lei estabelece uma série de princípios e medidas de controle técnico que devem ser seguidos para garantir a segurança e a privacidade dos dados pessoais identificáveis. E entre os principais impactos da LGPD está a garantia dos direitos dos titulares, que incluem o direito à portabilidade dos dados pessoais. Esses direitos são novos para o ordenamento jurídico e para empresas públicas e privadas, e devem ser respeitados dentro de um prazo razoável previsto pela lei brasileira. Em resumo, as instituições devem estar preparadas para cumprir com as exigências da lei e garantir a proteção dos dados pessoais dos titulares (PINHEIRO, 2023).

Com efeito, diante deste novo cenário criado pela Lei Geral de Proteção de Dados, e das consequências desastrosas àqueles que a descumprirem, iniciou-se, a partir da publicação da norma, em agosto de 2018, uma corrida frenética para sua análise e implantação, notadamente para as empresas que, de qualquer forma, coletassem e manipulassem dados pessoais.

E, nesse contexto, as Instituições Financeiras foram atingidas em cheio. Talvez poucas empresas mantenham, em seus cadastros, mais dados pessoais de clientes que os Bancos. Foi neste ambiente que se idealizou o presente trabalho: em que medida a LGPD impactou as Instituições Financeiras e, para além disso, de que forma o setor de compliance bancário poderia ajudar nesse cenário transformador, a fim de garantir o cumprimento da norma. O problema estava, então, apresentado<sup>39</sup>.

Para tanto, neste estudo, examinou-se as exigências legais trazidas pela LGPD às empresas do setor bancário. E, em seguida, apresentou-se os procedimentos

---

<sup>39</sup> De que forma é possível adaptar o sistema de *compliance* para o setor bancário, de modo que atenda as inovações criadas pela Lei Geral de Proteção de Dados, e, de consequência, reduza os riscos de danos administrativos e financeiros dela decorrentes?

de *compliance* disponíveis para, paralelamente a outros setores da Instituição, dar vazão ao cumprimento rigoroso da novel legislação.

Chegou-se, então, à parte final, onde apresenta-se um *estudo de caso*, de acordo com o setor de conformidade e *compliance* do Banco da Amazônia, importante Banco Público Federal, certamente o maior agente de fomento da região norte do Brasil, e ator principal e exclusivo na aplicação do FNO – Fundo Constitucional de Financiamento do Norte, criado pelo art. 159, da CF/88, e regulamentado pela Lei 7.897/1989.

Este Relatório técnico, ao final, concentrou-se em sugerir um aprimoramento do atual modelo de conformidade do Banco estudado, com a criação de uma nova Coordenadoria de Trabalho, unicamente responsável pelo *compliance* ligado à Lei Geral de Proteção de Dados. A sugestão indicada não se trata de uma proposição exclusiva ao Banco da Amazônia, mas sim a todas as Instituições Financeiras, à rede bancária e agentes financeiros.

A criação de um setor/órgão de conformidade é obrigatório aos Bancos, conforme já destacado em linhas pretéritas, isso desde a Resolução BACEN 2554/1998 e hoje materializado pela Lei das Estatais.

Desta forma, a criação de um órgão específico e individualizado, unicamente ligado à gestão e controle dos dados, poderá concentrar, em local próprio, atividades coordenadas para controlar e monitorar todos os processos da Instituição Financeira que envolvam a coleta e a segurança dos dados, objetivo maior da LGPD.

Uma Coordenação de Compliance ligada à LGPD poderá criar e facilitar os mecanismos de gestão, com origem desde às agências da rede bancária, na ponta da Instituição, onde geralmente a coleta dos dados se inicia, até o destino final, com Operador e o Controlador dos dados. Este novo panorama justifica a concepção de uma área independente, na medida em que o risco das sanções legais, decorrentes da Lei 13.709/2018, vão muito além das perdas financeiras. Há o risco, iminente, das perdas reputacionais derivadas da falta de cumprimento das Leis e normas regulamentadoras, e a perda da credibilidade junto ao mercado.

A Lei Geral de Proteção de Dados criou uma agência reguladora, a Autoridade Nacional de Proteção de Dados (ANPD). Desde o início da vigência da norma, referido órgão vem, paulatinamente, se estruturando, e, quando chegar ao seu ápice, de gestão e controle, as consequências legais do descumprimento da lei certamente baterão

às portas das empresas, organizações, pessoas físicas, enfim, todos aqueles que manipulem dados sem o devido rigor.

E as multas, como à sociedade exposto neste trabalho, são milionárias, o que será determinante para a continuidade dos negócios. Os dados pessoais, como fator de geração de divisas, somente serão garantidos pela efetiva aplicação da LGPD, seja de forma coercitiva ou espontânea, a fim de ser o elo garantidor das riquezas do novo petróleo na atualidade (TEIXEIRA, [2020]).

Não há espaço para retrocesso!

## REFERÊNCIAS

10 BASES Legais da LGPD: [Tabela com todas as definições]. *In: Legalcloud Consultoria LTDA*, 5 nov. 2020. Disponível em: <https://legalcloud.com.br/bases-legais-lgpd-tabela/>. Acesso em: 11 mar. 2022.

ALVES, Jorge. *Compliance para Mercados Regulados*. *In: CONGRESSO DE COMPLIANCE*, 3., 2013. *Anais [...]*. São Paulo: IBC Brasil, 2013. (pelo Banco Votorantim).

BANCO CENTRAL DO BRASIL. Resolução nº 2.554. de 24 de setembro de 1998. Dispõe sobre a implantação e implementação de sistema de controles internos. Brasília, DF, 1998. 5 p. Disponível em: [https://www.bcb.gov.br/pre/normativos/res/1998/pdf/res\\_2554\\_v3\\_P.pdf](https://www.bcb.gov.br/pre/normativos/res/1998/pdf/res_2554_v3_P.pdf). Acesso em: 11 mar. 2022.

BANCO DA AMAZÔNIA. [Site]. Belém-Pará, [s. d]. Disponível em: <https://www.bancoamazonia.com.br/>. Acesso em: 11 jan. 2023.

BANCO DA AMAZÔNIA. **Carta anual de políticas públicas e governança corporativa**: exercício 2021. Belém-Pará, abr. 2021. Disponível em: <https://www.bancoamazonia.com.br/component/edocman/carta-anual-de-politicas-publicas-2021/viewdocument/5033>. Acesso em: 12 fev. 2023.

BANCO DA AMAZÔNIA. Estrutura Organizacional. [2023?]. Disponível em: <https://www.bancoamazonia.com.br/index.php/relacoes-com-investidores/sobre-o-banco/estrutura-organizacional>. Acesso em: 15 jan. 2023.

BANCO DA AMAZÔNIA. FNO Fundo Constitucional de Financiamento do Norte (LEIS Nº 7.827/1989, Nº 9.126/1995 e Nº 10.177/2001). Processo de Contas Ordinárias Exercício de 2017. Belém-Pará, abr. 2018. Disponível em: <https://antigo.mdr.gov.br/images/stories/acessoainformacao/relatoriodegestao/2017/fno-RelatorioGestao.pdf>. Acesso em: 12 fev. 2023.

BANCO DA AMAZÔNIA. O papel estratégico do BASA para o Desenvolvimento da Amazônia, incluindo os bancos do Brasil e do Nordeste, como operadores do Fundo Constitucional de Financiamento do Centro-Oeste (FCO) e do Fundo Constitucional de Financiamento do Nordeste (FNE). Brasília, DF, AEBA, 7 nov. 2019. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/cindra/arquivos/07-11-2019-2>. Acesso em: 15 jan. 2023.

BANCO DA AMAZÔNIA. **Relatório Anual Integrado e Sustentabilidade 2021**. Belém-Pará, abr. 2022. Disponível em: <https://www.bancoamazonia.com.br/component/edocman/relatorio-anual-integrado-e-sustentabilidade-2021/viewdocument/5229?Itemid=0>. Acesso em: 12 fev. 2023.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BRASIL. [Código Civil (2002)]. **Código civil brasileiro e legislação correlata**. 2. ed. Brasília, DF: Senado Federal, Subsecretaria de Edições Técnicas, 2008. 616 p.

Disponível em:

<https://www2.senado.leg.br/bdsf/bitstream/handle/id/70327/C%C3%B3digo%20Civil%20%20ed.pdf>. Acesso em: 11 jan. 2023.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**: texto constitucional promulgado em 5 de outubro de 1988, com as alterações determinadas pelas Emendas Constitucionais de Revisão nos 1 a 6/94, pelas Emendas Constitucionais nos 1/92 a 91/2016 e pelo Decreto Legislativo no 186/2008. Brasília, DF: Senado Federal, Coordenação de Edições Técnicas, 2016. 496 p. ISBN: 978-85-7018-698-0. Disponível em:

[https://www2.senado.leg.br/bdsf/bitstream/handle/id/518231/CF88\\_Livro\\_EC91\\_2016.pdf](https://www2.senado.leg.br/bdsf/bitstream/handle/id/518231/CF88_Livro_EC91_2016.pdf).

Acesso em: 15 maio 2017.

BRASIL. Despachos do Presidente da República. Mensagem nº 451, de 14 de agosto de 2018. **Diário Oficial da União**: seção 1, Brasília, DF, ano 155, n. 157, p. 75-81, 15 ago. 2018a. ISSN 1677-7042. Disponível em:

[http://www.planalto.gov.br/ccivil\\_03/\\_Ato2015-2018/2018/Msg/VEP/VEP-451.htm](http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Msg/VEP/VEP-451.htm).

Acesso em: 4 mar. 2021.

BRASIL. Lei n. 13.303, de 30 de junho de 2016. Dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios. **Diário Oficial da União**: seção 1, Brasília, DF, ano 153, n. 125, p. 1-10, 1 jul. 2016. ISSN 1677-7042. Disponível em:

<https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=1&data=01/07/2016>. Acesso em: 15 mar. 2022.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). **Diário Oficial da União**: seção 1, Brasília, DF, ano 155, n. 157, p. 59-64, 15 ago. 2018b. ISSN 1677-7042. Disponível em:

<https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=515&pagina=59&data=15/08/2018>. Acesso em: 15 maio 2021.

BRASIL. Lei n. 9.613, de 3 de março de 1998. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores, a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências. **Diário Oficial da União**: seção 1, Brasília, DF, ano 136, n. 42, p. 1-3, 4 mar. 1998. ISSN 1677-7042.

Disponível em:

<https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=13&data=04/03/1998>. Acesso em: 15 mar. 2022.

BRASIL. Lei nº 12.846, de 1 de agosto de 2013. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. **Diário Oficial da União**: seção 1, Brasília, DF, ano 150, n. 148, p. 1-3, 2 ago. 2013. ISSN 1677-7042.

Disponível em:

<https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=02/08/2013&jornal=1&pagina=2&totalArquivos=128>. Acesso em: 4 mar. 2021.

BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. **Diário Oficial da União**: seção 1, Brasília, DF, ano 156, n. 130, p. 1-3, 9 jul. 2019. ISSN 1677-7042. Disponível em:

<https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=515&pagina=1&data=09/07/2019>. Acesso em: 12 mar. 2022.

BRASIL. Lei nº 7.827, de 27 de setembro de 1989. Regulamenta o art. 159, inciso I, alínea c, da Constituição Federal, institui o Fundo Constitucional de Financiamento do Norte - FNO, o Fundo Constitucional de Financiamento do Nordeste - FNE e o Fundo Constitucional de Financiamento do Centro-Oeste - FCO, e dá outras providências. Brasília, DF, 27 set. 1989. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/l7827.htm](http://www.planalto.gov.br/ccivil_03/leis/l7827.htm). Acesso em: 1 jan. 2023.

BRASIL. Medida Provisória nº 869, de 27 de dezembro de 2018. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. **Diário Oficial da União**: seção 1, Brasília, DF, ano 155, n. 149, p. 8-9, 28 dez. 2018c. ISSN 1677-7042. Disponível em:

<https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=515&pagina=59&data=15/08/2018>. Acesso em: 15 maio 2021.

BRASIL. Ministério da Integração e do Desenvolvimento Regional. Política Nacional de Desenvolvimento Regional. Brasília, DF, 6 mar 2023. Disponível em: <https://www.gov.br/mdr/pt-br/assuntos/desenvolvimento-regional/pndr>. Acesso em: 15 mar. 2023.

BRASIL. Superior Tribunal de Justiça. **Súmula 550/STJ**. Recurso especial repetitivo. Consumidor. Credit scoring. Recurso especial representativo de controvérsia. Tema 710. Direito do consumidor. Banco de dados. Arquivos de crédito. Sistema credit scoring. Compatibilidade com o direito brasileiro. Brasília, DF: STJ, 19 out. 2015. Doc. LEGJUR 158.0515.0000.0000. Disponível em: <https://www.legjur.com/sumula/busca?tri=stj&num=550#:~:text=26.,dados%20consi%20derados%20no%20respectivo%20c%C3%A1culo.%C2%BB>. Acesso em: 1 mar. 2022.

COIMBRA, Marcelo de Aguiar; MANZI, Vanessa Alessi (Coord.). **Manual de Compliance**: preservando a boa governança e a integridade das organizações. São Paulo: Atlas, 2010.

COSTA, Divino Placido da. BASA realiza palestra do Projeto Rota do FNO. In: GUARAÍ (Município). **Câmara Municipal de Guaraí**, Guaraí, TO, 31 maio 2017. Disponível em: <https://www.guarai.to.leg.br/institucional/noticias/basa-realiza-palestra-do-projeto-rota-do-fno>. Acesso em: 2 fev. 2023.

DOYLE, Eleanor *et al.* *Compliance-innovation: a quality-based route to sustainability*. **Journal of the Cleaner Production**, [s.l], v. 210, p. 266-275, 10 fev. 2019. ISSN 1879-1786.

FEBRABAN. **Função de Compliance**. [s.n]: Grupo de Trabalho-ABBI-FEBRABAN, jul. 2009. Disponível em: [http://www.abbi.com.br/download/funcaoodecompliance\\_09.pdf](http://www.abbi.com.br/download/funcaoodecompliance_09.pdf). Acesso em: 29 mar. 2022.

FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais: noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (org.). **A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters / Revista dos Tribunais, [2019a]. p. 23-52. ISBN 978-85-5321-663-5. Disponível em: [https://www.academia.edu/40040787/Compliance\\_de\\_dados\\_pessoais](https://www.academia.edu/40040787/Compliance_de_dados_pessoais). Acesso em: 15 maio 2021.

FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (org.). **A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters / Revista dos Tribunais, [2019b]. p. 99-129. ISBN 978-85-5321-663-5. Disponível em: [https://www.academia.edu/40040787/Compliance\\_de\\_dados\\_pessoais](https://www.academia.edu/40040787/Compliance_de_dados_pessoais). Acesso em: 15 maio 2021.

FRAZÃO, Ana. Programas de *compliance* e critérios de responsabilização de pessoas jurídicas por ilícitos administrativos. *In*: ROSSETTI, Maristela Abla; PITTA, Andre Grunspun. **Governança corporativa: avanços e retrocessos**. São Paulo: Quartier Latin, 2007. p. 42.

FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. *Compliance de dados pessoais*. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (org.). **A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters / Revista dos Tribunais, [2019]. p. 677-715. Cap. 10. ISBN 978-85-5321-663-5. Disponível em: [https://www.academia.edu/40040787/Compliance\\_de\\_dados\\_pessoais](https://www.academia.edu/40040787/Compliance_de_dados_pessoais). Acesso em: 15 maio 2021.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2009.

GIOVANINI, Wagner. **Compliance a excelência na prática**. São Paulo, 2014.

GOMES, Jose. É possível ter/estar em *compliance* e inovar. **Compliance e Inovação: Será?**, 10 abr. 2018. Disponível em: <https://medium.com/compliance-e-inova%C3%A7%C3%A3o-ser%C3%A1/%C3%A9-poss%C3%ADvel-ter-estar-em-compliance-e-inovar-77774ed559ed>. Acesso em: 12 mar. 2022.

HIJAZ, Tailine Fátima. A importância do *compliance* para a efetivação de medidas anticorrupção no contexto da sociedade de risco e do Direito Penal Econômico. **Boletim Científico ESMPU**, Brasília, DF, ano 15, n. 48, p. 155-190, jul./dez. 2016. ISSN 1676-4781. Disponível em: <https://escola.mpu.mp.br/publicacoescientificas/index.php/boletim/article/view/479>. Acesso em: 15 mar. 2022.

MANZI, Vanessa Alessi. **Compliance no Brasil**: consolidação e perspectivas. São Paulo: Saint Paul, 2008.

MENDES, Laura Schertel. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. In: SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (coord.). **Lei Geral de Proteção de Dados**. São Paulo: Revista dos Tribunais, 2019. p. 35-46. (Caderno Especial, nov. 2019).

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova lei de proteção de dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. **Revista de Direito do Consumidor**, Brasília, DF, v. 120, ano 27, p. 469-483, nov/dez, 2018. Disponível em: <https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/1116>. Acesso em: 15 mar. 2022.

MORAIS, Eslei José de. **Controles internos e estrutura de decisão organizacional**: o caso da Contadoria do Banco do Brasil. Dissertação (Mestrado em Administração) – Universidade Federal do Paraná, Curitiba, 2005.

OCDE. **Manual de Oslo**: proposta de diretrizes para coleta e interpretação de dados sobre inovação tecnológica. Traduzido das edições originais em inglês e francês pelo FINEP. [Rio de Janeiro]: FINEP, 2004. Disponível em: [http://www.finep.gov.br/images/a-finep/biblioteca/manual\\_de\\_oslo.pdf](http://www.finep.gov.br/images/a-finep/biblioteca/manual_de_oslo.pdf). Acesso em: 1 jan. 2022.

OLIVA, Milena Donato; SILVA, Rodrigo da Guia. Notas sobre o *compliance* no direito brasileiro. **REVISTA QUAESTIO IURIS**, Rio de Janeiro, v. 11, n. 4, p. 2708-2729, dez. 2018. ISSN 1516-0351. DOI: <https://doi.org/10.12957/rqi.2018.33843>. Disponível em: <https://www.e-publicacoes.uerj.br/index.php/quaestioiuris/article/view/33843>. Acesso em: 05 abr. 2022.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais**: comentários à lei N 13709/2018 (LGPD). 4. ed. São Paulo: Saraiva Jur, 2023.

SAMPAIO, Joelson. A evolução do programa de *compliance* no Brasil. In: Colunas do Nefin. **Valor Investe**. [s.l], 20 jun. 2019. Disponível em: <https://valorinveste.globo.com/blogs/nefin/coluna/a-evolucao-dos-programas-de-compliance-no-brasil.ghtml>. Acesso em: 15 jul. 2019.

SEBBEN, Naiara Anna. **O direito à proteção de dados pessoais e o mercado de crédito no Brasil**: análise à luz da lei n° 13.709/2018 (LGPD) e da lei complementar n° 166/2019. Orientadora: Suelen Carls. 2020. 144 f. Dissertação (Mestrado em

Direito) - Universidade de Marília, Marília, SP, 2020. Disponível em: <https://portal.unimar.br/site/public/pdf/dissertacoes/595A37243A61B8D7FCAD52829C604839.pdf>. Acesso em: 1 mar. 2022.

SENAS, Alexandre. Abertura de Capital: o fundamental papel do *compliance* para a transparência de processos e a valorização da sua empresa no mercado de ações nacionais e internacionais. In: CONGRESSO DE *COMPLIANCE*, 3., 2013. **Anais** [...]. São Paulo: IBC Brasil, 2013. (pela Deloitte Touche Tohmatsu).

SOUZA, Jane Dias Gomes de. A importância da função de *compliance* em instituições financeiras. 2013. 46 p. MBA (Especialização em Finanças) - Ibmec Business School, Rio de Janeiro, 2013. Disponível em: <https://web.bndes.gov.br/bib/jspui/handle/1408/7025>. Acesso em: 15 mar. 2022.

SZTAJN, Rachel; SILVA, Reinaldo Marques da. “*Compliance*” e LGPD. **Campo Grande News**: conteúdo de verdade, Campo Grande – MS, 18 out. 2020. Disponível em: <https://www.campograndenews.com.br/artigos/compliance-e-lgpd>. Acesso em: 15 abr. 2022.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica.com**: revista eletrônica de direito civil, Rio de Janeiro, v. 9, n. 1, p. 1-38, 9 maio 2020. E-ISSN 2316-8374. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/510>. Acesso em: 5 mar. 2022.

TEIXEIRA, Ilderlandio. A LGPD como fonte de riqueza!. **JusBrasil**, [2020]. Disponível em: <https://ilderlandio.jusbrasil.com.br/artigos/783994130/a-lgpd-como-fonte-de-riqueza>. Acesso em: 11 mar. 2023.

WAINER, Jacques. Métodos de pesquisa quantitativa e qualitativa para a ciência computação. In: KOWALTOWSKI, Tomasz; BREITMAN, Karin (org.). **Atualização em informática**. Porto Alegre: SBC, 2007. p. 221-262.

