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

ARTHUR CRAVO BATTESINI

ADEQUAÇÃO DE ESCRITÓRIOS DE ADVOCACIA À LEI GERAL DE PROTEÇÃO DE DADOS

Porto Alegre
2023

ARTHUR CRAVO BATTESINI

Adequação de Escritórios de Advocacia à Lei Geral de Proteção de Dados

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

Orientador: Prof. Dr. Cristiano Colombo

Porto Alegre
2023

B565a Bettesini, Arthur Cravo.
Adequação de escritórios de advocacia à lei geral de proteção de dados / Arthur Cravo Battesini – 2023.
99 f. : 30 cm.

Dissertação (mestrado) – Universidade do Vale do Rio dos Sinos, Programa de Pós-Graduação em Direito da Empresa e dos Negócios, Porto Alegre, 2023.
"Orientador: Prof. Dr. Cristiano Colombo."

1. Compliance. 2. Proteção de dados. 3. Advocacia. 4. Governança corporativa. 5. Termo de consentimento. I. Título.

CDU 658.011.1

Dados Internacionais de Catalogação na Publicação (CIP)
(Bibliotecária: Bruna Sant'Anna – CRB 10/2360)

ARTHUR CRAVO BATTESINI

Adequação de Escritórios de Advocacia à Lei Geral de Proteção de Dados

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

Aprovada em: _____ de _____ de _____.

Componente da Banca Examinadora – Instituição a que pertence

Componente da Banca Examinadora – Instituição a que pertence

Componente da Banca Examinadora – Instituição a que pertence

Aos meus familiares, em especial meus Pais, Eugênio e Débora,
e à minha companheira, Carolina, por todos os incentivos.

AGRADECIMENTOS

Inicialmente, gostaria de agradecer a meus pais, Eugênio e Débora, sempre presentes nesta caminhada pelo mundo acadêmico, e sempre me incentivando a ir para a frente, bem como a meu irmão Bruno, por estar lá quando precisei. A meus avós, Íris, Valdir e Alfeu, por todo o carinho ao longo da jornada.

À minha namorada, Carol, pelo verdadeiro companheirismo que me ofereceu nestes últimos anos, muito desafiadores, mas juntos prevalecemos. Ainda, um agradecimento especial a seus pais, meus sogros, que sempre me acolheram da melhor forma possível.

Ainda, gostaria de agradecer especialmente à meu orientador, Prof. Dr. Cristiano Colombo, por todo o auxílio durante esta preciosa etapa acadêmica, e à Universidade do Vale do Rio dos Sinos, pelo acolhimento.

“Isn't heaven amazing? No matter how many times you look at it, it's never the same twice. This sky now only exists in this instant.”

Hitsugaya Toshiro

RESUMO

O presente trabalho possui como tema o *compliance* da Lei Geral de Proteção de Dados, Lei 13.709/18 (LGPD), na atividade advocatícia. Mais especificamente, é necessário observar como a promulgação da LGPD influencia na atuação de escritórios de advocacia que lidam com diversos dados pessoais, sendo necessário realizar uma adequação nos processos internos que lidam com os mesmos. A partir desta linha, se procura responder ao seguinte problema: Que providências, então, devem ser tomadas por escritórios para realizar a adequação de seus processos internos à Lei Geral de Proteção de Dados? Com relação à metodologia, a dissertação será confeccionada a partir do método hipotético-dedutivo, com uma análise crítica do material bibliográfico coletado, advindo de livros, artigos e periódicos com foco na temática de proteção de dados, e em matéria de regulação da própria atividade advocatícia. Tem-se como hipótese que a LGPD traz uma série de regulamentos que demandam a atenção dos escritórios, sendo necessário reconhecer as peculiaridades de cada área de atuação da advocacia. Como objetivo geral, logo, se tem analisar as medidas a serem implementadas por escritórios de advocacia, com relação a seu tratamento de dados pessoais, à luz da LGPD. Como objetivo específico, se tem estabelecer medidas específicas a serem implementadas, bem como a criação de um termo de consentimento de uso de dados à luz de diferentes áreas de atuação da advocacia. Foi possível, desta forma, rever a bibliografia de matérias adjacentes, e estabelecer medidas a serem implementadas pelos escritórios, bem como criar um termo de consentimento de uso de dados para os mesmos.

Palavras-Chave: Compliance; Lei Geral de Proteção de Dados; Advocacia; Governança; Termo de Consentimento.

ABSTRACT

The present work has as its theme the compliance of the General Data Protection Law, Law 13.709/18 (LGPD), in law practice. More specifically, it is necessary to observe how the enactment of the LGPD influences the performance of law firms that deal with various personal data, and it is necessary to adapt the internal processes that deal with them. From this point of view, an attempt is made to answer the following question: What steps, then, should law firms take to adapt their internal processes to the General Data Protection Law? Regarding methodology, the dissertation will be prepared from a critical analysis of the collected bibliographic material, coming from books, articles and periodicals focused on data protection, and on matters of regulation of the legal activity itself. It is hypothesized that the LGPD brings a series of regulations and requirements that demand the attention of law firms, and it is necessary to recognize the peculiarities of each area of advocacy. As a general objective, therefore, we must analyse the measures to be implemented by law firms, regarding their processing of personal data, considering the LGPD. As a specific objective, we must establish specific measures to be implemented by the same, as well as create a consent form for the use of data considering different areas of advocacy. It was possible, therefore, to review the data protection bibliography, as well as the legal regulations, and to establish measures to be implemented by the offices, as well as to create a term of consent for the use of data for them.

Keywords: Brazilian General Data Protection Law; Compliance; Law Practice; Consent Term.

LISTA DE ABREVIATURAS

ANPD	Autoridade Nacional de Proteção de Dados
CF	Constituição Federal
DPO	Data Protection Officer
GDPR	General Data Protection Regulation
IBGC	Instituto Brasileiro de Governança Corporativa
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados
MCI	Marco Civil da Internet
OAB	Ordem dos Advogados do Bracil
RGPD	Regulamento Geral de Proteção de Dados
RIPD	Relatório de Impacto à Proteção de Dados
UE	União Europeia

SUMÁRIO

1 INTRODUÇÃO 12

2 VISÃO GERAL DA LEI 13.709/18 16

2.1 ANTECESSORES EM PROTEÇÃO DE DADOS NO ÂMBITO INTERNACIONAL 16
2.2 DOS ANTECEDENTES HISTÓRICOS E DO CONTEXTO DA LEI GERAL DE PROTEÇÃO DE DADOS 18
2.3 ESTRUTURA DA LGPD 25

3 O PAPEL DO COMPLIANCE DIGITAL PARA A IMPLEMENTAÇÃO DA LGPD. 44

3.1 O COMPLIANCE TRADICIONAL 44
3.2 CARACTERIZAÇÃO DO COMPLIANCE DIGITAL 49
3.3 COMPLIANCE DIGITAL E A LGPD 51

4 A IMPORTÂNCIA DA ADEQUAÇÃO DOS ESCRITÓRIOS DE ADVOCACIA À LGPD 55

4.1 A ADVOCACIA 4.0 55
4.2 A LGPD COMO FONTE DE REGULAÇÃO DA ATIVIDADE ADVOCATÍCIA ... 57
4.3 RELAÇÃO DE ESCRITÓRIOS DE ADVOCACIA COM CLIENTES E COLABORADORES 61
4.4 REGULAÇÃO DO USO DE DADOS PARA ESCRITÓRIOS DE ADVOCACIA 67

5 PROPOSTA DE TERMO DE CONSENTIMENTO DE USO DE DADOS 79

5.1 MODELO DE TERMO DE CONSENTIMENTO DE USO DE DADOS 79
5.2 EXPOSIÇÃO DE MOTIVOS 84

6 CONCLUSÃO 89

REFERÊNCIAS 92

1 INTRODUÇÃO

A Lei Geral de Proteção de Dados traz diversos comandos que exigem ajustes nos escritórios de advocacia, a fim de garantir o uso adequado dos dados pessoais que se encontram em seu domínio. Desta forma, cabe a eles garantir as condições para que estes direitos sejam respeitados, em conformidade com a nova legislação. A fim de criar uma estratégia abrangente para sua implementação, se demonstra necessário não apenas soluções de tecnologia da informação, como também acompanhamento jurídico e reformulação de diversos processos internos, justamente focando a criação de uma cultura voltada para a segurança digital.

Desta forma, de maneira a delimitar o tema, tem-se que é necessário, logo, observar como a promulgação da LGPD influencia na atuação de escritórios de advocacia que lidam com diversos dados pessoais, tanto de terceiros quanto de colaboradores. Ainda, é essencial realizar uma adequação nos processos internos que lidam com os mesmos, e estabelecer termos de consentimento para as diferentes áreas de atuação profissional dentro da advocacia.

A fim, logo, de se moldar o trabalho, procura-se resolver o seguinte problema de pesquisa: Que providências, então, devem ser tomadas por escritórios para realizar a adequação de seus processos internos à Lei Geral de Proteção de Dados? A hipótese básica de trabalho é que a LGPD traz uma série de regulamentos e requisitos que demandam a atenção dos escritórios, sendo necessário reconhecer as peculiaridades de cada área de atuação da advocacia. Devem, então, fazer uma readequação em seus processos internos para conciliá-los com as novas demandas regulatórias, através das práticas de compliance jurídica, e estabelecer termos de consentimento de uso de dados para suas áreas específicas de atuação dentro da advocacia.

Como objetivo geral, tem-se o de analisar as medidas a serem implementadas por escritórios de advocacia, com relação a seu tratamento de dados pessoais, à luz da Lei Geral de Proteção de Dados. Em termos de objetivos específicos, se tem estabelecer medidas específicas a serem implementadas pelo mesmo, bem como criar um termo de consentimento de uso de dados à luz de diferentes áreas de atuação da advocacia. Com relação à metodologia, a dissertação foi confeccionada a partir de uma análise crítica do material bibliográfico

coletado, advindo de livros, artigos e periódicos com foco na temática de proteção de dados, e em matéria de regulação da própria atividade advocatícia.

Com relação à legislação de proteção de dados, esta possui inspiração no General Data Protection Regulation (GDPR)[1], construído pela União Europeia, dando especial enfoque na proteção de dados de pessoas naturais, titulares de dados, e, em muitos casos, consumidores. O GDPR, ainda, criou a obrigação de países que realizem comércio com o Espaço Econômico Europeu de estabelecerem suas próprias legislações de proteção de dados, tendo assim fortemente inspirado a própria Lei Geral de Proteção de Dados brasileira.

Ainda, com a criação da SEC, ou Securities and Exchange Commission, órgão norte-americano responsável pelas transações de valores mobiliários, se começa a instituir a obrigação de contratar compliance officers para criar procedimentos internos de controles e treinar colaboradores dentro das organizações. Com a lei Foreign Corrupt Practice Act[2], no ano de 1977, os EUA se comprometeram a combater a corrupção internacional. Em razão de sua promulgação, houve uma mudança de pensamento mundial com relação às práticas do chamado suborno internacional, e, após uma resistência inicial, diversos países criaram suas próprias legislações lidando sobre o tema. Ainda, esta lei traz consigo o dever das empresas de, justamente, criar mecanismos e procedimentos internos de auditoria, e criação de códigos de ética e conduta internos, mecanismos de compliance modernos.

A matéria de proteção de dados, ainda, requer especial cuidado com relação à sua implementação dentro de escritórios de advocacia. Estes lidam com informações altamente sensíveis de seus clientes, dada a natureza da profissão, que atua sem intenção mercantil e sempre visando o melhor interesse de seu cliente. Esta relação, pautada pela confiança, é estabelecida pelo próprio Estatuto da Ordem dos Advogados do Brasil[3], que também estabeleceu o dever de sigilo do advogado, este inerente à profissão e crítico com relação à proteção de dados de clientes pelos escritórios de advocacia.

---

[1] UNIÃO EUROPÉIA. **Regulamento 679, de 14 de abril de 2016.** Regulamento Geral sobre a Proteção de Dados. Disponível em: https://gdpr-info.eu/. Acesso em: nov. 2022.

[2] ESTADOS UNIDOS DA AMÉRICA. **Foreign corrupt practices act**. 1977. Disponível em: https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act. Acesso em: jan. 2023.

[3] BRASIL. **Lei n. 8.906, de 4 de julho de 1994.** Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8906.htm. Acesso em: jan. 2023.

A atividade advocatícia, ainda, possui uma variedade de áreas de atuação, com diversas necessidades específicas em relação à proteção de dados, sendo essencial personalizar as medidas de compliance a serem adotadas, em especial ao que tange ao termo de consentimento de uso de dados utilizado pelos escritórios de advocacia. Desta forma, é perceptível a necessidade de a Lei Geral de Proteção de Dados ser estudada dentro do contexto advocatício, sempre focando no compliance interna e na readequação de seus processos internos, de maneira a evitar potenciais riscos e aumentar a segurança dos dados resguardados. Ainda, justamente pelo escopo de atuação da atividade advocatícia, é importante frisar a necessidade de adotar um termo de consentimento que englobe as necessidades específicas do escritório em questão.

Tratar-se-á, inicialmente, do trajeto histórico, tanto internacional quanto nacional, da proteção de dados, para uma melhor compreensão de seu contexto. Após, se realizará um estudo geral sobre a Lei Geral de Proteção de Dados, Lei 13.709 de 2018, passando por seus princípios norteadores e sua estrutura geral, sempre focando em aspectos importantes para sua implementação para a advocacia.

No primeiro capítulo, será trazido uma visão geral da Lei Geral de Proteção de Dados, começando por seus antecessores em proteção de dados no âmbito internacional, como o General Data Protection Regulation da União Européia, e o Califórnia Consumer Protection Act, nos Estados Unidos. Ainda, tratará dos antecedentes históricos e do contexto da LGPD no cenário nacional, através de seu histórico e predecessores, o Marco Civil da Internet e a Lei de Acesso à Informação. Por último, se verá a estrutura geral da lei, seus princípios norteadores e seus pontos relevantes para a aplicação em escritórios de advocacia.

O segundo capítulo trará uma contextualização do compliance tradicional, bem como a caracterização do compliance digital, e, especialmente, suas aplicações dentro da proteção de dados, e, mais especificamente, sua complementariedade com a Lei Geral de Proteção de Dados.

O terceiro capítulo estudará a importância da adequação de escritórios de advocacia à LGPD, começando pela caracterização da advocacia 4.0, e sua relação regulatória com a mesma. Ainda, se verá a relação de escritórios de advocacia, tanto com seus clientes quanto com colaboradores. A partir disto, serão revistas medidas concretas que devem idealmente ser tomadas por escritórios de advocacia

para melhorar sua segurança digital, e criado um modelo de termo de consentimento de uso de dados voltado para a atividade advocatícia.

Por fim, se criará uma proposta de termo de consentimento de uso de dados visando a atuação de escritórios de advocacia, objetivando abranger a variedade de dados utilizados em diferentes áreas da profissão. Se criará o modelo do termo, bem como uma exposição de motivos para as cláusulas do mesmo.

Com relação à metodologia, esta dissertação será confeccionada, então, a partir de uma análise crítica do material coletado através do método hipotético-dedutivo, buscando coerência e clareza no raciocínio utilizado, a fim de atingir os resultados pretendidos com a pesquisa. Será utilizado na pesquisa bibliografia advinda de livros, artigos e periódicos, com foco na temática da lei geral de proteção de dados, bem como foco em matéria de regulação da própria atividade advocatícia, particularmente a gestão e regulação de dados dentro dos escritórios de advocacia. A pesquisa irá também abranger outras fontes, como legislação pertinente e jurisprudência dos tribunais brasileiros.

2 VISÃO GERAL DA LEI 13.709/18

2.1 ANTECESSORES EM PROTEÇÃO DE DADOS NO ÂMBITO INTERNACIONAL

A proteção de dados está em papel de destaque na última década em escala internacional. Diversas nações estão a criar legislações específicas para o processamento, tratamento e armazenamento de dados digitais. Os principais antecessores à Lei Geral de Proteção de Dados se encontram na União Europeia, e no Estado da Califórnia, nos Estados Unidos, como visto a seguir.

O Conselho Europeu, no ano de 1981, estabeleceu sua Convenção 108[4], uma das primeiras iniciativas internacionais de fornecer uma proteção aos dados pessoais dos cidadãos, precedida por uma lei no condado de Hesse, na Alemanha, em 1978, sendo considerada uma das primeiras peças de legislação a tratar do tema de proteção de dados, como coloca Jeferson Araújo.[5]

Já em termos atuais, o Regulamento Geral sobre a Proteção de Dados (General Data Protection Regulation 2016/679[6]), também conhecido por RGPD ou GDPR, é o regulamento da União Europeia que conceitua, estabelece e regulamenta a disciplina de proteção de dados pessoais. Criado em 2016, sua vigência e implementação se deram em 2018. Além de envolver organizações europeias, também se estende a todos aqueles que possuam negócios dentro do Espaço Econômico Europeu.

Seu antecedente, o chamado Data Protection Directive, ou Diretiva 95/46/EC[7], de 1995, também tratava da questão do processamento de dados dentro da União Europeia. No entanto, era apenas uma diretiva, o que significa que não obriga imediatamente seus membros, pendendo de ulterior internalização, através de normativas, como coloca Neil Robinson[8]. Esta falta de coesão na matéria

---

[4] UNIÃO EUROPEIA. **Convenção 108, para a Proteção das Pessoas Relativamente ao Tratamento de Dados de Caracter Pessoal**. Conselho Europeu, 1981.

[5] ARAÚJO, Jeferson. **A História Brasileira de Proteção aos Dados: O Advento da LGPD e a sua Influência No Acesso aos Dados Médicos no Brasil**. Disponível em: https://www.nucleodoconhecimento.com.br/lei/advento-da-lei Acesso em Junho de 2023.

[6] UNIÃO EUROPEIA. **Regulamento (UE) 2016/679.** Regulamento Geral sobre a Proteção deDados (RGPD). 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=PT. Acesso em: jan. 2023.

[7] UNIÃO EUROPEIA. **Diretiva de proteção de dados pessoais (95/46/CE**). 1995. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046. Acesso em: jan. 2023.

[8] ROBINSON, Neil *et al.* **Review of the european data protection directive**. Pittsburg: Rand Corporation, 2009. Disponível em:

dificultava um esforço inter-países na matéria de proteção de dados, levando ao estabelecimento do Regulamento Geral sobre a Proteção de Dados, de natureza vinculante a seus membros.

O RGPD, desta forma, tem como principal intenção dar aos usuários controle sobre seus dados pessoais, e, especialmente, simplificar a relação entre todo o território da União Europeia com relação ao tratamento dos dados [9], nos ensinamentos de Mark Philips. Isto facilitaria negócios feitos entre diferentes países, padronizando os processos envolvendo dados. Assim, organizações que coletam, realizam tratamento e armazenamento de dados pessoais e possuem vínculo com o Espaço Econômico Europeu devem observar este regulamento em seus processos internos.

Também estabelece medidas que visam aumentar a transparência de todo o processo, de acordo com Voigt[10], tendo como foco a questão do dever de divulgação que possui o controlador dos dados. Este deve, desta forma, divulgar o método que os dados são armazenados, bem como o propósito de sua coleta, e vincula o consentimento da parte com seu direito de revogá-lo a qualquer momento, sem necessidade de justificação. Ainda, estabelece em seu artigo 37 o papel do data protection officer (oficial de proteção de dados). É um funcionário que possui conhecimento em tecnologia da informação, bem como conhecimento dos regulamentos de dados. Sua função é exclusivamente a de organizar o compliance da organização com relação a estas novas normas de proteção de dados. Tanto instituições públicas quanto privadas devem possuir um DPO, que pode ser um funcionário interno ou uma atividade terceirizada, desde que não haja conflito de interesses com outras funções performadas.

Este Data Protection Officer, como coloca Lambert [11], deve possuir o conhecimento em compliance e em tecnologia da informação, bem como criar, organizar e manter registradas a integralidade das transações envolvendo dados que a organização realize. Controladores e operadores de dados que não sejam da

---

https://www.huntonak.com/files/webupload/PrivacyLaw_review_of_eu_dp_directive.pdf. Acesso em: abr. 2023.

[9] PHILIPS, Mark. International data-sharing norms: from the OECD to the general data protection regulation (GDPR). **Human Genetics,** n. 137, p. 575–582, 2018. Disponível em: https://doi.org/10.1007/s00439-018-1919-7. Acesso em: jan. 2023.

[10] VOIGT, Paul. **The EU general data protection regulation (GDPR):** a practical guide. [*s.l.*]: Springer, 2017.

[11] LAMBERT, Paul. **The data protection officer:** profession, rules and role. New York: CRC Press, 2017.

União Europeia devem também realizar o apontamento de um DPO desde que realizem transações dentro do Espaço Econômico Europeu, de acordo com seu artigo 27.

Já com relação aos Estados Unidos da América, o estado da Califórnia se demonstrou pioneiro na proteção de dados, criando o California Consumer Privacy Act[12], ou CCPA. Desenvolveu sua tramitação durante um período similar ao da LGPD, sendo convertido em legislação também em 2018. O CCPA, desta forma, guarda a intenção de estabelecer proteção aos usuários virtuais, lhes dando acesso a seus dados, e proibindo a venda dos mesmos a terceiros, como coloca Lydia de la Torre[13]. Permite, ainda, que estes solicitem exclusão de seus dados pessoais da base de dados que se encontrem armazenados.

O CCPA estabeleceu regras próprias de compliance que devem ser seguidas por qualquer organização que se encaixe em seus requisitos: possuir faturamento mínimo de 25 milhões de dólares ao ano, ou que metade de seu faturamento tenha como origem a venda dos dados armazenados de usuários. Ainda estabelece também um regime de responsabilidade próprio para aqueles que se encaixem nos requisitos, bem como diversas sanções em caso de brecha ao regulamento. Sendo o estado com a maior concentração de empresas de tecnologia dos Estados Unidos, a Califórnia traz então o pioneirismo em termos de proteção a dados pessoais, visando justamente seu conhecido “Vale do Silício”, onde se encontram as maiores empresas com produtos digitais do mundo, como coloca Saxenian[14]. Desta forma, criar regras de governança e compliance digital se demonstrou essencial para o Estado.

2.2 DOS ANTECEDENTES HISTÓRICOS E DO CONTEXTO DA LEI GERAL DE PROTEÇÃO DE DADOS

[12] CALIFORNIA. **California consumer privacy act**. 2018. Disponível em: https://oag.ca.gov/-privacy/ccpa. Acesso em: jan. 2023.
[13] DE LA TORRE, Lydia, **A guide to the california consumer privacy act of 2018**. Santa Clara: Santa Clara University, 2018. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3275571. Acesso em: abr. 2023.
[14] SAXENIAN, Annalee. The genesis of silicon valley. **Built Environment**, v. 9, n. 1, 1983.

A Lei Geral de Proteção de Dados (abreviada para LGPD), Lei nº 13.709[15], de 2018, é a principal legislação brasileira para o tratamento de dados pessoais por organizações, tanto governamentais quanto por empresas ou integrantes do terceiro setor. Traz diversas alterações com relação à Lei 12.965, o Marco Civil da Internet[16], bem como matéria inédita do setor de tecnologia.

Sendo um importante precursor do setor de regulação tecnológica no Brasil, merece uma análise mais profunda sobre o contexto de sua criação, bem como de sua estrutura, para uma melhor contextualização de sua implementação dentro do setor de advocacia, que tende a lidar com uma quantidade crescente de dados pessoais em suas atividades.

O Marco Civil da Internet, a Lei n° 12.965, de 23 de abril de 2014[17], cria regulações para o uso da internet no Brasil, e diversas diretrizes a serem seguidas pelo Poder Público na utilização da mesma. Lei pioneira em termos de matéria de tecnologia no Brasil, teve como origem um contexto único, cercado de discussões sobre o tema por diversos grupos, sendo considerada um dos mais complexos processos legislativos, como colocam Leite e Lemos[18] . Trouxe intensa discussão ao longo de seu projeto, e com diversos opositores, como empresas do setor de telefonia. Acabou, no entanto, como uma regulação pioneira no contexto internacional em termos de matéria digital.

Ofereceu uma verdadeira consolidação de diversos princípios encontrados em outras fontes de regulação, as concentrando em uma única legislação. Além desta consolidação, ainda, trouxe diversas matérias inéditas relacionadas à proteção no meio digital. Foi apelidada de “constituição da internet”[19], tendo sido discutida por meio de um site aberto ao público. Com a criação do Comitê Gestor da Internet (CGI), no ano de 1995, foi iniciada uma discussão pública sobre como

---

[15] BRASIL. **Lei n. 13.709 de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: jan. 2023.

[16] BRASIL. **Lei no 12.965, de 23 de abril de 2014.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: dez. 2022.

[17] BRASIL. **Lei no 12.965, de 23 de abril de 2014.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: dez. 2022.