ISBN 978-65-00-66778-3



9 786500 667783

# COMPLIANCE



## **APÊNDICE D – CARTILHA**

**CARTILHA DE COMPLIANCE PARA  
ADAPTAÇÃO À LGPD NAS  
INSTITUIÇÕES FINANCEIRAS**

**REGULATIONS**

**RULES - LAW**

**REQUIREMENTS**

**COMPLIANCE**

**STANDARDS**

**TRANSPARENCY**

**POLICIES**

**CARTILHA DE COMPLIANCE PARA  
ADAPTAÇÃO À LGPD NAS  
INSTITUIÇÕES FINANCEIRAS**

**REGULATIONS**

**RULES - LAW**

**REQUIREMENTS**

**COMPLIANCE**

**STANDARDS**

**TRANSPARENCY**

**POLICIES**

**Mauricio Cordenonzi**

DISCENTE DO MESTRADO PROFISSIONAL DO PROGRAMA DE PÓSGRADUAÇÃO  
EM PROPRIEDADE INTELECTUAL E TRANSFERÊNCIA DE TECNOLOGIA PARA A  
INOVAÇÃO/UFT

**Prof. Gilson Porto Jr.**

DOCENTE DO MESTRADO PROFISSIONAL DO PROGRAMA DE PÓSGRADUAÇÃO  
EM PROPRIEDADE INTELECTUAL E TRANSFERÊNCIA DE TECNOLOGIA PARA A  
INOVAÇÃO/UFT

**CARTILHA DE  
COMPLIANCE PARA  
ADAPTAÇÃO À LGPD  
NAS INSTITUIÇÕES  
FINANCEIRAS**

Palmas/TO  
2023



*Creative Commons "by-nc-sa" licenses*

*O conteúdo deste trabalho, exceto quando houver ressalva, é publicado sob a licença CC Atribuição 4.0*

Capa e contracapa - Canva  
Ilustrações - PNGWING

#### Dados da Catalogação *Anglo-American Cataloguing Rules – AACR2*

---

**C794c**

Cordenonzi, Mauricio

Cartilha de Compliance para adaptação à LGPD nas instituições financeiras [recurso eletrônico]. / Mauricio Cordenonzi, Francisco Gilson Rebouças Porto Junior. -- Palmas, TO: [S.n], 2023.  
47 f.; il. Color.

Material como produto da Dissertação de Mestrado do PROFNIT/UFT.

1. Direito – proteção de dados. 2. *Compliance*. 3. Bancos - Clientes. 4. LGPD. I. Porto Junior, Francisco Gilson Rebouças Porto Junior. II. Título.

CDD 332.1068  
CDU 347.734: 342.721(81)  
LCC KF6449.

---

Ficha Catalográfica elaborada por *Marcelo Diniz* - CRB 2/1533.

[Resolução CFB nº 184, de 29 de setembro de 2017.](#)

TODOS OS DIREITOS RESERVADOS - A reprodução total ou parcial de qualquer forma ou por qualquer meio deste documento é autorizado desde que citada a fonte. A violação dos direitos do autor ([Lei nº 9.610/98](#)) é crime estabelecido pelo artigo 184 do Código Penal.

# SUMÁRIO

<b>APRESENTAÇÃO</b> .....	6
<b>COMPLIANCE</b> .....	7
<b>A LEI DE DADOS PESSOAIS EM UM PANORAMA GERAL E NO CONTEXTO HISTÓRICO</b> .....	8
<b>COMPLIANCE E AS INSTITUIÇÕES FINANCEIRAS</b> .....	10
<b>COMPLIANCE E A INOVAÇÃO</b> .....	12
<b>COMPLIANCE E A LGPD</b> .....	14
<b>AS EXIGÊNCIAS LEGAIS TRAZIDAS PELA LGPD AO SETOR BANCÁRIO</b> .....	15
<b>AS BASES LEGAIS - O CONSENTIMENTO - ARTIGO 7º, I, DA LGPD</b> .....	17
<b>AS BASES LEGAIS - A EXECUÇÃO DE CONTRATO - ARTIGO 7º, V, DA LGPD</b> .....	19
<b>AS BASES LEGAIS - A PROTEÇÃO DO CRÉDITO - ARTIGO 7º, X, DA LGPD</b> .....	20
<b>AS BASES LEGAIS - CUMPRIMENTO DE OBRIGAÇÃO LEGAL - ARTIGO 7º, II, DA LGPD</b> .....	21
<b>O LEGÍTIMO INTERESSE UTILIZADO NA ATIVIDADE BANCÁRIA - UMA BASE LEGAL QUESTIONADA</b> .....	22
<b>OS PROCEDIMENTOS E AS OPÇÕES PRÁTICAS DE COMPLIANCE DISPONÍVEIS À IMPLEMENTAÇÃO DO TRATAMENTO DE DADOS AO SETOR BANCÁRIO - OS DESAFIOS</b> .....	23
<b>O ESTUDO DE CASO E A CRIAÇÃO DE UMA UNIDADE DE COMPLIANCE INDEPENDENTE</b> .....	24
<b>LEI Nº 13.709/2018 - LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS - LGPD</b> .....	27

## APRESENTAÇÃO

O estudo é dirigido ao compliance do setor bancário, para adaptação à Lei Geral de Proteção de Dados (LGPD). A área de compliance é essencial e obrigatória para as instituições financeiras e foi modificada pela LGPD, que impôs novas exigências para proteção de dados. A partir da vigência da nova lei, as empresas que coletam e mantêm dados em seus cadastros devem se reestruturar ou correm o risco de pagar multas de até cinquenta milhões de reais. O estudo apresenta as principais bases legais aplicadas aos agentes financeiros e, ao final, um projeto para a criação de uma nova coordenação na área de compliance para o setor bancário, que incorporou as inovações da LGPD e visa reduzir os riscos de danos administrativos, financeiros e reputacionais decorrentes das multas pelo descumprimento da lei.



## COMPLIANCE

Compliance pode ser conceituado como um conjunto de ações que visam garantir o cumprimento de normas legais e regulamentares, além de políticas e diretrizes de negócios e atividades empresariais e institucionais. Essas ações têm como objetivo evitar, detectar e solucionar desvios e inconformidades, buscando mitigar riscos legais/regulatórios e de reputação. O compliance é um modelo de gestão que tem origem no setor bancário, mas que hoje é amplamente aplicável em diversas áreas, como trabalhista, tributária, ambiental, entre outras. Um bom programa de compliance deve obedecer e especificar de forma clara as fases de implantação e consecução de seus objetos e objetivos. Além disso, a adoção de programas de integridade pode despertar confiança nos parceiros comerciais, consumidores, funcionários e colaboradores de uma organização. O CADE é uma autarquia federal que exerce em todo o território nacional a defesa da concorrência e dos direitos do consumidor, e tem como um de seus objetivos fomentar a cultura de compliance nas empresas brasileiras.



## **A LEI DE DADOS PESSOAIS EM UM PANORAMA GERAL E NO CONTEXTO HISTÓRICO**

O sistema brasileiro de proteção de dados seguiu o modelo europeu. As primeiras leis surgiram na Alemanha e na Suécia, ainda nas décadas de 1960 e 1970. Passados os anos, e diante de um mercado avassalador, inúmeros países passaram a legislar sobre a matéria, até que a União Europeia promulgou a Diretiva 95/46/CE, em 1995. A norma foi um marco no campo da proteção de dados, e dispôs sobre o tratamento de dados e direitos dos usuários em todos os países membros do bloco, colocando todos sob a mesma legislação (MONTEIRO et al., [2019]; PARLAMENTO EUROPEU, 1995). Esta norma vigorou até maio de 2018, quando entrou definitivamente em vigor o Regulamento nº 2016/679, de 27 abril de 2016, conhecido como General Data Protection Regulation (“GDPR”), a nova lei geral de proteção de dados da União Europeia. A GDPR é reconhecidamente a lei de maior proteção de dados pessoais do mundo. A sua rede de proteção se estende para além das fronteiras da União Europeia, e atinge dados de qualquer país que, de alguma forma, possui contato com o mercado europeu. No Brasil, diante de um novel e desconhecido cenário, a exemplo do resto do mundo, era premente a necessidade de uma legislação especial para tratamento e defesa deste novo patrimônio. A importância dos dados pessoais transcendeu ao aspecto meramente financeiro, dado à forma e a velocidade de como as informações passaram a circular, no mundo globalizado. E, assim, o contexto reclamou a edição de um novo arcabouço legal, que dessa efetiva proteção aos dados pessoais, e que passaram a

integrar, de forma efetiva, os direitos da personalidade, e por isso, tornaram-se vetores das vidas e das liberdades individuais, assim como da sociedade e da própria democracia (FRAZÃO, [2019b]). E é neste conturbado panorama, diante da mercantilização dos dados pessoais frente à extrema urgência de sua proteção, que surge, no ano de 2018, já com certo atraso, a Lei Federal 13.709.



## COMPLIANCE E AS INSTITUIÇÕES FINANCEIRAS

De acordo com Manzi (2008), o compliance teve origem nas instituições financeiras, com a criação do Banco Central Americano (*Board of Governors of the Federal Reserve*), em 1913. Logo após a quebra da Bolsa de Nova York de 1929, foi criada a política intervencionista *New Deal*, em uma tentativa de intervir na economia para “corrigir as distorções naturais do capitalismo”.

Também os escândalos que envolvem grandes bancos (Enron e a Lehman Brothers, no exterior, e o Banco Nacional e o Banestado, no Brasil, p. ex.), nos últimos anos, têm sido marcantes e atacam diretamente a reputação das empresas, causando impacto no valor de mercado das mesmas. Por esse motivo, o mercado regulatório e os órgãos de controle estatais entenderam a necessidade de implementação de instrumentos de governança e conformidade nas instituições financeiras, como órgãos obrigatórios, a fim de dinamizar os riscos do setor e minimizar os prejuízos. No Brasil, a Resolução BACEN 2554/1998 tornou obrigatória a implantação e implementação de controles internos nas instituições financeiras, independentemente do porte das mesmas, enquanto a Lei das Estatais (Lei Federal nº 13.303/2016) estabeleceu a obrigação dos estatutos das empresas públicas, economias mistas e suas respectivas subsidiárias observarem regras de governança corporativa, transparência e práticas de gestão de riscos e controle interno. Para além disso, a criação da Comissão de Valores Mobiliários (CVM), autarquia federal responsável por fiscalizar e desenvolver o mercado de valores mobiliários no país, influencia diretamente no controle das

Instituições Financeiras. Dentre as normas da CVM que tratam do compliance, destacam-se a Instrução CVM nº 586/2017 e a Instrução CVM nº 558/2015.