[18] LEITE, George Salomão; LEMOS, Ronaldo (Coord.). **Marco civil da internet**. São Paulo: Atlas, 2014. p. XXVIII.

[19] GALINDO, Hercília. A “constituição da internet” brasileira requer atenção. **Folha de Pernambuco**, 26 jun. 2017. Disponível em: https://www.folhape.com.br/noticias/a-constituicao-da-internet-brasileira-requer-atencao/25427/. Acesso em: mar. 2023.

adequadamente regular o uso da internet, coloca Adachi[20]. Com poucas normas concretas na época, havia logo considerável insegurança jurídica devido a tal, bem como decisões por vezes contraditórias do Poder Judiciário. O uso cada vez mais difundido da internet, logo, exigia esta regulação, e sua falta estava por impedir o avanço tecnológico do país.

Após a criação do CGI, um projeto conhecido como “Lei Azeredo”, projeto de lei 84 de 1999 com o apelido homenageando Eduardo Azeredo, ex-senador, provocou fortes debates. O projeto possuía restrições significativas ao uso da internet, até mesmo criminalizando diversas atividades virtuais corriqueiras, como a transferência de músicas para o computador de arquivos externos. Com toda a rigidez, o projeto ganhou o apelido de “AI-5 da internet”[21], fazendo referências à ditadura militar. Devido a isto, houve considerável mobilização popular para que o projeto de lei não fosse aprovado, e que fosse criada legislação mais razoável para a utilização da internet.

Outro considerável gatilho para o debate e aprovação do Marco Civil da Internet foi o incidente “WikiLeaks”, site manejado na época por Edward Snowden[22]. Edward divulgou informações pertinentes à espionagem por parte dos Estados Unidos da América contra diversos países, onde o Brasil estaria incluído na lista de países atingidos, bem como a presidente da época, Dilma Rousseff, e diversas instituições do país. Devido à repercussão do caso, denota-se uma urgência de o governo brasileiro começar a atuar dentro do campo virtual, pois estava a sofrer prejuízos no campo internacional pela falta de uma regulação do campo da internet, tomando logo os primeiros passos para a criação do Marco Civil da Internet.

A Fundação Getúlio Vargas, à época, foi então aproximada pelo Ministério da Justiça para servir de coordenação para o projeto que viria a se tornar o MCI, como coloca Fiorillo[23]. Um site virtual foi criado, “culturadigital.org/marcocivil”; uma verdadeira plataforma virtual para colaboração diretamente com o público, em uma

---

[20] ADACHI, Tomi. **Comitê gestor da internet no Brasil (CGI.br):** uma evolução do sistema de informação nacional moldada socialmente. Tese (Doutorado) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2011. Disponível em: https://www.teses.usp.br/teses/disponiveis/12/12139/tde-10102011-165732/pt-br.php. Acesso em: mar. 2023.

[21] REZENDE, Pedro Antônio Dourado de. **Lei Azeredo, AI-5 digital e a cultura da história.** 2009. Disponível em: https://cic.unb.br/~rezende/trabs/azeredo3.html. Acesso em: jan. 2023.

[22] WIKILEAKS. **Blog WikiLeaks**. Disponível em: https://wikileaks.org/. Acesso em: jan. 2023.

[23] FIORILLO, Celso Antonio Pacheco. **O marco civil da internet e o meio ambiente digital na sociedade da informação:** comentários à Lei 12.965/2014. São Paulo: SaraivaJur, 2015.

empreitada única na história brasileira[24]. Em primeiro momento, discutiu-se os princípios de utilização da internet, para servir de fundamentação para construir o texto do que viria a se tornar a primeira peça de legislação a tratar do uso da internet no país. Ainda, o próprio texto legislativo foi novamente levado a debate público através da plataforma criada para tal, com todos aqueles que quisessem participar do processo de elaboração.

Ainda, este processo elencado em transparência e democracia, aliado a um importante tópico dentro de tecnologia da informação levou o Marco Civil da Internet a receber considerável atenção e elogios da comunidade internacional durante sua promulgação, sendo considerado uma legislação altamente avançada por diversas fontes, como o criador da World Wide Web, Tim Berners-Lee, altamente favorável à lei e descrevendo o Brasil como "um pioneiro da democracia digital a inaugurar uma nova era onde os direitos dos cidadãos seriam protegidos por leis com um escopo digital"[25], saudando em especial a intenção de levar em consideração tecnologia moderna dentro do processo legislativo.

A lei, no entanto, também se encontrou fortemente criticada, em especial com relação a seu escopo considerável, e que na prática possuiria baixa aplicação, especialmente em casos concretos. Como coloca Eduardo Tomasevicius[26], "Embora se tenha comemorado sua aprovação, [...] essa lei apresenta poucas inovações e muitas insuficiências e deficiências de cunho jurídico". Levanta Tomasevicius que regular uma estrutura como a internet através de uma única lei seria basicamente impossível, e que o simples fato de codificar certos princípios gerais não influenciaria em nada a vida do cidadão médio, sendo apenas uma forma de propaganda pública por parte do governo.

Com relação à sua estrutura, o MCI elencou, inicialmente, 3 princípios norteadores, sendo eles a neutralidade da internet, a fiscalização e a privacidade do usuário[27]. Esta privacidade, no caso, seria uma garantia de inviolabilidade para os

---

[24] Disponível em: http://arquivo.edemocracia.camara.leg.br/web/marco-civil-da-internet/inicio#.YJybE6Fv-Uk. Acesso em: jan. 2023.

[25] CRIADOR da Web divulga apoio ao marco civil da internet no Brasil. **G1 Globo**. 24 mar. 2014. Disponível em: http://g1.globo.com/tecnologia/noticia/2014/03/criador-da-web-divulga-apoio-ao-marco-civil-da-internet-no-brasil.html. Acesso em: mar. 2023.

[26] TOMASEVICIUS FILHO, Eduardo. **Marco civil da internet:** uma lei sem conteúdo normativo. São Paulo: Faculdade de Direito, Universidade de São Paulo, São Paulo, 2015.

[27] DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord**.). Direito e internet**. São Paulo: Quartier Latin, 2015. T. 1: Marco civil da Internet (Lei n. 12.965/2014).

mesmos, devendo haver sigilo dos provedores, devendo ser inquebrável, exceto por ordem judicial.

O princípio da fiscalização, elencado na subseção II do MCI, estabelece os regulamentos necessários para o processo de armazenamento e tratamento de dados, bem como estabelece a responsabilidade dos provedores pelos mesmos, dentro do prazo de um ano. Este princípio, posteriormente, é expandida pela própria Lei Geral de Proteção de Dados.

O princípio da neutralidade, de acordo com Pacheco[28], serve especificamente para reprimir qualquer tipo de ação que possa ser considerada abusiva por aqueles que prestam serviços relacionados à internet, como provedores. Não seria permitido, desta forma, o bloqueio de sites específicos. O objetivo é justamente o de aumentar uma possível igualdade para os usuários, evitando situações onde existam acessos que excluíssem parte dos mesmos. A lei também elenca exceções para tal princípio, nomeadamente em casos onde exista situação de emergência, quebras de segurança e falta de estabilidade da rede.

O MCI traz, ainda, diversos princípios secundários além dos três norteadores. Um deles é justamente a responsabilização dos agentes. João Quinelato[29] coloca que a lei cria, desta forma, previsão de responsabilização civil dos agentes participantes, em especial provedores de internet. Seu art. 18, por exemplo, os isenta de responsabilidade pelo conteúdo criado por usuários. Ainda, a lei traria uma lista meramente exemplificativa, que ressalta justamente que os princípios ali incluídos devem incluir os demais do ordenamento, bem como de tratados internacionais.

Em seu art. 2º, estabelece seus principais fundamentos: o reconhecimento da escala mundial de rede; os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais; a pluraridade e a diversidade; a abertura e a colaboração; a livre iniciativa e concorrência; e a finalidade social da rede.

Estes fundamentos alinham-se, desta forma, com os fundamentos elencados na própria Constituição Federal[30], como coloca Peck[31], justamente apontando para o

---

[28] FIORILLO, Celso Antonio Pacheco. **O marco civil da internet e o meio ambiente digital na sociedade da informação:** comentários à Lei 12.965/2014. São Paulo: SaraivaJur, 2015.
[29] QUEIROZ, João Quinelato. **Responsabilidade civil na rede:** danos e liberdades à luz do marco civil da internet. Rio de Janeiro: Processo, 2019.
[30] BRASIL. **Constituição da República Federativa do Brasil**. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: jan. 2023.
[31] PINHEIRO, Patricia Peck. **Direito digital**. São Paulo: Saraiva Jur, 2021.

tratamento deste espaço virtual como um espaço público, onde se realizam negócios e pessoas lidam com situações privadas. Assim, a proteção deve complementar aquilo que é esperado nos demais espaços públicos.

Ainda, o Marco Civil da Internet estabelece diversas ferramentas para cooperação internacional, justamente pelo fato de possuir um caráter transnacional em termos dos direitos que tutela. Exemplo é o pedido de assistência jurídica previsto em seu artigo 10º, parágrafo 2º, onde é possível coletar provas que se encontram fora do país, tanto para processos judiciais quanto para investigações criminais, ou para acessar dados com origem do Brasil que se encontram em servidores estrangeiros, e vice-versa. Estas ferramentas permitem considerável agilidade nestas situações em que demandem acesso a dados situados fora do país.

O MCI, em seu art. 5º, estabelece importantes definições, utilizadas até mesmo pela própria Lei Geral de Proteção de Dados. Strahus[32] postula que estas definições são fundamentais para a propagação da proteção de rede no Brasil. A lei estabelece a internet como sendo “um sistema constituído do conjunto de protocolos lógicos, estruturado em uma escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes”. Traz também diversas definições técnicas, como a de terminal, de registros de acesso, de aplicação, entre outros. Definições importantes em termos de clarear e estabelecer matéria legislativa sobre tecnologia da informação.

Desta forma, o MCI estabeleceu diversas fundações para as futuras peças legislativas que tratassem da internet, postula Patrícia Pinheiro[33]. No entanto, especialmente devido a seu escopo generalista, o Marco Civil da Internet teria trabalhado o aspecto de proteção de dados de maneira muito limitada, sendo necessária sua complementação posterior, nomeadmente pela própria Lei Geral de Proteção de Dados.

Com relação específica à proteção de dados dentro da legislação pátria, a principal fonte prévia à LGPD foi a Lei de Acesso à Informação, Lei nº. 12.527, de 2011[34]. Uma lei ordinária, ela estabelece justamente os regulamentos que são exigidos pelo art. 5º, inciso XXXIII, e os arts. 37, §3° e 216, §2°da Constituição

---

[32] STRAHUS, Rodrigo. **Direito digital:** o marco civil brasileiro da internet e as inovações jurídicas no ciberespaço. Curitiba: FASP Universitária, 2018.
[33] PINHEIRO, Patricia Peck. **Direito digital**. São Paulo: Saraiva Jur, 2021.
[34] BRASIL. **Lei 12.527, de 18 de novembro de 2011.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: jan. 2023.

Federal. Estes artigos tratam sobre o acesso à informação pelos cidadãos com relação a bancos de dados públicos, logo, o estabelecendo como direito fundamental.

Esta lei é uma iniciativa de adequação ao chamado “Open Government Initiative”, um programa dos Estados Unidos da América que propõe aumentar o nível de transparência do governo de todos aqueles que aderissem ao plano[35]. Ainda existia legislação federal esparsa que tratava da proteção de dados, mas apenas de maneira superficial. Exemplo disto é a Lei n. 11.111/05[36]. Trata sobre acesso a arquivos públicos, criando a regulação exigida pela parte final do disposto no inciso XXXIII do caput do art. 5º da Constituição Federal de 1988.

A Lei de Acesso à Informação[37] estabelece, assim, que os cidadãos possuem o direito de ter acesso a todas as informações não-sigilosas acerca de diversos dados institucionais, como para o acompanhamento de programas governamentais, auditorias, matérias de transparência do orçamento público, processos de licitação, entre outros. Em seu art. 1º, estabelece uma importante definição sobre quais pessoas jurídicas suas normas se aplicam:

> Art. 1º Esta Lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal.
> Parágrafo único. Subordinam-se ao regime desta Lei:
> I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;
> II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.
> Art. 2º Aplicam-se as disposições desta Lei, no que couber, às entidades privadas sem fins lucrativos que recebam, para realização de ações de interesse público, recursos públicos diretamente do orçamento ou mediante subvenções sociais, contrato de gestão, termo de parceria, convênios, acordo, ajustes ou outros instrumentos congêneres.
> Parágrafo único. A publicidade a que estão submetidas as entidades citadas no caput refere-se à parcela dos recursos públicos recebidos e à sua destinação, sem prejuízo das prestações de contas a que estejam legalmente obrigadas.

---

[35] ATTARD, Judie *et al*. A systematic review of open government data initiatives. **Science Direct,** v. 32, n. 4, p. 399-418, oct. 2015. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0740624X1500091X. Acesso em: mar. 2023.

[36] BRASIL. **Lei n. 11.111, de 5 de maio de 2005.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/lei/l11111.htm. Acesso em: mar. 2023.

[37] BRASIL. **Lei 12.527, de 18 de novembro de 2011.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: jan. 2023.

A Lei Geral de Proteção de Dados também se utilizou desta definição, com o intuito de estabelecer sua aplicabilidade com relação a pessoas jurídicas de direito público, e por ser este o principal dispositivo legal o qual trabalhava com a proteção de dados à época de sua criação. Como coloca Limberger[38], estas definições legais vem a estabelecer importantes precedentes para o ordenamento jurídico pátrio, devido à falta de amparo ao tema, em especial na época da LAI.

2.3 ESTRUTURA DA LGPD

A Lei Geral de Proteção de Dados, ou Lei 13.709/18[39] estabelece matéria relacionada ao processamento e armazenamento de dados pessoais. Traz conteúdo legislativo inédito, e também altera diversos artigos relacionados a dados pessoais em legislações anteriores, como o Marco Civil da Internet. Seu propósito é justamente elevar o Brasil a um nível adequado de proteção de dados a fim de se aproximar do contexto internacional, como colocam Cots e Oliveira.[40]

Em seus artigos iniciais, estabelece diversos princípios e fundamentos, a começar pelo seu escopo, estabelecido em seu art. 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.
> Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observados pela União, Estados, Distrito Federal e Municípios.

Aplica-se, desta forma, para pessoas naturais e pessoas jurídicas, sejam de direito privado ou público. Deve também ser observada ao se tratar de dados em meio físico, além do digital. O parágrafo único do artigo 1º, ainda, estabelece que

---

[38] LIMBERGER, Têmis. **O direito à Intimidade na era da informática:** a necessidade de proteção de dados pessoais. Porto Alegre: Livraria do Advogado, 2007.
[39] BRASIL. **Lei n. 13.709 de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: jan. 2023.
[40] COTS, Márcio; OLIVEIRA, Ricardo. **Lei geral de proteção de dados pessoais comentada**. São Paulo: Thomson Reuters, 2019.

suas normas devem ser observadas por todos os entes da federação: União, Estados, Distrito Federal e Municípios, pois suas normas seriam de interesse nacional.

Frazão[41] postula que a lei cobre qualquer operação que envolva tratamento de dados, independente de este ser feito por pessoa jurídica ou natural. Ainda, independe do meio que são tratados os dados, ou seu país de origem. Como condição, postula que a operação deve ser realizada dentro de território brasileiro, e tenha como principal objetivo a oferta ou fornecimento de bens ou serviços. Ainda, também se aplica caso os dados tenham sido coletados em território nacional.

Já no parágrafo I de seu artigo 3º, a lei caracteriza que "território nacional" seria considerado quando o titular daqueles dados se encontra em solo nacional durante o momento da coleta dos mesmos pela organização.Em seu art. 4º, elenca diversas exceções para sua aplicação, ao longo de seus quatro incisos. Estas exceções seriam as seguintes: quando o uso dos dados não possuir fim econômico, que tenham fins exclusivamente particulares ou jornalísticos, ou possivelmente acadêmicos ou artísticos.

Ainda, para o fim acadêmico, estabelece que devem ser seguidos os artigos 7º a 11, onde tratam de situações em que haja ilicitude no tratamento de dados. O artigo também estabelece que a lei não deve ser aplicada em casos onde se tenha fins de defesa nacional ou segurança pública e do Estado, ou, ainda, em atividades de repressão ou investigação de infrações penais. Nestes casos, o artigo estabelece que deva ser criada regulação por meio de lei própria, que estabeleça medidas proporcionais e necessárias ao atendimento do interesse público presente.

Por fim, em seu inciso IV também elenca a hipótese de exclusão para tratamentos dos dados que tenham origem fora do território brasileiro, e que também não sejam objeto de comunicação ou uso compartilhado com agentes brasileiros, nem de transferências internacionais com demais países. Patrícia Peck[42] postula que esta hipótese apenas teria validade quando o país de origem dos dados já possuir uma legislação adequada para a proteção de dados, que se alinhe com os da legislação brasileira.

---

[41] FRAZÃO, Ana *et al.* **A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters, 2019.

[42] PINHEIRO, Patricia Peck. **Direito digital**. São Paulo: Saraiva Jur, 2021.

Com relação a definições, a Lei Geral de Proteção de Dados estabelece diversas que agregam ao contexto de proteção de dados, em seu artigo 5º. Muitas destas se destacam por fornecerem maior contexto à própria peça de legislação, de acordo com Vinícius Albuquerque Lima[43]. Elenca, desta forma, três diferentes tipos de dados: sensíveis, pessoais ou anonimizados. Estabelece também a definição de banco de dados, sendo este um conjunto estruturado de dados pessoais. Cria também a figura da Autoridade Nacional de Proteção de Dados, ou ANPD.

Ainda dispõe sobre os operadores dos dados como sendo pessoas (tanto naturais quanto jurídicas, privadas ou públicas) a quem compete as decisões dentro do processo de tratamento de dados. Também define o encarregado, que seria a pessoa indicada pelo próprio operador para fazer a conexão com os titulares dos dados e a Autoridade Nacional de Proteção de Dados. Estabelece também o que seria o próprio tratamento de dados em seu inciso X: “

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

Estabelece, ainda, diversas ferramentas auxiliares para a proteção do tratamento de dados, como o relatório de impacto à proteção de dados, e a do órgão de pesquisa de proteção de dados. O relatório de impacto seria uma espécie de documentação, em que o controlador descreveria todos os processos em que passaram os dados, os quais poderiam gerar qualquer tipo de risco ou serem considerados críticos. Deve, no mesmo documento, estabelecer medidas preventivas, e mecanismos que permitam mitigar o risco destes processos.

A inspiração para isto seria a Avaliação de Impacto da Privacidade, criado pelo Information Commissioner’s Office, a autoridade de proteção de dados da União Europeia, coloca Cíntia Rosa.[44] Também prevê que a Autoridade Nacional de

---

[43] LIMA, Vinícius Albuquerque**. A lei n° 13.709/18 (Lei Geral de Proteção aos Dados Pessoais – LGPD) e sua relação com a advocacia:** o advogado e seus deveres quanto ao tratamento dos dados pessoais. 2021. Disponível em: https://jus.com.br/artigos/94515/a-lei-n-13-709-18-lei-geral-de-protecao-aos-dados- pessoais-lgpd-e-sua-relacao-com-a-advocacia-o-advogado-e-seus-deveres-quanto- ao- tratamento-dos-dados-pessoais. Acesso em: dez. 2022.

[44] LIMA, Cíntia Rosa Pereira de. **Autoridade nacional de proteção de dados e a efetividade da Lei Geral de Proteção de Dados:** de acordo com a Lei Geral de Proteção de Dados (Lei n.

Proteção de Dados possa estabelecer diretrizes para este relatório de impacto. O órgão de pesquisa, por sua parte, foi definido no inciso XVIII:

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

Com relação aos agentes de tratamento de dados, o Anteprojeto da Lei de Proteção de Dados, no ano de 2011, relacionava as figuras do responsável e do subcontratado. O responsável, no caso, poderia ser tanto pessoa física quanto jurídica, de direito público ou privado. Era quem tomaria as decisões finais com relação aos dados. O subcontratado, por outro lado, seria apenas uma pessoa jurídica que deveria seguir as decisões que haviam sido estabelecidas previamente pelo responsável do tratamento. Esta seria uma tentativa de melhor criar uma estrutura de responsabilização por parte do Anteprojeto, de acordo com comentários realizados pela FGV-Rio em contribuição ao mesmo.[45]

Com o aprofundamento do debate com relação a uma possível lei de proteção de dados, no entanto, se criaram diversas variações dessas figuras, finalmente resultando em três finais, na forma do controlador, do encarregado e do operador. Estas figuras seriam semelhantes às do Regulamento Geral de Proteção de Dados da União Europeia[46], a seus equivalentes: controller, processor, e data privacy officer.

A Lei Geral de Proteção de Dados, em seu art. 6º, traz seus princípios norteadores. Elenca dez ao todo, que servem como guia para toda a atividade de tratamento de dados: finalidade, livre acesso, adequação, qualidade dos dados, necessidade, adequação, transparência, livre acesso, prestação de contas, não-discriminação, responsabilização, e a boa-fé, estabelecida no caput do artigo.

13.709/2018 e as alterações da Lei n. 13.853/2019), o Marco Civil da Internet (Lei n. 12.965/2014) e as sugestões de alteração do CDC (PL 3.514/2015). São Paulo: Almedina, 2020.

[45] MONCAU, Luiz Fernando *et al.* **Contribuição do Centro de Tecnologia e Sociedade da FGV DIREITO RIO ao debate público sobre o Anteprojeto de Lei de Proteção de Dados Pessoais**. Rio de Janeiro:FGV, 2015. Disponível em: https://bibliotecadigital.fgv.br/dspace/handle/10438/17472. Acesso em: abr. 2023.

[46] UNIÃO EUROPEIA. **Regulamento (UE) 2016/679.** Regulamento Geral sobre a Proteção deDados (RGPD). 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=PT. Acesso em: jan. 2023.

A Lei Geral de Proteção de Dados traz, assim, destaque para o consentimento do usuário, e procura protegê-lo de atos que possam causar-lhes dano através de seus dados, por parte dos provedores. Estabelece, ainda, um rol de diversos princípios que complementam os demais, e postula no artigo 64 que este rol não é exaustivo, mas meramente exemplificativo, e devem ser complementares aos princípios presentes no ordenamento, bem como em tratados internacionais.

Coloca também o princípio da boa-fé em destaque, ao longo de seu artigo 6º , e artigo 52, parágrafo 1º. O princípio da boa-fé, um dos pilares do direito brasileiro, é estabelecida no Código Civil [47], servindo de fundamento para diversas peças legislativas. Judith Martins-Costa [48] postula que a boa-fé estabelece diversos deveres, bem como limita o exercício de diversos direitos, e, em sua forma comum, se estabelece como o dever de ser leal, bem como o dever de seguir uma conduta esperada de agentes com boas intenções.

Judith[49] ainda coloca outras modalidades para a boa-fé, sendo elas a objetiva e a subjetiva. A boa-fé objetiva seria, em termos gerais, a que trata do comportamento da parte, de sua conduta ao longo de toda a relação, e de como deve se portar em situações que apareçam durante a mesma. Já a boa-fé subjetiva, por sua vez, é a crença de que as partes agem de forma leal e respeitosa entre si, tendo consciência de suas boas intenções na relação jurídica. A denotação de "subjetiva" se dá por considerar não apenas as ações das partes, mas também suas intenções originais.

A intenção da Lei Geral de Proteção de Dados em seu artigo 6º, desta forma, é levantar a dita boa-fé objetiva, de acordo com Sheila Garcia[50]. Esta buscaria justamente impor uma conduta leal das partes, com respaldo no próprio Código Civil Brasileiro, que a estabelece como uma cláusula geral para contratos, bem como veda ações dadas de má-fé, contemplando a boa-fé subjetiva.

Essencial relevar, ainda, que os contratos de utilização de dados pessoais são majoritariamente contratos de adesão. Estes, como postula Carlos Bittar [51] possuem como principal característica sua praticidade e conveniência para

---

[47] BRASIL. **Lei n. 10.406, de 10 de janeiro de 2002**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: mar. 2023.
[48] MARTINS-COSTA, Judith. **A boa-fé no direito brasileiro**. São Paulo: Revista dos Tribunais, 1999.
[49] MARTINS-COSTA, Judith. **A boa-fé no direito brasileiro**. São Paulo: Revista dos Tribunais, 1999.
[50] GARCIA, Sheila. **A tutela da privacidade e dos dados pessoais na er a da vigilância**. [*s.l.*]: Processo, 2022.
[51] BITTAR, Carlos Alberto. **Os contratos de adesão e o controle de cláusulas abusivas**. São Paulo: SaraivaJur, 1991.

operações, comerciais ou não, de alta escala. No entanto, há proteção adicional para a parte aderente a estes contratos, considerada hipossuficiente, por não ter influência na criação do mesmo, apenas sujeita às cláusulas previamente escritas pela outra parte.