Outro fator preponderante, derivado de boa gestão de compliance aplicado às Instituições Financeiras, é a criação de uma estrutura de governança, direcionada ao suporte aos acionistas e outra de suporte à gestão. Esta última é formada pelo gerenciamento de risco, controles internos, compliance e jurídico. O compliance atua como órgão de suporte à gestão do Banco e à Alta Administração. O Instituto Brasileiro de Governança Corporativa (IBGC) define a governança corporativa como o sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre proprietários, Conselho de Administração, Diretoria e órgãos de controle. O compliance é um dos princípios básicos de governança corporativa, ao lado da transparência, equidade e prestação de contas. O modelo de compliance não deve ser restrito às assessorias jurídicas, mas sim integrado aos processos da empresa. O gestor do compliance deve garantir a adequação, o fortalecimento e o funcionamento do sistema de controles internos, disseminando a cultura de controles para assegurar o cumprimento das leis e regulamentos existentes. Como se vê, portanto, a conformidade tem ligação estreita com todos os demais atores dentro da Instituição, até em razão do controle e fiscalização exercidos, mesmo que em diferentes níveis. E, a verticalidade da atuação do compliance irá depender do quão longe quer chegar à empresa (do Banco, no caso), diante do cenário e objetivos delineados e frente a gestão e análise dos riscos do mercado



## COMPLIANCE E A INOVAÇÃO

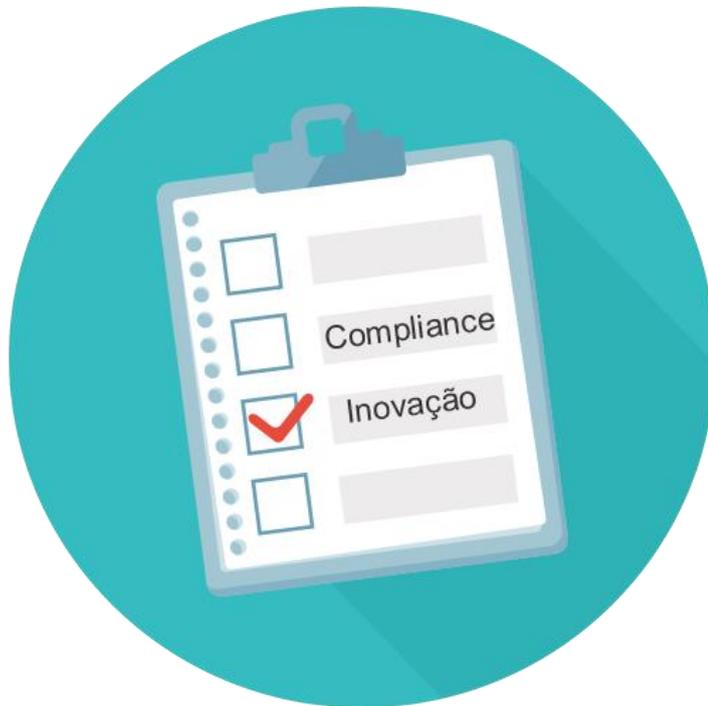
A inovação é a introdução de um bem ou serviço novo ou significativamente melhorado, no que se refere às suas características ou usos previstos, ou ainda, à implementação de métodos ou processos de produção, distribuição, marketing ou organizacionais novos ou significativamente melhorados (MANUAL DE OSLO. OCDE, 2004).

O compliance, no Brasil, ainda é embrionário. Iniciou-se, timidamente, nos anos 1990, com modelos estrangeiros. E, ao certo, para tomar fôlego e gerar resultados, depende de um processo crucial de aculturação tanto das empresas quanto dos empregados nos tempos atuais. (SAMPAIO, 2019). No cenário legal, normativo, a conformidade ganhou força com a edição da Lei Federal 12.846/2013, a qual dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, a chamada Lei anticorrupção.

Inovar, oportunizar o crescimento da empresa, mas de forma organizada, sustentável e em conformidade. Este é o desafio das organizações, hodiernamente, e aqui o compliance e a inovação se entrelaçam. Para Doyle et al, 2019, a sustentabilidade é abordada no contexto amplamente definido, ou seja, baseia-se na capacidade de uma organização equilibrar as necessidades de curto e longo prazo das partes interessadas.

Crescer, inovar, mas com responsabilidade e em conformidade: esta é a pedra nevrálgica do sistema atual. Por isso, o compliance e toda sua rede é o assunto dominante, atualmente, no mundo corporativo. A gestão e o

cumprimento das normas devem estar alinhados aos objetivos finalísticos da organização, e não ser enxergado, dentro e fora da empresa, como um fator inibidor da inovação ou até mesmo bloqueador no âmbito comercial em detrimento do grau de cumprimento e exigências legais e normativas (GIOVANINI, 2014).



## COMPLIANCE E A LGPD

A cultura da conformidade nas grandes corporações, no Brasil, a Lei Anticorrupção e a Lei Geral de Proteção de Dados (LGPD) têm incentivado a aplicação de instrumentos de compliance nas empresas. A LGPD estabelece a obrigação de todas as empresas, públicas ou privadas, garantir a governança das informações e dados pessoais que detêm, e pune severamente eventuais vazamentos ou espoliações desses dados. Para cumprir a LGPD, as empresas precisam reestruturar seus sistemas normativos internos, revisar as rotinas dos processos internos e o tráfego dos dados de acordo com o tratamento exigido pela norma, o que pode ser garantido ou ter seus efeitos mitigados através da aplicação de um rígido modelo de compliance. Daí a importância de as instituições financeiras aprimorarem a rotina do tratamento de dados pessoais, pois a má gestão desses dados pode desaguar em um descumprimento legal em cascata e consequências imprevisíveis à empresa. Os autores comentados no texto defendem que a adoção de mecanismos de compliance é um valioso instrumento para a promoção de condutas compatíveis com a regulamentação legal e para a efetividade dos direitos e prevenção de danos.



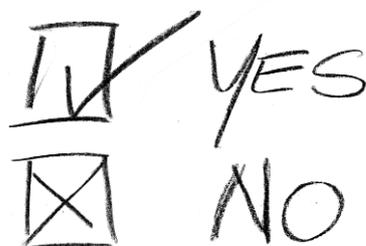


## **AS EXIGÊNCIAS LEGAIS TRAZIDAS PELA LGPD AO SETOR BANCÁRIO**

A LGPD regula a coleta, o tratamento, o armazenamento e o compartilhamento de dados pessoais, e as instituições financeiras devem seguir as normas estabelecidas. Na classificação feita pela Lei, os dados bancários, em regra, não são classificados como sensíveis, situação que afasta a exigência, em geral, do consentimento do proprietário para a coleta e o tratamento do dado. Isso não afasta a necessidade e a prudência do agente financeiro em, sempre que possível, tomar a anuência do proprietário ao coletar e manipular seus dados. Importante esclarecer, também, a existência de outras legislações extravagantes que, somadas à LGPD, impõem às Instituições Financeiras obrigações e exigências no tratamento de informações desta natureza, tais como a Lei 4.595/64 (Lei do Mercado Financeiro), e a Lei Complementar 105/2001, conhecida como a Lei do Sigilo Bancário e a prevenção à lavagem de dinheiro. Assim, as Instituições Financeiras tratam dos dados pessoais, assim definidos aqueles insertos no artigo 5º, I, da LGPD. Nessa grande plêiade normativa, a LGPD traz em seu bojo normas gerais, aplicadas indistintamente a todos os destinatários, e outras específicas, identificadas e aplicadas ao diretamente ao setor bancário, no tratamento de dados dos clientes, dos fornecedores, empregados, terceirizados e afins. A LGPD, assim como uma parte considerável das leis, traz em seu bojo normas regras gerais, normas programáticas e princípios, os quais, em que pese um alto grau de abstração,

orientam a aplicação da lei e devem ser rigorosamente seguidos pelos destinatários. Esta cartilha apresenta, em resumo, as normas aplicadas na atividade primária dos agentes financeiros, que é na concessão do crédito. E, em seguida, de que forma o setor de compliance, do agente bancário, pode garantir o efetivo cumprimento das exigências da LGPD, mitiga-lo. Nesse contexto, destacam-se 03 (três) bases legais aplicadas aos agentes financeiros para o tratamento de dados pessoais, previstas no art. 7º da Lei 13.709/2018: fornecimento de consentimento pelo titular, necessidade para a execução de contrato ou procedimentos preliminares, e proteção do crédito. Além disso, as medidas tomadas pelas instituições financeiras para avaliar a capacidade de crédito do cliente e as bases legais que justificam o tratamento de seus dados pessoais durante esse processo.

## **AS BASES LEGAIS - O CONSENTIMENTO - ARTIGO 7º, I, DA LGPD**



O consentimento como base legal para o tratamento de dados pessoais pelo Banco, com base no artigo 7º, inciso I, da LGPD. A análise dos princípios da LGPD revela a preocupação do legislador com a participação do indivíduo no fluxo de suas informações, reforçando a ideia e importância do consentimento. O consentimento é definido como uma manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. No caso dos bancos, o consentimento assume uma importância destacada, dado ao amplo e propagado direito à informação e às normas do Código de Defesa do Consumidor. A revogação do consentimento, em casos de contratos bancários, não pode ser realizada por ato unilateral do titular, e este deverá buscar uma declaração judicial, desde que comprovada a infração contratual da Instituição Financeira.

**Tabela – Bases Legais da LGPD**

<b>HIPÓTESES DE TRATAMENTO DE DADOS</b>	<b>DEFINIÇÃO</b>	<b>BASE LEGAL</b>
Consentimento do titular	Consentimento para tratamento dos dados pessoais deverá ser livre e inequívoco	art 7, I, LGPD
Cumprimento de obrigação legal ou regulatória	Pode ocorrer por força de lei anterior ou para garantir a ordem e segurança social	art 7, II, LGPD
Uso compartilhado de dados pela administração pública	Feito com a finalidade específica da execução de política pública formalmente instituída por Lei ou Ato administrativo.	art 7, III, LGPD
Realização de estudos e pesquisas	Tratamento para pesquisas ou estudos para saúde pública ou programas de governo	art 7, IV, LGPD
Execução ou preparação de contrato	Fazer parte de contrato consentimento específico do titular para utilização de <b>negócio jurídico em que seja parte</b>	art 7, V, LGPD
Exercício de direitos em processos judicial, administrativo ou arbitral	Feito com a finalidade específica de lei anterior ou para garantir a ordem e segurança social	art 7, VI, LGPD
Proteção da vida ou da incolumidade física	Tratamento de dados em favor do titular do dado em casos de necessidade de tutela do bem maior da pessoa natural	Art. 7, VII, LGPD
Tutela da saúde do titular	Única hipótese de tratamento de dado manejado por agente exclusivo profissional de saúde, serviços de saúde ou autoridade sanitária	Art. 7, VIII, LGPD
Legítimo interesse	Previsão geral e subsidiária mediante previa e expressa motivação pelo controlador da finalidade e necessidade (legítimo interesse) do tratamento	Art 7. IX, LGPD
Proteção do crédito	Tratamento para proteção e manutenção do crédito	Art. 7. X, LGPD

Fonte: (10 BASES..., 2020).