Os contratos de adesão, coloca desta forma, se encontram muito presentes nas relações onde há tratamento de dados de usuários, feito este pelos provedores. Desta forma, as proteções à esta parte hipossuficiente devem ser reafirmadas[52]. Ainda, pelos usuários possuírem seus dados pessoais passando por tratamento, se deve reforçar a questão do consentimento, bem como procurar sempre aumentar o nível de transparência da relação.

O artigo 6º traz, ainda, por meio de seu inciso I, o princípio da finalidade, que estabelece como tal: “realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades”. Com o objetivo de aumentar a proteção à parte dos usuários, como coloca Bioni[53], impede o provedor, desta forma, de utilizar estes dados para outros fins alheios aos que foi-lhe dado consentimento por parte dos mesmos, buscando novamente transparência no processo.

Ainda, o artigo 6º estabelece a possibilidade de se retirar o consentimento por parte do usuário, em caso onde haja alteração na finalidade para os dados, devendo isto ser comunicado ao usuário, que pode discordar da nova finalidade. Por último, o artigo 10º estabelece os usos que podem ser considerados legítimos para o uso dos dados: quando houver o apoio e promoção de atividades do controlador; proteção ao exercício regular dos direitos do titular; e quando o tratamento for baseado no legítimo interesse do mesmo, aqui restringindo apenas aos dados estritamente necessários.

Estes parágrafos estabelecem justamente a importância do princípio da finalidade, de maneira que restringem o uso dos dados pessoais apenas estritamente necessários para atingir a finalidade pretendida originalmente, e previamente consentida pelo usuário. Ainda, estabelece a possibilidade de a

---

[52] BITTAR, Carlos Alberto. **Os contratos de adesão e o controle de cláusulas abusivas**. São Paulo: SaraivaJur, 1991.

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

Autoridade Nacional de Proteção de Dados solicitar eventuais relatórios sobre estas finalidades.

Em seu parágrafo 2º, ressalta quanto à importância de haver transparência ao longo de todo o processo, em especial para com o usuário. Ainda, em seu art. 23, a LGPD estabelece uma alteração à Lei de Acesso à informação, especificamente com relação ao tratamento de dados feito pelo poder público. Ademais, outros princípios contidos no artigo 6º se encontram associados ao próprio princípio da finalidade, este inclusive sendo citado diretamente nos demais.

Com relação ao princípio da adequação, este relaciona a importância de o tratamento feito com os dados seja compatível com a finalidade inicial que foi divulgada ao usuário final. Isto possui justamente a função de fortalecer, novamente, a transparência de todo o processo de tratamento de dados, de acordo com Rosa Pereira Lima.[54]

No princípio da necessidade, temos que este tratamento que está sendo realizado com os dados deve se limitar a fazer o mínimo possível que seja necessário para cumprir aquela finalidade original, em especial abrangendo apenas os dados que sejam necessários e evitando demasiados processos nos mesmos. Desta forma, se aumenta a responsabilidade que o controlador dos dados teria, de acordo com Patrícia Pinheiro[55], utilizando apenas os que seriam realmente necessários, e se relacionando ao princípio seguinte, que seria do livre acesso de dados. Este é, basicamente, uma garantia que o usuário deve ter da possibilidade de consultar, de maneira facilitada e completamente gratuita, com relação ao processo que seus dados estão sofrendo, juntamente com o controlador dos mesmos.

O princípio da qualidade dos dados elenca que sempre devem haver atualizações dos dados, bem como averiguação de sua veracidade, de maneira constante, durante o tempo que se encontrarem sob a proteção do provedor. Cria, assim, uma relação de responsabilidade deste, e de seus bancos de dados, para com os usuários. A Lei Geral de Proteção de Dados, desta forma, estabelece

---

[54] LIMA, Cintia Rosa Pereira de (Coord.). **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020.

[55] PINHEIRO, Patricia Peck**. Proteção de dados pessoais comentários à Lei n. 13.709/2018:** (LGPD). 3. ed.São Paulo: Saraiva Jur, 2021.

diversas situações onde o titular dos dados pode exigir correções ou atualizações, como em seu artigo 18, inciso III[56].

A transparência, aqui, é elencada também como princípio da LGPD, que acaba por permear todos os demais: “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”. Necessário, logo, incluir na comunicação com os usuários o máximo de claridade e precisão possíveis, de forma que se torne possível obter um consentimento específico em relação ao processo pelo quais passarão os dados, como traz Patrícia Pinheiro[57]. O próprio Marco Civil da Internet, em seu artigo 7º, estabelece que o usuário possui este direito à informação com relação a seus dados.

Traz também o princípio da segurança. Este confere para o provedor a responsabilidade de sempre estar em dia com relação às medidas, tanto técnicas quanto administrativas, que são tomadas dentro do processamento dos dados. Devem ser impedidos, desta forma, acessos que não sejam autorizados, ou situações que possam arriscar a integridade da operação, ou causar perdas ou alterações dos dados.

Em seu capítulo VII, ainda, a Lei Geral de Proteção de Dados estabelece práticas e orientações com relação à segurança dos dados. Estas ressaltam a responsabilidade do provedor, nos casos onde existam brechas de segurança desnecessárias. Ainda, traz o princípio da prevenção. Este, como coloca Rosa[58] estabelece que devem ser adotadas diversas medidas de prevenção por parte dos provedores, de tal forma que não existam riscos de vazamentos ou de eventos que causem dano aos dados armazenados.

Já o denominado princípio da não-discriminação, postula, estabelece que estes dados armazenados não podem ser usados para fins de discriminação, fins ilícitos ou fins considerados abusivos. Esta preocupação é redobrada em situações onde se lide com dados sensíveis, por estes possuirem uma natureza delicada, que

---

[56] 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: III - correção de dados incompletos, inexatos ou desatualizados. **Lei 13.709**, op cit.

[57] PINHEIRO, Patricia Peck**. Proteção de dados pessoais comentários à Lei n. 13.709/2018:** (LGPD). 3. ed.São Paulo: Saraiva Jur, 2021.

[58] LIMA, Cintia Rosa Pereira de (Coord.). **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020.

propicia possíveis métodos de discriminação. Este princípio estabelece, logo, que os usuários devam ser protegidos destas situações.

Por fim, traz também o princípio da responsabilização e prestação de contas. Conforme Patrícia Pinheiro[59], este cria uma estrutura de responsabilização do provedor com relação ao usuário, bem como estabelece que o agente que performe o tratamento dos dados faça uma adequada prestação de contas de todo o processo, sempre levando em consideração a boa-fé, e buscando ao máximo a transparência para a relação: ”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.”.

O agente de tratamento de dados, de acordo com Kremer[60], deve realizar a devida diligência em qualquer processo envolvendo os mesmos, estabelecendo procedimentos de segurança e governança. Ainda, é responsabilizado caso exista alguma situação que venha a ferir algum dos princípios previamente elencados. Dentro desta prestação de contas, há também o relatório que é devido para a Autoridade Nacional de Proteção de Dados, bem como medidas de transparência que são devidas ao titular dos dados, em particular com relação à finalidade dos dados e consentimento do dito titular com ela.

A Lei Geral de Proteção de Dados estabelece três tipos de dados: pessoais, sensíveis e anonimizados. Dados pessoais, trazem Teixeira e Guerreiro[61], são os dados estabelecidos em lei, que possibilitam uma identificação do usuário, e podem ser o nome, número do cadastro de pessoa física, registro geral, ou fotos, de titulares já identificados ou que possam vir a ser. Ainda entram nesta categoria diversas informações gerais, tanto qualitativas quanto quantitativas, como histórico de compras. No caso de informações delicadas, como etnia, religião, entre outros, podem ser considerados como dados pessoais sensíveis, por ser possível criar uma situação de discriminação do usuário.

Já os dados anonimizados se relacionam com titulares onde não é possível realizar sua identificação, tendo sido descaracterizados. No caso, a Lei Geral de Proteção de Dados, em seu artigo 12, os excluiu do rol de proteção da mesma, com

---

[59] PINHEIRO, Patricia Peck**. Proteção de dados pessoais comentários à Lei n. 13.709/2018:** (LGPD). São Paulo: Saraiva Jur, 2021.

[60] KREMER, Bianca. **Os agentes de tratamento de dados pessoais**. São Paulo: Arquipélago, 2020.

[61] TEIXEIRA, Tarcísio; GUERREIRO, Ruth Maria. **Lei geral de proteção de dados pessoais (LGPD):** comentada artigo por artigo. São Paulo: SaraivaJur, 2022.

exceção de casos onde possam ter seu processo de anonimização revertidos de alguma maneira.

Desta maneira, se for possível realizar o rastreamento através de brechas neste processo de anonimização, por quaisquer meios, estes dados não são considerados verdadeiramente anonimizados, conforme Doneda [62] . Logo, encontram-se na proteção da LGPD fornecida aos usuários. A Lei ainda trouxe a definição de dados pseudonimizados, que são justamente os dados que acabaram sofrendo este processo de anonimização, no entanto, por quaisquer motivos ele não foi efetivo, e é possível o rastreio da forma original dos mesmos. Assim, se encaixam na proteção oferecida pelo artigo 12, independentemente do processo de anonimização.

A anonimização, como estabelece Gisele Krauer[63], é usualmente atingida através de uma duplicação de bases de dados. Desta forma, a cópia seria processada através desta anonimização, mas os dados originais ainda se encontrariam em sua forma original, identificável. A Lei Geral de Proteção de Dados estabelece tal caso em seu artigo 13, parágrafo 4º:

> Art. 13, §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.

Krauer, ainda, estabelece que a criptografia dos dados serve um importante papel no processo de anonimização, mas não deve ser confundido com o mesmo, sendo apenas uma ferramenta de compliance útil para aperfeiçoar a segurança do tratamento, considerando que a própria Lei Geral de Proteção de Dados não elenca o tópico da criptografia em seu texto:

> De forma bastante simplificada, a criptografia é sobre codificar e decodificar dados. Basicamente, ela consiste em uma prática na qual um dado é codificado por meio de um algoritmo (no exemplo acima, uma mensagem enviada é codificada). Esse algoritmo trabalha de forma conjunta com uma chave, que define como a mensagem será cifrada (codificada). [...] A palavra criptografia sequer aparece no texto da LGPD. Ela pode ser

[62] DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. **Revista dos Tribunais**, São Paulo, v. 998, 2018.

[63] KAUER, Gisele. **Anonimização, pseudonimização e criptografia:** perguntas frequentes, definições e o que diz a LGPD. InfraNews Telecom, 2023. Disponível em: https://www.infranewstelecom.com.br/anonimizacao-pseudonimizacao-e-criptografia-perguntas-frequentes-definicoes-e-o-que-diz-a-lgpd/. Acesso em: mar. 2023.

> utilizada como uma boa prática em segurança da informação e proteção de dados, mas não existe qualquer obrigatoriedade em utilizá-la.

Por último, os dados pessoais considerados sensíveis são relacionados com informações íntimas do titular, como traz Patrícia Peck[64]. Exemplos disto são orientações religiosas ou sexuais, opiniões políticas, ou qualquer tipo de dado que possa levar a situações de discriminação. Em seu artigo 5º, a Lei Geral de Proteção de Dados estabelece as condições para os dados serem considerados sensíveis:

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

Já em seu capítulo II, “Do tratamento de dados pessoais”, a Lei Geral de Proteção de Dados estabelece normas a respeito do processamento dos dados em si, que devem ser levados em consideração juntamente com os princípios anteriormente trabalhados. Em seu artigo 7º, traz 10 situações nas quais é permitido realizar o tratamento dos dados.

Desta forma, o tratamento realizado em dados pessoais deve sempre se encaixar dentro destas hipóteses, salvo em situações que configurem hipóteses de exclusão da aplicação da LGPD, elencados em seu artigo 4º, previamente analisado. As hipóteses são abrangentes, de forma a englobar diversas situações onde haja a necessidade de proteção ao longo do tratamento para o titular dos dados, como coloca Patrícia Pinheiro.[65]

Em seu inciso I, estabelece a regra geral e hipótese mais recorrente: o titular cede seu consentimento para que o tratamento dos dados seja realizado. Esta cessão apenas ocorre caso o titular esteja em situação de ter este consentimento como seu direito disponível, feito mediante sua autorização, e sempre respeitando os limites impostos pelos termos tanto da legislação quanto do caso concreto em que se encontra.