## **AS BASES LEGAIS - A EXECUÇÃO DE CONTRATO - ARTIGO 7º, V, DA LGPD**

Segunda base legal prevista no artigo 7º, V, da Lei Geral de Proteção de Dados (LGPD) para a utilização de dados pelas Instituições Financeiras, que permite o tratamento de dados pessoais 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. Essa base legal assemelha-se ao consentimento, na medida em que o proprietário já é contratante ou pretende formalizar um contrato, onde será necessário o fornecimento de seus dados ao controlador. O texto discute a possibilidade de colheita e tratamento de dados sem consentimento, mas ressalta a importância de obter autorização prévia do cliente para formação do cadastro e análise dos dados financeiros como condição pré-contratual. O tratamento de dados financeiros merece análise e tratamento diferenciado, devido à sua importância e à legislação vigente.



## **AS BASES LEGAIS - A PROTEÇÃO DO CRÉDITO - ARTIGO 7º, X, DA LGPD**

A terceira base legal prevista no artigo 7º, X, da Lei Geral de Proteção de Dados (LGPD), que permite o tratamento de dados para a proteção do crédito. Essa base legal tem o objetivo de ampliar e facilitar a concessão de crédito e melhorar a análise de riscos pelas instituições financeiras. A proteção do crédito abrange a avaliação da capacidade de pagamento e da probabilidade de inadimplência do indivíduo, o que ajuda a mitigar os riscos da concessão de crédito. O texto destaca a importância de integrar a LGPD com a legislação referente à proteção do crédito, como o Código de Defesa do Consumidor e a Lei do Cadastro Positivo. A prevenção de fraudes é outro aspecto importante dessa base legal, pois permite às empresas de crédito controlar possíveis fraudadores e a indústria dos documentos falsos.



## **AS BASES LEGAIS - CUMPRIMENTO DE OBRIGAÇÃO LEGAL - ARTIGO 7º, II, DA LGPD**

A quarta base legal permitida pela LGPD para a utilização pelas Instituições Financeiras, que é a utilização em casos de cumprimento de uma obrigação decorrente de lei. Essa base legal é importante para as instituições financeiras, pois a evolução das legislações de controle de capitais e evasão de divisas criaram obrigações cujo descumprimento leva a graves sanções. A Lei 9.613/1998, por exemplo, obriga os bancos a notificar o COAF sempre que identificarem transações com indícios de lavagem de dinheiro, financiamento de atividades terroristas ou outras práticas ilícitas previstas em lei. Quando existe uma obrigação legal, a base a ser utilizada é o artigo 7º, II, da LGPD, que dispensa o consentimento do titular.



## O LEGÍTIMO INTERESSE UTILIZADO NA ATIVIDADE BANCÁRIA - UMA BASE LEGAL QUESTIONADA

A utilização da base legal do Legítimo Interesse na atividade bancária, prevista no artigo 10 da Lei Geral de Proteção de Dados (LGPD). Esta base legal só pode ser utilizada para finalidades legítimas, considerando as situações concretas, e o controlador deve adotar medidas para garantir a transparência do tratamento dos dados baseado em seu legítimo interesse. Para utilizar essa base legal, o controlador deve realizar o chamado *legitimate interest assessment* (LIA), que avalia os interesses legítimos do controlador e o impacto sobre o titular dos dados, equilibrando os interesses e protegendo o titular dos dados de impactos indesejados. A utilização dessa base legal deve cumprir as expectativas dos interesses do titular





## **OS PROCEDIMENTOS E AS OPÇÕES PRÁTICAS DE COMPLIANCE DISPONÍVEIS À IMPLEMENTAÇÃO DO TRATAMENTO DE DADOS AO SETOR BANCÁRIO - OS DESAFIOS**

O compliance (conformidade e integridade) como órgão de governança obrigatório dentro das Instituições Financeiras. Embora não haja uma obrigatoriedade legal de criação de um setor de conformidade, a prática é incentivada como forma de prevenir infrações ou minimizar seus danos, caso ocorridos. Com a criação da Lei Geral de Proteção de Dados (LGPD), torna-se ainda mais importante a criação de um setor de regulação interno, que atue de forma concreta e efetiva, minimizando as chances de ocorrência de ilícitos e a aplicação das penalidades existentes na norma. O programa de compliance deve iniciar com a identificação precisa dos riscos da atividade e mapear eventuais gargalos quanto a hipóteses de descumprimento das normas, através de mecanismos de gestão e de forma pretérita.

## **O ESTUDO DE CASO E A CRIAÇÃO DE UMA UNIDADE DE COMPLIANCE INDEPENDENTE**

A instituição de um sistema de compliance é obrigatório dentro de toda e qualquer Instituição Financeira, a rigor do artigo 2º, da Resolução 4.595/2017, do Banco Central do Brasil, e, para o caso dos Bancos Públicos, pela Lei das Estatais.

A Lei Geral de Proteção de Dados trouxe uma grande leva de conceitos, normas abertas e de aplicação indefinida, um novo marco regulatório, que, inclusive, para fiscalização de eventuais desajustes e irregularidades, criou uma Agência Reguladora, no caso a ANPD. Nesse contexto, um setor de regulação interno, nas veias da organização, que atue de forma concreta e efetiva, certamente minimiza as chances de ocorrência de ilícitos e a aplicação das severas penalidades existentes na norma.

No estudo de caso apresentado de forma paralela à esta Cartilha, demonstrou-se, ao analisar a estrutura interna de uma Instituição Financeira, a ausência de um órgão específico de compliance para a gerência e o controle dos dados, a partir das obrigações advindas da LGPD. As áreas de conformidade do Agente Financeiro avaliado funcionam de maneira efetiva. Prova disso são os índices de conformidade atingidos pela Instituição, seja em processos internos seja naqueles envolvendo terceiros, e, principalmente, na atuação junto ao público alvo, que é a venda de produtos e serviços. Todavia, não há um órgão/setor no Banco junto ao compliance responsável, especificamente, pelo controle e aplicação específica das normas da Lei 13.709/2018.

Neste particular apontou-se um novo modelo de solução: pela envergadura e importância da LGPD, através das normas e obrigações previstas na Lei 13.709/2018, a propôs-se a criação de uma nova Coordenadoria, para análise, fiscalização e aplicabilidade da lei. Com efeito, um órgão estritamente ligado à área gera o aprimoramento do sistema de compliance, especificamente ligado à atividade de coleta e controle, e o sigilo e a confidencialidade do processamento e armazenamento dos dados. E, neste ponto, a criação de uma Coordenadoria própria, e independente, unicamente ligada à proteção de dados (LGPD), será ponto fundamental para aperfeiçoar o sistema de controle e mitigar os riscos, principalmente face às multas milionárias previstas na legislação.

Um órgão específico e individualizado, unicamente ligado à gestão e controle dos dados, poderá concentrar-se em atividades coordenadas para controlar e monitorar todos os processos da Instituição Financeira que envolvam a coleta e a segurança dos dados, objetivo maior da LGPD. Uma Coordenação de Compliance ligada à LGPD poderá criar mecanismos de gestão, com origem desde às agências da rede bancária, na ponta da Instituição, onde geralmente a coleta dos dados se inicia, até o destino final, com o Operador e o Controlador dos dados.

A gestão dos dados pessoais e a própria gestão do compliance justificam referida criação, na medida em que o risco das sanções legais, decorrentes da Lei 13.709/2018, vão muito além das perdas financeiras. Há o risco, iminente, das perdas reputacionais derivadas da falta de cumprimento das Leis e normas regulamentadoras, e a perda da credibilidade junto ao mercado.

Atualmente, o mercado, principalmente o financeiro, exige do Banco um cumprimento estrito de princípios e condutas éticas, e a política de integridade e conformidade nos negócios recebe um grau máximo de controle, o que, também, justifica ao nosso ver a criação da referida unidade independente.





# LEI Nº 13.709/2018 - LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS - LGPD

**O PRESIDENTE DA REPÚBLICA** Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

## CAPÍTULO I

### DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, 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 e o livre desenvolvimento da personalidade da pessoa natural.

Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. [\(Incluído pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

I - o respeito à privacidade;

II - a autodeterminação informativa;

III - a liberdade de expressão, de informação, de comunicação e de opinião;

IV - a inviolabilidade da intimidade, da honra e da imagem;

V - o desenvolvimento econômico e tecnológico e a inovação;

VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Art. 3º Esta Lei aplica-se 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, desde que:

I - a operação de tratamento seja realizada no território nacional;

~~II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;~~

~~II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou~~ [\(Redação dada pela Medida Provisória nº 869, de 2018\)](#)

II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou [\(Redação dada pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

§ 2º Exceção-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:

I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

II - realizado para fins exclusivamente:

a) jornalístico e artísticos; ou

b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;

b) acadêmicos; [\(Redação dada pela Medida Provisória nº 869, de 2018\)](#)

b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;

III - realizado para fins exclusivos de:

a) segurança pública;

b) defesa nacional;

c) segurança do Estado; ou

d) atividades de investigação e repressão de infrações penais; ou

IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

~~§ 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.~~

~~§ 2º O tratamento dos dados a que se refere o inciso III do caput por pessoa jurídica de direito privado só será admitido em procedimentos sob a tutela de pessoa jurídica de direito público, hipótese na qual será observada a limitação de que trata o § 3º.~~ [\(Redação dada pela Medida Provisória nº 869, de 2018\)](#)

§ 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.

~~§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.~~

~~§ 3º Os dados pessoais constantes de bancos de dados constituídos para os fins de que trata o inciso III do caput não poderão ser tratados em sua totalidade por pessoas jurídicas de direito privado, não incluídas as controladas pelo Poder Público.~~ [\(Redação dada pela Medida Provisória nº 869, de 2018\)](#)

§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.

~~§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado.~~ [\(Revogado pela Medida Provisória nº 869, de 2018\)](#)

§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público. [\(Redação dada pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

~~VIII - encarregado: pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional;~~

~~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;~~ [\(Redação dada pela Medida Provisória nº 869, de 2018\)](#)

VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); [\(Redação dada pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

IX - agentes de tratamento: o controlador e o operador;

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

XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

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 públicos 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;

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;

~~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;~~

~~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; e [\(Redação dada pela Medida Provisória nº 869, de 2018\)](#)~~

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; e [\(Redação dada pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

~~XIX - autoridade nacional: órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento desta Lei.~~

~~XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei. [\(Redação dada pela Medida Provisória nº 869, de 2018\)](#)~~

XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. [\(Redação dada pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

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.

## CAPÍTULO II

### DO TRATAMENTO DE DADOS PESSOAIS

#### Seção I

##### **Dos Requisitos para o Tratamento de Dados Pessoais**

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 terceiro;

~~VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;~~

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; [\(Redação dada pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, 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 Nos casos de aplicação do disposto nos incisos II e III do caput deste artigo e excetuadas as hipóteses previstas no art. 4º desta Lei, o titular será informado das hipóteses em que será admitido o tratamento de seus dados. [\(Revogado pela Medida Provisória nº 869, de 2018\)](#)~~

~~§ 1º~~ [\(Revogado\)](#). [\(Redação dada pela Lei nº 13.853, de 2019\)](#)

~~§ 2º A forma de disponibilização das informações previstas no § 1º e no inciso I do caput do art. 23 desta Lei poderá ser especificada pela autoridade nacional. [\(Revogado pela Medida Provisória nº 869, de 2018\)](#)~~

~~§ 2º~~ [\(Revogado\)](#). [\(Redação dada pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

§ 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. [\(Incluído pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.

§ 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

§ 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.

§ 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

§ 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.

§ 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

I - finalidade específica do tratamento;

II - forma e duração do tratamento, observados os segredos comercial e industrial;

III - identificação do controlador;

IV - informações de contato do controlador;

V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

VI - responsabilidades dos agentes que realizarão o tratamento; e

VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

§ 1º Na hipótese em que o consentimento é requerido, esse 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.

§ 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

§ 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.

Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I - apoio e promoção de atividades do controlador; e

II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

## Seção II

### Do Tratamento de Dados Pessoais Sensíveis

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da [Lei nº 9.307, de 23 de setembro de 1996 \(Lei de Arbitragem\)](#);

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

~~f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou~~

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou [\(Redação dada pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

§ 2º Nos casos de aplicação do disposto nas alíneas "a" e "b" do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.

§ 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.

~~§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nos casos de portabilidade de dados quando consentido pelo titular.~~

~~§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses de: — [\(Redação dada pela Medida Provisória nº 869, de 2018\)](#)~~

~~I — portabilidade de dados quando consentido pelo titular; ou — [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)~~

~~II — necessidade de comunicação para a adequada prestação de serviços de saúde suplementar. — [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)~~

§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: [\(Redação dada pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

I - a portabilidade de dados quando solicitada pelo titular; ou [\(Incluído pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo. [\(Incluído pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

§ 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários. [\(Incluído pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

§ 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

§ 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.

Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

§ 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais.

§ 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro.

§ 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.

§ 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

### **Seção III**

#### **Do Tratamento de Dados Pessoais de Crianças e de Adolescentes**

Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

§ 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.

§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.

§ 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

§ 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.

§ 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

### **Seção IV**

#### **Do Término do Tratamento de Dados**

Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

II - fim do período de tratamento;

III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou

IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

I - cumprimento de obrigação legal ou regulatória pelo controlador;

II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou

IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

## CAPÍTULO

III

### DOS DIREITOS DO TITULAR

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 e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;~~

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; ([Redação dada pela Lei nº 13.853, de 2019](#)) [Vigência](#)

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. ([Redação dada pela Lei nº 13.853, de 2019](#)) [Vigência](#)

§ 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

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 revisão, por pessoa natural, de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive de decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.~~

~~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. (Redação dada pela Medida Provisória nº 869, de 2018).~~

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. (Redação dada pela Lei nº 13.853, de 2019) Vigência

§ 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). (Incluído pela Lei nº 13.853, de 2019) Vigência

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.

CAPÍTULO

IV

DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

### Seção I

#### Das Regras

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 interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;

II - (VETADO); e

~~III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei.~~

III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e (Redação dada pela Lei nº 13.853, de 2019) Vigência

IV - (VETADO). (Incluído pela Lei nº 13.853, de 2019) Vigência

§ 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento.

§ 2º O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no caput deste artigo de instituir as autoridades de que trata a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

§ 3º Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data), da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo), e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

§ 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei.

§ 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo.

Art. 24. As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.

Parágrafo único. As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos deste Capítulo.

Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:

I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na [Lei nº 12.527, de 18 de novembro de 2011 \(Lei de Acesso à Informação\)](#);

II - (VETADO);

~~III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.~~

~~III - se for indicado um encarregado para as operações de tratamento de dados pessoais, nos termos do art. 39; [Redação dada pela Medida Provisória nº 869, de 2018](#)~~

III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.

~~IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneros; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)~~

~~V - na hipótese de a transferência dos dados objetivar a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados; ou [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)~~

IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneros; ou [\(Incluído pela Lei nº 13.853, de 2019\)](#)

V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades. [\(Incluído pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

~~VI - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)~~

§ 2º Os contratos e convênios de que trata o § 1º deste artigo deverão ser comunicados à autoridade nacional.

Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto:

~~Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa jurídica de direito privado dependerá de consentimento do titular, exceto: [\(Redação dada pela Medida Provisória nº 869, de 2018\)](#)~~

Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto:

I - nas hipóteses de dispensa de consentimento previstas nesta Lei;

II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; ou

III - nas exceções constantes do § 1º do art. 26 desta Lei.

Parágrafo único. A informação à autoridade nacional de que trata o caput deste artigo será objeto de regulamentação. [\(Incluído pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

Art. 28. (VETADO).

~~Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, às entidades do Poder Público, a realização de operações de tratamento de dados pessoais, informe específico sobre o âmbito e a natureza dos dados e demais detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei.~~

~~Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do Poder Público a realização de operações de tratamento de dados pessoais, as informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei. [\(Redação dada pela Medida Provisória nº 869, de 2018\)](#)~~

Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do poder público a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei. [\(Redação dada pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

Art. 30. A autoridade nacional poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais.

## Seção II Da Responsabilidade

Art. 31. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.

Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

## CAPÍTULO V DA TRANSFERÊNCIA INTERNACIONAL DE DADOS

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.

Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do [art. 1º da Lei nº 12.527, de 18 de novembro de 2011 \(Lei de Acesso à Informação\)](#), no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.

Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do caput do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração:

I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;

II - a natureza dos dados;

III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;

IV - a adoção de medidas de segurança previstas em regulamento;

V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e

VI - outras circunstâncias específicas relativas à transferência.

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.

§ 2º Na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação da autoridade nacional, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento, quando necessário.

§ 3º A autoridade nacional poderá designar organismos de certificação para a realização do previsto no caput deste artigo, que permanecerão sob sua fiscalização nos termos definidos em regulamento.

§ 4º Os atos realizados por organismo de certificação poderão ser revistos pela autoridade nacional e, caso em desconformidade com esta Lei, submetidos a revisão ou anulados.

§ 5º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no caput deste artigo serão também analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos §§ 1º e 2º do art. 46 desta Lei.

Art. 36. As alterações nas garantias apresentadas como suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no inciso II do art. 33 desta Lei deverão ser comunicadas à autoridade nacional.

## CAPÍTULO VI DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS

### Seção I

#### Do Controlador e do Operador

Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

Art. 40. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.

## Seção II

### Do Encarregado pelo Tratamento de Dados Pessoais

Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

§ 2º As atividades do encarregado consistem em:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - receber comunicações da autoridade nacional e adotar providências;

III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

§ 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

§ 4º [\(VETADO\)](#). [\(Incluído pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

## Seção III

### Da Responsabilidade e do Ressarcimento de Danos

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:

I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

§ 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

§ 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.

§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

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 terceiro.

Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

I - o modo pelo qual é realizado;

II - o resultado e os riscos que razoavelmente dele se esperam;

III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.

## CAPÍTULO VII

### DA SEGURANÇA E DAS BOAS PRÁTICAS

## **Seção I**

### **Da Segurança e do Sigilo de Dados**

Art. 46. Os agentes de tratamento 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.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

Art. 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.

§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso de a comunicação não ter sido imediata; e

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

§ 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:

I - ampla divulgação do fato em meios de comunicação; e

II - medidas para reverter ou mitigar os efeitos do incidente.

§ 3º No juízo de gravidade do 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 terceiros não autorizados a acessá-los.

Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

## **Seção II**

### **Das Boas Práticas e da Governança**

Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

I - implementar programa de governança em privacidade que, no mínimo:

a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

g) conte com planos de resposta a incidentes e remediação; e

h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.

§ 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.

## CAPÍTULO VIII DA FISCALIZAÇÃO

### Seção I

#### Das Sanções Administrativas

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: [\(Vigência\)](#)

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração;

VII - (VETADO);

VIII - (VETADO);

IX - (VETADO).

X - ~~(VETADO);~~ [\(Incluído pela Lei nº 13.853, de 2019\)](#); [\(Promulgação partes vetadas\)](#)

XI - ~~(VETADO);~~ [\(Incluído pela Lei nº 13.853, de 2019\)](#); [\(Promulgação partes vetadas\)](#)

XII - ~~(VETADO);~~ [\(Incluído pela Lei nº 13.853, de 2019\)](#); [\(Promulgação partes vetadas\)](#)

X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

§ 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:

I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;

II - a boa-fé do infrator;

III - a vantagem auferida ou pretendida pelo infrator;

IV - a condição econômica do infrator;

V - a reincidência;

VI - o grau do dano;

VII - a cooperação do infrator;

VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;

IX - a adoção de política de boas práticas e governança;

X - a pronta adoção de medidas corretivas; e

XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

~~§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas em legislação específica.~~

§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990, e em legislação específica. [\(Redação dada pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

~~§ 3º O disposto nos incisos I, IV, V, VI, VII, VIII e IX do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na [Lei nº 8.112, de 11 de dezembro de 1990 \(Estatuto do Servidor Público Federal\)](#), na [Lei nº 8.429, de 2 de junho de 1992 \(Lei de Improbidade Administrativa\)](#), e na [Lei nº 12.527, de 18 de novembro de 2011 \(Lei de Acesso à Informação\)](#).~~

§ 3º O disposto nos incisos I, IV, V, VI, X, XI e XII do **caput** deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na [Lei nº 8.112, de 11 de dezembro de 1990](#), na [Lei nº 8.429, de 2 de junho de 1992](#), e na [Lei nº 12.527, de 18 de novembro de 2011](#). [\(Redação dada pela Lei nº 13.853, de 2019\)](#)

§ 4º No cálculo do valor da multa de que trata o inciso II do caput deste artigo, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea.

§ 5º O produto da arrecadação das multas aplicadas pela ANPD, inscritas ou não em dívida ativa, será destinado ao Fundo de Defesa de Direitos Difusos de que tratam o art. 13 da Lei nº 7.347, de 24 de julho de 1985, e a Lei nº 9.008, de 21 de março de 1995. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

~~§ 6º (VETADO). — (Incluído pela Lei nº 13.853, de 2019) [\(Promulgação partes vetadas\)](#)~~

§ 6º As sanções previstas nos incisos X, XI e XII do **caput** deste artigo serão aplicadas: [\(Incluído pela Lei nº 13.853, de 2019\)](#)

I - somente após já ter sido imposta ao menos 1 (uma) das sanções de que tratam os incisos II, III, IV, V e VI do **caput** deste artigo para o mesmo caso concreto; e [\(Incluído pela Lei nº 13.853, de 2019\)](#)

II - em caso de controladores submetidos a outros órgãos e entidades com competências sancionatórias, ouvidos esses órgãos. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

§ 7º Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo. [\(Incluído pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

Art. 53. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa. [\(Vigência\)](#)

§ 1º As metodologias a que se refere o caput deste artigo devem ser previamente publicadas, para ciência dos agentes de tratamento, e devem apresentar objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa, que deverão conter fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos nesta Lei.