---

[64] PINHEIRO, Patricia Peck**. Proteção de dados pessoais comentários à Lei n. 13.709/2018:** (LGPD).São Paulo: Saraiva Jur, 2021.

[65] PINHEIRO, Patricia Peck. **Proteção de dados pessoais comentários à Lei n. 13.709/2018:** (LGPD). São Paulo: Saraiva Jur, 2021.

Ainda, os incisos V e VII estabelecem duas situações onde o consentimento do titular é relevado para analisar a viabilidade do tratamento de seus dados pessoais. No inciso V, levanta-se a hipótese de quando os dados forem necessários para a execução de eventual contrato em que seja parte o titular dos direitos. Já no inciso VII, seria para situações onde haja matéria de saúde, relevantes para o titular ou para terceiro.

Nos demais incisos, logo, as hipóteses ignoram se há o consentimento do titular ou não para permitir o tratamento dos dados pessoais. Em seu inciso II, estabelece situações onde os dados seriam necessários quando houver o dever de cumprir algum tipo de obrigação legal para o controlador. Em seu inciso VI, estabelece que é possível ao controlador realizar tratamento dos dados sem o consentimento também para o exercício regular de direitos em processos, sejam judiciais, administrativos ou arbitrais.

Em seu inciso III, estabelece que o poder público pode realizar tratamento de dados pessoais quando este for necessário para executar políticas públicas, desde que previstas em lei ou regulação diversa, uma de diversas concessões especiais que a Lei Geral de Proteção de Dados faz para o tratamento de dados pela administração pública.

Apenas dados que se apresentem como necessários para a finalidade original informada pelo controlador tem sua utilização permitida para estes fins, conforme o próprio princípio da finalidade, estabelece Frazão[66]. Desta forma, se não se encontrarem nas hipóteses do artigo 10º, são considerados ilícitos. Ainda, o próprio artigo 10º estabelece que as atividades de destino dos dados, realizadas pelo controlador, devem ser também legítimas e lícitas, e não apenas o processo de tratamento de dados em si.[67]

O capítulo II, ainda, em sua seção, II, estabelece diversas finalidades consideradas lícitas para estes tratamento dos dados pessoais sensíveis, dado a natureza dos mesmos, exigindo cautela e discricionariedade por parte do controlador em maior grau que dados pessoais regulares.

Para diferenciar o consentimento do usuário com relação a seus dados sensíveis, a LGPD, em seu artigo 11, inciso I, a lei estabelece que o tratamento

---

[66] FRAZÃO, Ana *et al.* **A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters, 2019.

[67] FRAZÃO, Ana *et al.* **A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters, 2019.

destes dados deve se dar apenas quando houver consentimento de forma específica e destacada, com uma finalidade especificada de maneira detalhada. Isto se deve pelo fato de estes dados considerados sensíveis, caso ocorra seu vazamento ou rastreamento do usuário, podem levar a cenários de discriminação. Logo, ao estabelecer um consentimento específico, se aumenta a transparência da relação, e se oferece uma camada adicional de proteção aos usuários.[68]

Ainda, o próprio artigo 11 levanta diversas hipóteses de exceção a este consentimento específico, em seu inciso II. Em essência, a lei se preocupa em excetuar situações onde o poder público necessite dos dados para políticas públicas, ou realização de estudos relevantes. Ainda, também excetua situações onde haja o exercício regular de direitos, por tutela da saúde, proteção da vida, e garantia de prevenção à fraude.

Esta lista possui natureza taxativa, coloca Patrícia Pinheiro[69]. Ou seja, estabelece todas as hipóteses onde, excepcionalmente, haja a dispensa de consentimento do titular dos dados para seu tratamento. Não há, no entanto, previsão de dispensa de consentimento para casos onde o tratamento dos dados seja necessário para a execução de contrato legal.

Já em sua seção III, estabelece regulamentos para o tratamento de dados pessoais de crianças e adolescentes, composta apenas por seu artigo 15. Desta forma, a Lei Geral de Proteção de Dados cria uma importante diferenciação ao lidar com menores de idade, bem como seu predecessor, o Regulamento Geral de Proteção de Dados. Esta proteção adicional é relevante, pois estes não podem dar seu consentimento para o tratamento de seus dados.

No artigo 14, caput, se dá, logo, que este tratamento de dados pessoais de crianças e adolescentes deve apenas ser realizado quando tiver o seu melhor interesse como objetivo. O parágrafo 1º coloca que a autorização de pais ou responsável legal é necessário para o tratamento, e seu parágrafo 2º prevê que todo o processo de tratamento dos dados deve ser público, reforçando assim a transparência do mesmo.

Ainda, o artigo 14 estabelece hipótese única para realizar este tratamento dos dados sem o consentimento de pais ou responsável legal: apenas quando a

---

[68] LIMA, Cintia Rosa Pereira de (Coord.). **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020.

[69] PINHEIRO, Patricia Peck. **Proteção de dados pessoais comentários à Lei n. 13.709/2018:** (LGPD). São Paulo: Saraiva Jur, 2021.

utilização dos dados for necessária para possibilitar o contato com os pais ou responsáveis do menor, ou para sua proteção. Devem, ainda, ser utilizados apenas uma única vez, e não podem ser armazenados para uso posterior, ou repassados a terceiros.

No entanto, pelo alto uso feito da internet por usuários menores de idade[70], a LGPD estabelece diretrizes necessárias para obter o consentimento dos mesmos. Apenas pode ser obtido o consentimento quando for possível determinar objetivamente que este foi dado por seus pais ou responsável legal, respeitando os limites da tecnologia, e com esforços razoáveis da parte do controlador. Ainda, não pode o consentimento ser parte de jogos, aplicativos ou quaisquer outras atividades digitais, além dos que forem necessários para seu funcionamento.

Já em seu parágrafo 6º, o artigo 14 estabelece que informações obtidas através deste consentimento devem estar claras e transparentes. Desta forma, estabelece Lóssio[71], as mesmas devem ser redigidas de forma a serem de fácil entendimento, e sempre considerando as limitações físicas e mentais do usuário, possibilitando uso de recursos audiovisuais que se demonstrem necessários para facilitar seu entendimento por parte da criança ou adolescente, ou do responsável legal.

Em sua seção IV, a Lei Geral de Proteção de Dados descreve como deve ser manejado o término do tratamento dos dados. Desta forma, estabelece 4 hipóteses que ensejam o encerramento, descritas em seu artigo 15. A primeira hipótese é a verificação de que houve o alcance da finalidade do tratamento, ou de que os dados não são mais necessários para se chegar à mesma. Ainda, caso ocorra o fim do período alocado para o tratamento.

Também se encerra o tratamento quando há a comunicação do titular dos dados, sendo possível este se utilizar de seu direito de revogar o consentimento dado. Por último, deve-se encerrar o tratamento quando haja determinação da Autoridade Nacional de Proteção de Dados, dada por violação aos preceitos da Lei Geral de Proteção de Dados.

---

[70] AGENCIA BRASIL. **Brasil tem 24,3 milhões de crianças e adolescentes que usam internet.** 2019. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2019-09/brasil-tem-243-milhoes-de-criancas-e-adolescentes-utilizando-internet. Acesso em Janeiro de 2023.

[71] LÓSSIO, Claudio Joel Brito. **Proteção de dados e compliance digital.** São Paulo, Almedina, 2021.

Ainda, é necessário, conforme estabelece o artigo 16, que sejam eliminados os dados armazenados para tratamento. Ainda estabelece o artigo hipóteses onde é permitido conservar os dados utilizados, excepcionalmente: necessidade de cumprimento legal por parte do controlador; estudos por órgãos de pesquisa, desde que se proceda à anonimização dos dados; transferência a terceiro, caso se respeitem os preceitos da lei; e para utilização exclusiva do próprio controlador, conquanto os dados foram anonimizados, e que seja proibido o acesso a qualquer tipo de terceiro a eles.

Desta forma, ocorre o término justamente em decorrência da finalização natural do tratamento, ou em situações onde haja a revogação de consentimento pelo titular, ou, ainda, a pedido da Autoridade Nacional de Proteção de Dados. Estas hipóteses de conservação dos dados são apenas para situações excepcionais, como coloca Doneda,[72] e exigem um processo de anonimização dos dados, de tal forma que estes não se vinculem mais a seus titulares, logo, não mais fazendo parte do escopo da LGPD.

Com relação ao capítulo III, são elencados os direitos dos titulares. Relacionam-se, assim, com os próprios direitos fundamentais elencados na Constituição Federal Brasileira, conforme artigo 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.”O próprio art. 5º da CF[73] estabelece a previsão de considerar estes direitos como fundamentais.

Ainda, estabelece que o titular possui o direito de obter informações com relação a seus dados, necessitando apenas de uma requisição em formato simplificado, conforme artigo 19. Esta requisição pode ser realizada a qualquer momento, tanto virtualmente quanto de forma impressa. Idealmente deve conter o máximo de informação possível a respeito dos dados. O controlador possui, assim, o prazo de quinze dias úteis para responder, no entanto, a Autoridade Nacional de Proteção de Dados pode rever o prazo, de acordo com Cíntia Rosa.[74]

---

[72] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 3. ed. São Paulo: Thomson Reuters, 2021.

[73] BRASIL. **Proposta de Emenda à Constituição - PEC 17/2019.** Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757. Acesso em: jan. 2023.

[74] LIMA, Cíntia Rosa Pereira de. **Autoridade nacional de proteção de dados e a efetividade da Lei Geral de Proteção de Dados:** de acordo com a Lei Geral de Proteção de Dados (Lei n.

No capítulo IV, estabelece diversas medidas aplicáveis apenas para o poder público, que possui um regime diferenciado com relação à proteção de dados. Como principal regra, tem em seu artigo 23 que o tratamento de dados realizado por pessoa jurídica de direito público deve apenas ser feito quando for necessário para atingir sua finalidade pública, sempre em busca do interesse público, e basicamente estabelece em seu artigo 24 condições mínimas para que se valide o tratamento, como o alinhamento da finalidade do tratamento com a competência da entidade que o realizar.

Ao tratar da transferência internacional de dados, a LGPD tem por principal preocupação estabelecer condições mínimas de proteção de dados para o país que fizer parte da transferência juntamente com o Brasil, como coloca Patrícia Pinheiro.[75] Estabelece, logo, em seu capítulo V, hipóteses onde a transferência de dados é permitida: quando o país estiver com condições mínimas de proteção de dados, ou quando o controlador dos dados fornecer comprovação de que garantirá a segurança dos dados. Em seu artigo 34, estabelece que as condições mínimas devem ser avaliadas pela Autoridade Nacional de Proteção de Dados.

Em seus capítulos finais, a LGPD estabelece o sistema regulatório e fiscalizatório, na forma da Autoridade Nacional de Proteção de Dados, ou ANPD. Criada em 2018 pela medida provisória nº 869[76], convertida na Lei nº 13.853[77], de 8 julho de 2019. Trata-se de autarquia, conforme a Lei 14.460/22. Possui papel-chave na implementação da Lei Geral de Proteção de Dados, devendo orientar, fiscalizar, sancionar e regular a matéria de proteção de dados, possuindo inclusive poder de polícia para tal.

Em seu texto original, a própria LGPD estabelecia uma previsão legal para criá-la. O presidente Michel Temer, no entanto, vetou os dispositivos referentes a tal, por conter "vício de origem"[78], pois tal lei não poderia legislar com relação à organização do Estado, responsabilidade esta do Poder Executivo. Por isto se criou

---

13.709/2018 e as alterações da Lei n. 13.853/2019), o Marco Civil da Internet (Lei n. 12.965/2014) e as sugestões de alteração do CDC (PL 3.514/2015). São Paulo: Almedina, 2020.

[75] PINHEIRO, Patricia Peck. **Direito digital**. São Paulo: Saraiva Jur, 2021.

[76] BRASIL. **Medida Provisória no 869, de 27 de dezembro de 2018**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm. Acesso em: jan. 2023.

[77] BRASIL. **Lei n. 13.853, de 8 de julho de 2019**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: jan. 2023.

[78] BRASIL. Câmara dos Deputados. Sancionada, com nove vetos, lei que cria Autoridade Nacional de Proteção de Dados **Agência Câmara de Notícias**, 2019. Disponível em: https://www.camara.leg.br/noticias/561908-SANCIONADA,-COM-NOVE-VETOS,-LEI-QUE-CRIA-AUTORIDADE-NACIONAL-DE-PROTECAO-DE-DADOS. Acesso em: jan. 2023.

a Medida Provisória 869, alterando a LGPD novamente para apenas autorizar a criação da mesma.