§ 2º O regulamento de sanções e metodologias correspondentes deve estabelecer as circunstâncias e as condições para a adoção de multa simples ou diária.

Art. 54. O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional.

Parágrafo único. A intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento. [\(Vigência\)](#)

## CAPÍTULO IX

### DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE

#### Seção I

##### Da Autoridade Nacional de Proteção de Dados (ANPD)

Art. 55. (VETADO).

~~Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados – ANPD, órgão da administração pública federal, integrante da Presidência da República. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)~~

~~Art. 55-B. É assegurada autonomia técnica à ANPD. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)~~

~~Art. 55-C. ANPD é composta por: [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)~~

~~I – Conselho Diretor, órgão máximo de direção; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)~~

~~II – Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)~~

~~III – Corregedoria; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)~~

~~IV – Ouvidoria; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)~~

~~V – órgão de assessoramento jurídico próprio; e [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)~~

~~VI – unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei.” [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)~~

~~Art. 55-D. O Conselho Diretor da ANPD será composto por cinco diretores, incluído o Diretor-Presidente. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)~~

§ 1º Os membros do Conselho Diretor da ANPD serão nomeados pelo Presidente da República e ocuparão cargo em comissão do Grupo Direção e Assessoramento Superior – DAS de nível 5. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

§ 2º Os membros do Conselho Diretor serão escolhidos dentre brasileiros, de reputação ilibada, com nível superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

§ 3º O mandato dos membros do Conselho Diretor será de quatro anos. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

§ 4º Os mandatos dos primeiros membros do Conselho Diretor nomeados serão de dois, de três, de quatro, de cinco e de seis anos, conforme estabelecido no ato de nomeação. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

§ 5º Na hipótese de vacância do cargo no curso do mandato de membro do Conselho Diretor, o prazo remanescente será completado pelo sucessor. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

Art. 55-E. Os membros do Conselho Diretor somente perderão seus cargos em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

§ 1º Nos termos do **caput**, cabe ao Ministro de Estado Chefe da Casa Civil da Presidência da República instaurar o processo administrativo disciplinar, que será conduzido por comissão especial constituída por servidores públicos federais estáveis. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

§ 2º Compete ao Presidente da República determinar o afastamento preventivo, caso necessário, e proferir o julgamento. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

Art. 55-F. Aplica-se aos membros do Conselho Diretor, após o exercício do cargo, o disposto no [art. 6º da Lei nº 12.813, de 16 de maio de 2013](#). [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

Parágrafo único. A infração ao disposto no **caput** caracteriza ato de improbidade administrativa. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

Art. 55-G. Ato do Presidente da República disporá sobre a estrutura regimental da ANPD. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

Parágrafo único. Até a data de entrada em vigor de sua estrutura regimental, a ANPD receberá o apoio técnico e administrativo da Casa Civil da Presidência da República para o exercício de suas atividades. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

Art. 55-H. Os cargos em comissão e as funções de confiança da ANPD serão remanejados de outros órgãos e entidades do Poder Executivo federal. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

Art. 55-I. Os ocupantes dos cargos em comissão e das funções de confiança da ANPD serão indicados pelo Conselho Diretor e nomeados ou designados pelo Diretor-Presidente. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

Art. 55-J. Compete à ANPD: [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

I – zelar pela proteção dos dados pessoais; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

II – editar normas e procedimentos sobre a proteção de dados pessoais; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

III – deliberar, na esfera administrativa, sobre a interpretação desta Lei, suas competências e os casos omissos; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

IV – requisitar informações, a qualquer momento, aos controladores e operadores de dados pessoais que realizem operações de tratamento de dados pessoais; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

V – implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

VI – fiscalizar e aplicar sanções na hipótese de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

VII – comunicar às autoridades competentes as infrações penais das quais tiver conhecimento; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

VIII – comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei praticado por órgãos e entidades da administração pública federal; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

IX – difundir na sociedade o conhecimento sobre as normas e as políticas públicas de proteção de dados pessoais e sobre as medidas de segurança; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

X – estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle e proteção dos titulares sobre seus dados pessoais, consideradas as especificidades das atividades e o porte dos controladores; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

XI – elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

XII – promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

XIII — realizar consultas públicas para colher sugestões sobre temas de relevante interesse público na área de atuação da ANPD; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

XIV — realizar, previamente à edição de resoluções, a oitiva de entidades ou órgãos da administração pública que sejam responsáveis pela regulação de setores específicos da atividade econômica; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

XV — articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

XVI — elaborar relatórios de gestão anuais acerca de suas atividades. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

§ 1º A ANPD, na edição de suas normas, deverá observar a exigência de mínima intervenção, assegurados os fundamentos e os princípios previstos nesta Lei e o disposto no art. 170 da Constituição. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

§ 2º A ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados, conforme legislação específica, e o tratamento de dados pessoais, na forma desta Lei. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

§ 3º A ANPD manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública que sejam responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar as competências regulatória, fiscalizatória e punitiva da ANPD. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

§ 4º No exercício das competências de que trata o **caput**, a autoridade competente deverá zelar pela preservação do segredo empresarial e do sigilo das informações, nos termos da lei, sob pena de responsabilidade. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

§ 5º As reclamações colhidas conforme o disposto no inciso V do **caput** poderão ser analisadas de forma agregada e as eventuais providências delas decorrentes poderão ser adotadas de forma padronizada. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, cujas demais competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

Parágrafo único. A ANPD articulará sua atuação com o Sistema Nacional de Defesa do Consumidor do Ministério da Justiça e com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais, e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

§ 1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República. [\(Incluído pela Lei nº 13.853, de 2019\)](#) [\(Revogado pela Medida Provisória nº 1.124, de 2022\)](#) [\(Revogado pela Lei nº 14.460, de 2022\)](#)

§ 2º A avaliação quanto à transformação de que dispõe o § 1º deste artigo deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD. [\(Incluído pela Lei nº 13.853, de 2019\)](#) [\(Revogado pela Medida Provisória nº 1.124, de 2022\)](#) [\(Revogado pela Lei nº 14.460, de 2022\)](#)

§ 3º O provimento dos cargos e das funções necessários à criação e à atuação da ANPD está condicionado à expressa autorização física e financeira na lei orçamentária anual e à permissão na lei de diretrizes orçamentárias. [\(Incluído pela Lei nº 13.853, de 2019\)](#) [\(Revogado pela Medida Provisória nº 1.124, de 2022\)](#) [\(Revogado pela Lei nº 14.460, de 2022\)](#)

Art. 55-A. Fica criada a Autoridade Nacional de Proteção de Dados – ANPD, autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal. [\(Redação dada pela Medida Provisória nº 1.124, de 2022\)](#)

Art. 55-A. Fica criada a Autoridade Nacional de Proteção de Dados (ANPD), autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal. [\(Redação dada pela Lei nº 14.460, de 2022\)](#)

Art. 55-B. É assegurada autonomia técnica e decisória à ANPD. [\(Incluído pela Lei nº 13.853, de 2019\)](#) [\(Revogado pela Medida Provisória nº 1.124, de 2022\)](#) [\(Revogado pela Lei nº 14.460, de 2022\)](#)

Art. 55-C. A ANPD é composta de: [\(Incluído pela Lei nº 13.853, de 2019\)](#)

I - Conselho Diretor, órgão máximo de direção; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

II - Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

III - Corregedoria; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

- IV - Ouvidoria; [\(Incluído pela Lei nº 13.853, de 2019\)](#)
- ~~V - órgão de assessoramento jurídico próprio; e [\(Incluído pela Lei nº 13.853, de 2019\)](#)~~
- ~~V - Procuradoria; e [\(Redação dada pela Medida Provisória nº 1.124, de 2022\)](#)~~
- V - (revogado); [\(Redação dada pela Lei nº 14.460, de 2022\)](#)
- V-A - Procuradoria; e [\(Incluído pela Lei nº 14.460, de 2022\)](#)

VI - unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei.  
[\(Incluído pela Lei nº 13.853, de 2019\)](#)

Art. 55-D. O Conselho Diretor da ANPD será composto de 5 (cinco) diretores, incluído o Diretor-Presidente.  
[\(Incluído pela Lei nº 13.853, de 2019\)](#)

§ 1º Os membros do Conselho Diretor da ANPD serão escolhidos pelo Presidente da República e por ele nomeados, após aprovação pelo Senado Federal, nos termos da alínea 'f' do inciso III do art. 52 da Constituição Federal, e ocuparão cargo em comissão do Grupo-Direção e Assessoramento Superiores - DAS, no mínimo, de nível 5. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

§ 2º Os membros do Conselho Diretor serão escolhidos dentre brasileiros que tenham reputação ilibada, nível superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados.  
[\(Incluído pela Lei nº 13.853, de 2019\)](#)

§ 3º O mandato dos membros do Conselho Diretor será de 4 (quatro) anos. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

§ 4º Os mandatos dos primeiros membros do Conselho Diretor nomeados serão de 2 (dois), de 3 (três), de 4 (quatro), de 5 (cinco) e de 6 (seis) anos, conforme estabelecido no ato de nomeação. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

§ 5º Na hipótese de vacância do cargo no curso do mandato de membro do Conselho Diretor, o prazo remanescente será completado pelo sucessor. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

Art. 55-E. Os membros do Conselho Diretor somente perderão seus cargos em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

§ 1º Nos termos do caput deste artigo, cabe ao Ministro de Estado Chefe da Casa Civil da Presidência da República instaurar o processo administrativo disciplinar, que será conduzido por comissão especial constituída por servidores públicos federais estáveis. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

§ 2º Compete ao Presidente da República determinar o afastamento preventivo, somente quando assim recomendado pela comissão especial de que trata o § 1º deste artigo, e proferir o julgamento. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

Art. 55-F. Aplica-se aos membros do Conselho Diretor, após o exercício do cargo, o disposto no [art. 6º da Lei nº 12.813, de 16 de maio de 2013](#). [\(Incluído pela Lei nº 13.853, de 2019\)](#)

Parágrafo único. A infração ao disposto no caput deste artigo caracteriza ato de improbidade administrativa.  
[\(Incluído pela Lei nº 13.853, de 2019\)](#)

Art. 55-G. Ato do Presidente da República disporá sobre a estrutura regimental da ANPD. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

§ 1º Até a data de entrada em vigor de sua estrutura regimental, a ANPD receberá o apoio técnico e administrativo da Casa Civil da Presidência da República para o exercício de suas atividades. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

§ 2º O Conselho Diretor disporá sobre o regimento interno da ANPD. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

Art. 55-H. Os cargos em comissão e as funções de confiança da ANPD serão remanejados de outros órgãos e entidades do Poder Executivo federal. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

Art. 55-I. Os ocupantes dos cargos em comissão e das funções de confiança da ANPD serão indicados pelo Conselho Diretor e nomeados ou designados pelo Diretor-Presidente. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

Art. 55-J. Compete à ANPD: [\(Incluído pela Lei nº 13.853, de 2019\)](#)

I - zelar pela proteção dos dados pessoais, nos termos da legislação; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

XII - elaborar relatórios de gestão anuais acerca de suas atividades; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

XV - arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da [Lei nº 10.741, de 1º de outubro de 2003 \(Estatuto do Idoso\)](#); [\(Incluído pela Lei nº 13.853, de 2019\)](#)

XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e [\(Incluído pela Lei nº 13.853, de 2019\)](#)

XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

§ 1º Ao impor condicionantes administrativas ao tratamento de dados pessoais por agente de tratamento privado, sejam eles limites, encargos ou sujeições, a ANPD deve observar a exigência de mínima intervenção, assegurados os fundamentos, os princípios e os direitos dos titulares previstos no [art. 170 da Constituição Federal](#) e nesta Lei. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

§ 2º Os regulamentos e as normas editados pela ANPD devem ser precedidos de consulta e audiência públicas, bem como de análises de impacto regulatório. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

§ 3º A ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados, conforme legislação específica, e o tratamento de dados pessoais, na forma desta Lei. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

§ 4º A ANPD manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública responsáveis pela regulação de setores específicos da atividade econômica e

governamental, a fim de facilitar as competências regulatória, fiscalizatória e punitiva da ANPD. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

§ 5º No exercício das competências de que trata o caput deste artigo, a autoridade competente deverá zelar pela preservação do segredo empresarial e do sigilo das informações, nos termos da lei. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

§ 6º As reclamações colhidas conforme o disposto no inciso V do caput deste artigo poderão ser analisadas de forma agregada, e as eventuais providências delas decorrentes poderão ser adotadas de forma padronizada. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

Parágrafo único. A ANPD articulará sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

Art. 55-L. Constituem receitas da ANPD: [\(Incluído pela Lei nº 13.853, de 2019\)](#)

I - as dotações, consignadas no orçamento geral da União, os créditos especiais, os créditos adicionais, as transferências e os repasses que lhe forem conferidos; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

II - as doações, os legados, as subvenções e outros recursos que lhe forem destinados; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

III - os valores apurados na venda ou aluguel de bens móveis e imóveis de sua propriedade; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

IV - os valores apurados em aplicações no mercado financeiro das receitas previstas neste artigo; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

V - (VETADO); [\(Incluído pela Lei nº 13.853, de 2019\)](#)

VI - os recursos provenientes de acordos, convênios ou contratos celebrados com entidades, organismos ou empresas, públicos ou privados, nacionais ou internacionais; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

VII - o produto da venda de publicações, material técnico, dados e informações, inclusive para fins de licitação pública. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

Art. 55-M. Constituem o patrimônio da ANPD os bens e os direitos: [\(Incluído pela Medida Provisória nº 1.124, de 2022\)](#)

I - que lhe forem transferidos pelos órgãos da Presidência da República; e [\(Incluído pela Medida Provisória nº 1.124, de 2022\)](#)

II - que venha a adquirir ou a incorporar. [\(Incluído pela Medida Provisória nº 1.124, de 2022\)](#)

Art. 55-M. Constituem o patrimônio da ANPD os bens e os direitos: [\(Incluído pela Lei nº 14.460, de 2022\)](#)

I - que lhe forem transferidos pelos órgãos da Presidência da República; e [\(Incluído pela Lei nº 14.460, de 2022\)](#)

II - que venha a adquirir ou a incorporar. [\(Incluído pela Lei nº 14.460, de 2022\)](#)

Art. 56. (VETADO).

Art. 57. (VETADO).

## Seção II

### Do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

Art. 58. (VETADO).

Art. 58-A. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto por vinte e três representantes, titulares suplentes, dos seguintes órgãos: [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

I - seis do Poder Executivo federal; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

II - um do Senado Federal; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

III - um da Câmara dos Deputados; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

IV - um do Conselho Nacional de Justiça; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

V - um do Conselho Nacional do Ministério Público; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

VI - um do Comitê Gestor da Internet no Brasil; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

VII - quatro de entidades da sociedade civil com atuação comprovada em proteção de dados pessoais; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

VIII - quatro de instituições científicas, tecnológicas e de inovação; e [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

IX - quatro de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

§ 1º Os representantes serão designados pelo Presidente da República. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

§ 2º Os representantes de que tratam os incisos I a VI do caput e seus suplentes serão indicados pelos titulares dos respectivos órgãos e entidades da administração pública. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

§ 3º Os representantes de que tratam os incisos VII, VIII e IX do ~~caput~~ e seus suplentes: [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

I - serão indicados na forma de regulamento; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

II - terão mandato de dois anos, permitida uma recondução; e [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

III - não poderão ser membros do Comitê Gestor da Internet no Brasil. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

§ 4º A participação no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será considerada prestação de serviço público relevante, não remunerada. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

Art. 58-B. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade: [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

I - propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

III - sugerir ações a serem realizadas pela ANPD; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

IV - elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

V - disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população em geral. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

Art. 58-A. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto de 23 (vinte e três) representantes, titulares e suplentes, dos seguintes órgãos: [\(Incluído pela Lei nº 13.853, de 2019\)](#)

I - 5 (cinco) do Poder Executivo federal; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

II - 1 (um) do Senado Federal; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

III - 1 (um) da Câmara dos Deputados; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

IV - 1 (um) do Conselho Nacional de Justiça; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

V - 1 (um) do Conselho Nacional do Ministério Público; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

VI - 1 (um) do Comitê Gestor da Internet no Brasil; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

VII - 3 (três) de entidades da sociedade civil com atuação relacionada a proteção de dados pessoais; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

VIII - 3 (três) de instituições científicas, tecnológicas e de inovação; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

IX - 3 (três) de confederações sindicais representativas das categorias econômicas do setor produtivo; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

X - 2 (dois) de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais; e [\(Incluído pela Lei nº 13.853, de 2019\)](#)

XI - 2 (dois) de entidades representativas do setor laboral. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

§ 1º Os representantes serão designados por ato do Presidente da República, permitida a delegação. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

§ 2º Os representantes de que tratam os incisos I, II, III, IV, V e VI do caput deste artigo e seus suplentes serão indicados pelos titulares dos respectivos órgãos e entidades da administração pública. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

§ 3º Os representantes de que tratam os incisos VII, VIII, IX, X e XI do caput deste artigo e seus suplentes: [\(Incluído pela Lei nº 13.853, de 2019\)](#)

I - serão indicados na forma de regulamento; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

II - não poderão ser membros do Comitê Gestor da Internet no Brasil; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

III - terão mandato de 2 (dois) anos, permitida 1 (uma) recondução. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

§ 4º A participação no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será considerada prestação de serviço público relevante, não remunerada. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

Art. 58-B. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade: [\(Incluído pela Lei nº 13.853, de 2019\)](#)

I - propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

III - sugerir ações a serem realizadas pela ANPD; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

IV - elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e [\(Incluído pela Lei nº 13.853, de 2019\)](#)

V - disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

Art. 59. (VETADO).

CAPÍTULO X  
DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 60. A [Lei nº 12.965, de 23 de abril de 2014 \(Marco Civil da Internet\)](#), passa a vigorar com as seguintes alterações: [Vigência](#)

“Art. 7º .....

[X](#) - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais;

.....” (NR)

“Art. 16. ....

[II](#) - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a proteção de dados pessoais.” (NR)

Art. 61. A empresa estrangeira será notificada e intimada de todos os atos processuais previstos nesta Lei, independentemente de procuração ou de disposição contratual ou estatutária, na pessoa do agente ou representante ou pessoa responsável por sua filial, agência, sucursal, estabelecimento ou escritório instalado no Brasil.

~~Art. 62. A autoridade nacional e o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep), no âmbito de suas competências, editarão regulamentos específicos para o acesso a dados tratados pela União para o cumprimento do disposto no [§ 2º do art. 9º da Lei nº 9.394, de 20 de dezembro de 1996 \(Lei de Diretrizes e Bases da Educação Nacional\)](#), e aos referentes ao Sistema Nacional de Avaliação da Educação Superior (Sinaes), de que trata a [Lei nº 10.861, de 14 de abril de 2004](#). [\(Revogado pela Medida Provisória nº 869, de 2018\)](#).~~

Art. 62. A autoridade nacional e o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep), no âmbito de suas competências, editarão regulamentos específicos para o acesso a dados tratados pela União para o cumprimento do disposto no [§ 2º do art. 9º da Lei nº 9.394, de 20 de dezembro de 1996 \(Lei de Diretrizes e Bases da Educação Nacional\)](#), e aos referentes ao Sistema Nacional de Avaliação da Educação Superior (Sinaes), de que trata a [Lei nº 10.861, de 14 de abril de 2004](#).

Art. 63. A autoridade nacional estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados.

Art. 64. Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

~~Art. 65. Esta Lei entra em vigor após decorridos 18 (dezoito) meses de sua publicação oficial.~~

~~Art. 65. Esta Lei entra em vigor: [\(Redação dada pela Medida Provisória nº 869, de 2018\)](#).~~

~~I - quanto aos art. 55-A, art. 55-B, art. 55-C, art. 55-D, art. 55-E, art. 55-F, art. 55-G, art. 55-H, art. 55-I, art. 55-J, art. 55-K, art. 58-A e art. 58-B, no dia 28 de dezembro de 2018; e [\(Incluído pela Medida Provisória nº 869, de 2018\)](#).~~

~~II - vinte e quatro meses após a data de sua publicação quanto aos demais artigos. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#).~~

Art. 65. Esta Lei entra em vigor: [\(Redação dada pela Lei nº 13.853, de 2019\)](#)

I - dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e [\(Incluído pela Lei nº 13.853, de 2019\)](#)

I-A - dia 1º de agosto de 2021, quanto aos arts. 52, 53 e 54; [\(Incluído pela Lei nº 14.010, de 2020\)](#)

II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

II - em 3 de maio de 2021, quanto aos demais artigos. [\(Redação dada pela Medida Provisória nº 959, de 2020\)](#) [\(Convertida na Lei nº 14.058, de 2020\)](#)

II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

Brasília, 14 de agosto de 2018; 197º da Independência e 130º da República.



A hand holding a pen is writing on a white sheet of paper attached to a clipboard. The paper is held by a silver clip at the top. The text 'Compliance' is written in a cursive script, and 'LGPD' is written in a bold, sans-serif font below it.

*Compliance*

**LGPD**