Anteriormente à sua concepção, foram criados projetos de lei que possuíam semelhante objetivo:estabelecer uma autoridade que possuísse poder para fiscalizar a proteção de dados,como o Projeto de Lei n. 6291/16[79]. Este alteraria o Marco Civil da Internet de forma a vedar o compartilhamento de dados entre provedores. Outro exemplo seria o Projeto de Lei n. 4060/12[80], cujo objetivo era estabelecer um sistema de autorregulação para os operadores de dados, semelhante ao CONAR - Conselho Nacional de Autorregulação Publicitária.

A partir deste, entidades representativa do setor de operadores de dados criariam uma sociedade sem fins lucrativos, encarregada de regular e fiscalizar o setor, estabelecem De Lucca e Lima[81]. Este modelo, no entanto, não se demonstraria adequado para a proteção de dados pessoais em específico, devido à sensibilidade da matéria, e à proteção necessária e consequências graves para os usuários caso existam desvios de conduta dos controladores, colocam.

Com a criação de um sistema de autorregulação, logo, incertezas e inconstâncias poderiam seriamente prejudicar os titulares dos dados. Com a criação da Autoridade Nacional, no entanto, é possível regulamentar o setor e lhe fornecer o poder de polícia próprio, lhe dando autonomia para gerenciar o altíssimo volume de dados sob a proteção da Lei Geral de Proteção de Dados, auxiliando na implementação da mesma e trazendo imparcialidade em um setor que lida com informações delicadas.[82]

A criação da Autoridade Nacional de Proteção de dados gerou diversos debates, no sentido de ser necessária para uma implementação bem-sucedida da LGPD, a fiscalizando. No entanto, a criação de um órgão próprio para tal gera custos significativos, em especial em período de recessão, como se encontrava durante o

---

[79] BRASIL. **Projeto de Lei 6291/2016**. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2113796. Acesso em: jan. 2023.

[80] BRASIL. **Projeto de Lei 4060/2012**. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066. Acesso em: jan. 2023.

[81] LIMA, Cintia Rosa Pereira de (Coord.). **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020.

[82] LIMA, Cíntia Rosa Pereira de. **Autoridade nacional de proteção de dados e a efetividade da Lei Geral de Proteção de Dados:** de acordo com a Lei Geral de Proteção de Dados (Lei n. 13.709/2018 e as alterações da Lei n. 13.853/2019), o Marco Civil da Internet (Lei n. 12.965/2014) e as sugestões de alteração do CDC (PL 3.514/2015). São Paulo: Almedina, 2020.

debate.[83] Esta preocupação se dá pelo fato desta necessitar lidar com tecnologia de ponta, e com elevado conhecimento técnico, aumentando exponencialmente os custos.

Conforme artigo 52 da Lei nº 13.853[84], a ANPD possui diversas funções que se relacionam com a proteção de dados, inclusive o poder de aplicar sanções administrativas caso encontre descumprimento à LGPD por parte dos operadores, como multas e bloqueios, bem como a eliminação de dados que se refiram às infrações realizadas.

Possui também a característica de promotora e instrutora da Lei Geral de Proteção de Dados, com o dever de liderar uma nova etapa no controle de dados no país. Deve não apenas fiscalizar as organizações privadas, mas também auxiliar na adaptação das entidades públicas, trabalhando com a conscientização da sociedade como um todo sobre a importância da proteção de dados, fenômeno recente até mesmo em termos internacionais.[85]

Com relação à estrutura da Autoridade Nacional de Proteção de Dados, é uma autarquia, de acordo com a Lei 14.460, de 2022. Sua composição parte de um conselho diretor, considerado seu órgão maior. Este possui o Diretor-Presidente, bem como outros quatro diretores regulares. Os membros são escolhidos diretamente pelo Presidente da República, e aprovados pelo Senado Federal. A primeira composição foi realizada por Jair Bolsonaro, Presidente da República, no ano de 2020[86]. Ainda, possui um cargo comissionado criado pela Lei 14.460 de Diretor-Presidente.

Seus diretores cumprem um mandato com duração de quatro anos, podendo ser afastados a qualquer momento que incorram em faltas graves, através de um procedimento administrativo disciplinar, pelo Presidente da República. Isto concede maior autonomia funcional aos mesmos, com sua saída se dando apenas por renúncia própria ou por decisão judicial com trânsito em julgado.

---

[83] TEIXEIRA, Tarcísio; GUERREIRO, Ruth Maria. **Lei geral de proteção de dados pessoais (LGPD):** comentada artigo por artigo. São Paulo: SaraivaJur, 2022.

[84] BRASIL. **Lei n. 13.853, de 8 de julho de 2019**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: jan. 2023.

[85] LIMA, Cíntia Rosa Pereira de. **Autoridade nacional de proteção de dados e a efetividade da Lei Geral de Proteção de Dados:** de acordo com a Lei Geral de Proteção de Dados (Lei n. 13.709/2018 e as alterações da Lei n. 13.853/2019), o Marco Civil da Internet (Lei n. 12.965/2014) e as sugestões de alteração do CDC (PL 3.514/2015). São Paulo: Almedina, 2020.

[86] TILT UOL. **Proteção de dados:** conheça os indicados por Bolsonaro para comandar a ANPD. 2020. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/10/17/conheca-os-indicados-por-bolsonaro-para-comandar-a-anpd.htm. Acesso em: jan. 2023.

Ainda, possui em sua estrutura o chamado Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. Este conselho tem o dever de aconselhar e guiar as ações da ANPD, e é composto de 25 membros ao total, apontados por diversas organizações, como o Poder Executivo, Senado, Conselho Nacional de Justiça, entre outros diversos, inclusive pela sociedade civil, empresas e trabalhadores do setor. Ainda possuem ouvidoria, corregedoria, bem como um órgão que fornece assistência jurídica, além de suas unidades administrativas próprias.

O Conselho Nacional de Proteção de Dados possui características semelhantes com o Comitê Europeu para a Proteção de Dados, ou CEPD,[87] uma organização independente da União Europeia que é composta por diversos representantes da Autoridade Europeia para a Proteção de Dados e outras autoridades nacionais. Este também possui o encargo de aconselhamento e acompanhamento das decisões tomadas na AEPD.

A União Europeia, em seu Regulamento Geral sobre a Proteção de Dados[88], estabelece como obrigatório a todos atuantes no Espaço Econômico Europeu que possuam regulação em matéria de proteção de dados. Parte da exigência é justamente que haja um sistema regulatório nacional em conjunto com a legislação de proteção de dados. Desta forma, a criação da Autoridade Nacional de Proteção de Dados permite ao Brasil transacionar dados com países integrantes da União Europeia.

A Autoridade Nacional de Proteção de Dados, logo, é essencial para uma implementação bem-sucedida da Lei Geral de Proteção de Dados no Brasil, partindo de um adequado aconselhamento e acompanhamento das organizações do setor, bem como servindo de fiscal em matéria de proteção de dados.

---

[87] LIMA, Cintia Rosa Pereira de (Coord.). **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020.

[88] UNIÃO EUROPEIA. **Regulamento (UE) 2016/679.** Regulamento Geral sobre a Proteção deDados (RGPD). 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=PT. Acesso em: jan. 2023.

3 O PAPEL DO COMPLIANCE DIGITAL PARA A IMPLEMENTAÇÃO DA LGPD

3.1 O COMPLIANCE TRADICIONAL

Compliance, termo em inglês que deriva do latim *complere,* significa se colocar em concordância com o que é pedido, como coloca Block[89]. Vem justamente de estar em concordância com regras e normas. Seu verbo, "*to comply*" (cumprir), exige sempre uma complementação: cumprir com algo em específico, que é imposto externamente à organização, e esta deve se adaptar da maneira que for possível. Não apenas seguir no sentido literal, como diz Block, mas assumir também um comportamento condizente com o objetivo geral das normas, além da natureza estritamente jurídica.

O IBGC, Instituto Brasileiro de Governança Corporativa, estabelece que o termo "compliance" abrange justamente o uso de boas-práticas na governança interna das empresas, com a finalidade de reduzir possíveis riscos[90]. Ainda, dentro de seu código de práticas de governança, estabelecem diversos princípios básicos. Os principais são a transparência, a prestação de contas e a equidade.

Para Stinco[91], o compliance deve ser entendida em sentido amplo, sendo ela a busca da coerência entre o que se espera da organização, que é o respeito às regras e a adoção de princípios coerentes com sua identidade, e o que é de fato praticado eu suas operações, atingindo entidades de todos os portes e setores.

É possível, desta forma, concluir que compliance é a adequação da empresa para regulamentações, de forma a reduzir potenciais riscos e criar estratégias para lidar com crises a partir de um planejamento que considere o caso concreto da empresa, como é colocado pelo IBGC[92]:

> A administração deve trabalhar para entender o perfil de riscos da organização, que deve estar alinhado com a sua identidade, e determinar seu apetite a riscos – ou seja, o nível de risco que está disposto a aceitar. Ao ser integrado ao planejamento estratégico, o gerenciamento de riscos se torna um alicerce para o sistema de compliance, contribuindo para o

[89] BLOCK, Marcella. **Compliance e governança corporativa**. São Paulo: Freitas de Bastos, 2020.
[90] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das melhores práticas de governança corporativa**. São Paulo, IBGC, 2015.
[91] STINCO, M. (Org**.). Compliance à Luz da Governança Corporativa**. São Paulo, SP: Instituto Brasileiro de Governança Corporativa, 2017.
[92] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das melhores práticas de governança corporativa**. São Paulo: IBGC, 2015.

> estabelecimento de processos alinhados e compromissos de curto e longo prazo documentados.

A figura do compliance, logo, deve partir de um comprometimento da gestão, e ser internalizado dentro da cultura organizacional, aliando um pensamento estratégico com uma conduta de responsabilidade da parte de todos envolvidos na organização. Ainda que não deixe a organização completamente à prova de riscos, certamente apriomorará os sistemas internos e permitirá sua gestão mais eficiente.

Como traz Block[93], há diversos pontos positivos que a adoção de uma cultura voltada para o compliance traz para a organização: o aumento na qualidade e velocidade das interpretações regulatórias e políticas, bem como de produtos em conformidade com o mercado; o aprimoramento do relacionamento com reguladores, inclusive o bom retorno das revisões dos supervisores com o devido acompanhamento das correções e deficiências por parte dos agentes de compliance; a melhoria de relacionamento com os clientes, acionistas e demais stakeholders; e a disseminação de padrões elevados de ética e cultura de compliance pela organização.

A falta desta cultura, estabelece Block[94], pode abrir a organização a diversos males, inclusive multas, dano à reputação da marca e da organização, cassação de licenças, sanções tanto a instituições quanto a indivíduos, entre outros. Como ilustra com a fala de Paul McNulty, ex-Vice-Procurador Geral dos Estados Unidos: “Se você pensa que compliance é caro, tente não o ter.”.

Compliance, logo, pode ser considerada uma área de suporte interna para as organizações, como coloca Marcos Assi[95]. Coloca que a iniciativa deve vir, inicialmente, do topo (*top down*), para que todos os integrantes da organização entendam que suas tomadas de decisão devem respeitar leis e normas, além de procedimentos internos preexistentes, sempre se pautando pela lógica de prevenir, detectar e responder a possíveis riscos. Ainda, estabelece que não basta apenas implementar tais políticas e procedimentos, mas sim ativamente cobrar a aplicação dos princípios na realização das atividades da organização, mantendo o adequado apoio e treinamento requeridos pelo nível de complexidade da atividade.

---

[93] BLOCK, Marcella. **Compliance e governança corporativa**. São Paulo: Freitas de Bastos, 2020.
[94] BLOCK, Marcella. **Compliance e governança corporativa**. São Paulo: Freitas de Bastos, 2020.
[95] ASSI, Marco. **Compliance:** como implementar. São Paulo: Trevisan, 2018.

O compliance, desta forma, é pautada por três pilares: prevenir, detectar e responder. Com relação à prevenção, coloca Lamboy[96], seria possivelmente o pilar mais crítico, possibilitando evitar as situações no lugar de necessitar remediá-las. Para ser eficaz nesta prevenção, logo, a organização deve instituir políticas e procedimentos internos claros com instruções que estejam de acordo com os objetivos internos que possuem para o compliance. Exemplo disso, traz, seriam os códigos de conduta, que devem abranger os aspectos mais relevantes da organização.

Com relação à detecção, estabelece que esta possui um papel fundamental para cobrir potenciais falhas resultantes da prevenção, especialmente através de canais de denúncia e outros mecanismos que permitam o descobrimento de inadequações. No entanto, é necessário pars tais mecanismos que haja confiança dos membros da organização nos mesmos, necessitando haver uso adequado destes por parte de seus usuários.

Na resposta, o terceiro e último pilar, devem ser implementadas políticas de consequências que estejam alinhadas com o código de conduta. Para tal, os processos internos devem ser adequadamente auditados e definidos a fim de se permitir uma rastreabilidade. As consequências devem ser claras e objetivas, evitando dar margem a possível abuso das mesmas.

Existem, ainda, outros pilares do compliance baseados em requerimentos do *Federal Sentencing Guidelines,* uma série de regras estabelecidas nos Estados Unidos da América pela Comissão de Sentenciamento, que publicou em 1984 um guia de compliance para empresas[97] como parte de suas diretivas. Os dez pilares estabelecidos são os que seguem, pelo instituto LEC [98] (Legal, Ethics and Compliance), aqui parafraseados:

1) Suporte da alta administração: o programa de compliance deve receber o aval explícito da administração da organização, e nomear um responsável

[96] LAMBOY, Christian Karl de. **Manual de compliance**. São Paulo: Instituto ARC, 2017.

[97] A versão atualizada está disponível em: https://web.archive.org/web/20120906064229/http://www.ussc.gov/Research/Research_Projects/Miscellaneous/15_Year_Study/chap1.pdf. Acesso em: jan. 2023

[98] SIBILE, Daniel; SERPA, Alexandre; FARIA, Felipe. **Os pilares do programa de compliance:** uma breve discussão. LEC, 2020. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/BibliotecaDigital/BibDigitalLivros/TodosOsLivros/Os-pilares-do-programa-de-compliance.pdf. Acesso em: jan. 2023.

pelo programa de compliance que possua autonomia de gestão. Ou seja, a alta administração deve ativamente praticar os princípios do compliance em suas atividades e apoiar ao máximo sua implementação no restante da organização.

2) Avaliação de riscos: a condução de análises de risco adequadas envolve planejamento e documentação dos processos internos, e o estabelecimento de medidas necessárias de contenção. O código de conduta, desta forma, deve se basear nos riscos previstos na etapa de avaliação.

3) Código de conduta: é a formalização da postura da empresa, levando em consideração os riscos avaliados, bem como a regulação aplicável para suas atividades. O código deve servir como uma bússola que irá guiar os membros da organização para um caminho de atos éticos e respeitosos para as normas.

4) Controles internos: são mecanismos para minimizar riscos da operação, bem como para se certificar de que as ações internas estão de acordo com a regulação. Idealmente devem estar formalizados dentro dos procedimentos internos.

5) Treinamento e comunicação: depois de realizada a identificação dos riscos e da formalização das políticas de compliance, deve ser feito o treinamento e comunicação dos mesmos para todos os membros da organização. Este pilar é essencial para o sucesso do programa de compliance, para disseminar os valores e procedimentos que se busca com o mesmo.

6) Canais de denúncia: canais de comunicação fornecem aos membros da organização um meio de denunciar atos que fujam ao código de conduta e a outras políticas implementadas. Deve ser seguro e fornecer aos mesmos um feedback apropriado, para aumentar sua confiabilidade.

7) Investigações internas: a organização deve possuir processos internos que permitam investigar denúncias de comportamentos ilícitos e que vão contra o código de conduta interno, bem como estabelecer as medidas a serem tomadas de maneira prévia.

8) Due diligence: toda vez que a organização for estabelecer compromissos com terceiros, deve realizar uma pesquisa adequada para verificar se possuem uma estrutura adequada e se possuem um histórico de condutas antiéticas, não apenas para se resguardar de possíveis complicações legais, mas também para reafirmar sua cultura ética interna.

9) Auditoria e monitoramento: para saber se o programa de compliance está sendo adequado, é importante implementar um processo de avaliação constante, e realizar auditorias frequentes, baseadas em métricas previamente estabelecidas. Com um monitoramento e documentação adequados, é facilitada a expansão do programa de compliance. Ainda, permite desta forma aumentar sua confiabilidade, bem como reforça a transparência dos processos internos.

10) Diversidade e inclusão: ao encontrar dilemas, o profissional de compliance deve ser objetivo, e relevar as circunstâncias do caso concreto, buscando justamente uma solução adequada da situação. Este preceito deve ser aplicado aos demais, fortalecendo a cultura de compliance da organização.

Com estas diretrizes, é possível perceber que a implementação de programas de compliance em muito agrega para a organização, em especial na época digital que nos encontramos. Com isto, o compliance tradicional vem tomando uma forma modernizada na forma do compliance digital, vista a seguir, que possui a estrutura geral semelhante, mas traz diversas ferramentas específicas para o trabalho virtual, em especial na proteção de dados.

3.2 CARACTERIZAÇÃO DO COMPLIANCE DIGITAL

Com a digitalização intensa encontrada na sociedade atual, e em especial dentro do meio profissional, através de softwares de gestão, que contém informações financeiras, dados sobre clientes, entre outros. Todas estas informações são armazenadas digitalmente, além dos diversos dados que são lançados através de aplicativos e sites. Com esta exposição virtual, se encontram grandes vulnerabilidades, requerendo, desta forma, um programa de compliance específico para o meio digital, como coloca Lóssio.[99]

Neste sentido, estabelece que todas as mudanças que a tecnologia traz na sociedade apontam justamente para um novo horizonte onde estas informações devem ser preservadas através de uma adequada proteção e prevenção de riscos. Operadores do Direito, desta forma, devem se pautar por uma atuação baseada dentro desta ética, assumindo responsabilidade em acompanhar estas inovações tecnológicas dentro do possível e utilizando-as como uma ferramenta de gestão.

Esta relação entre o Direito e a tecnologia vem se demonstrando cada vez mais importante, em especial na última década. Dentro do ambiente normativo, se desenham comportamentos padronizados em face de inúmeros cenários, mas dentro destes ambientes, como coloca Gilmar Mendes[100], deve haver espaço para observar o constante tráfego das relações socioculturais da sociedade. Este desenvolvimento tecnológico, logo, já pressuporia um regime jurídico que engloba todas as transformações que se fazem nos ambientes da sociedade.

Atos como o Marco Civil da Internet, logo, buscam justamente criar estas regulamentações preliminares e gerais sobre o tema de direito e tecnologia, mas certamente não são exaustivos, resultando na necessidade de sempre acompanhar as novidades para garantir que não sejam concorrentes a tutelas de direitos fundamentais.

Conforme o IBGC, ou Instituto Brasileiro de Governança Corporativa[101], os programas de compliance devem ser incorporados nas empresas, pois estas inovações tecnológicas podem vir a esbarrar em diversas legislações preexistentes.

---

[99] LÓSSIO, Claudio Joel Brito. **Proteção de dados e compliance digital.** São Paulo, Almedina, 2021.

[100] MENDES, Gilmar; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. **Direito, inovação e tecnologia**. São Paulo: Saraiva, 2015.

[101] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das melhores práticas de governança corporativa**. São Paulo: IBGC, 2015.

A estrutura destes negócios é constantemente reformulada com a introdução de novas tecnologias, e é de seu interesse estar de encontro com o que lhe é requerido legalmente, se utilizando de suas ferramentas e recursos de tecnologia da informação para preservar sua ética e cultura organizacional.

Atenção especial vem se dando na legislação para o tema de privacidade e proteção de dados de usuários, devido a este aumento no uso de tecnologia pelas empresas prestadoras de serviços. O próprio GDPR[102], regulamento europeu de proteção de dados e precursor internacional do tema, observa uma série de condutas que devem ser tomadas pelas empresas, condutas estas corroboradas pela própria Lei Geral de Proteção de Dados.

Marcella Block [103], neste contexto, estabelece certas medidas que as organizações devem tomar para a implementação de um programa de compliance digital: auditoria e consulta das medidas que se encontram no momento em uso, análise de licenças de software, atualização de políticas de privacidade, e, por mais importante, a criação de normas, procedimentos e processos de utilização interna que venham a tratar sobre a gestão de recursos de tecnologia da informação, bem como a criação de políticas internas para coibir eventuais abusos ou práticas ilegais e antiéticas que possam vir a colocar em risco a implementação das medidas práticas e a empresa como um todo. Coloca como medidas de implementação do compliance digital, aqui parafraseado:

1) Auditoria prévia com o fim de identificar as medidas que já estão sendo tomadas, para melhor redirecionar o uso para segurança e proteção, bem como identificar eventuais falhas que venham a acometer os sistemas;

2) Análise das licenças utilizadas para garantir segurança dos dados e prevenção a ataques cibernéticos, bem como verificar se está de acordo com a quantidade de tráfego de dados existentes nas redes em específico;

[102] UNIÃO EUROPEIA. **General data protection regulation 679/2016.** Disponível em https://gdpr-info.eu/. Acesso em: fev. 2023.
[103] BLOCK, Marcella. **Compliance e governança corporativa**. São Paulo: Freitas de Bastos, 2020.

3) Atualização da política de privacidade e dos termos de uso para devida adequação com a legislação pertinente, como o Marco Civil da Internet, a Lei Geral de Proteção de Dados e a Lei de acesso à informação;

4) Criação de normas, processos e procedimentos de utilização interna que tratem da gestão de recursos de tecnologia da informação, bem como a criação de políticas internas para coibir eventuais abusos ou práticas ilegais e antiéticas que possam vir a colocar em risco a implementação e a organização.

Desta forma, a figura do compliance digital em muito agrega para a execução adequada das medidas de readequação necessárias por parte das empresas. De acordo com Cavalari [104], aliando a tecnologia da informação ao compliance tradicional, o compliance digital permite minimizar potenciais riscos que venham a envolver as partes ao longo de todo o processo de tratamento dos dados, que podem vir na forma de vazamentos, falhas de comunicação ou até mesmo algum tipo de sanção legal.

Ainda, a existência de regulação própria, tanto para a utilização dos meios virtuais tanto quanto para a proteção dos dados das empresas, como coloca Marcos Assis, exige uma observância dos deveres de assimilar os novos requerimentos legais internamente, conhecendo seus limites legais e se reestruturando adequadamente para que cada área da empresa esteja apta a seguir estas novas regulações.

3.3 COMPLIANCE DIGITAL E A LGPD

O compliance digital possui diversas ferramentas que permitem a implementação da Lei Geral de Proteção de Dados de maneira mais abrangente dentro das organizações. Esta correlação é fortalecida com um sistema de compliance que respeite os preceitos básicos da LGPD, compostos pelos mecanismos de prevenção de riscos que visem à proteção de dados pessoais.[105]

---

[104] CAVALARI, Ana Paula França. **O compliance digital como ferramenta de gestão**. Porto Alegre: OAB/RS, 2020.

[105] LIMA, Cíntia Rosa Pereira de. **Autoridade nacional de proteção de dados e a efetividade da Lei Geral de Proteção de Dados:** de acordo com a Lei Geral de Proteção de Dados (Lei n.

Ainda, com a introdução de multa pecuniária de até 2% do valor do faturamento da empresa, além de outras imposições como suspensão parcial do banco de dados e até mesmo das próprias atividades de tratamento dos dados, como estabelece a Lei 13.853/19.[106] Desta forma, há incentivos financeiros e éticos/morais para a implementação de programa de compliance digital com foco na Lei Geral de Proteção de Dados pelas organizações.

A própria LGPD também elenca diversos mecanismos para implementação de seus princípios dentro da organização. Sua intenção, como coloca Patrícia Peck Pinheiro[107], além da proteção de dados pessoais dos cidadãos brasileiros, é a de fornecer um guia para organizações de como este tratamento de dados deve ser feito, e permitir maior segurança jurídica para as mesmas. Com uma direção objetiva, a LGPD permite, então, uma centralização dos regulamentos de proteção de dados, e a facilitação de sua implementação para as organizações.

A LGPD estabelece em seu art. 52 que a adoção de um sistema de compliance possui impacto na aplicação da multa pecuniária, servindo como redutor da multa, ainda que não vá eximir a empresa da responsabilização. É possível, desta forma, perceber que o objetivo do legislador é justamente o de incentivar a implementação de sistema de compliance digital voltada para a proteção de dados, como estabelece Donda.[108]

De acordo, ainda, com seu parágrafo 7º, há mais uma conexão com programas de compliance, de forma que investigações realizadas em função de possíveis vazamentos de dados podem prevenir a aplicação de penalidades, caso realizadas antecipadamente:

> 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.

13.709/2018 e as alterações da Lei n. 13.853/2019), o Marco Civil da Internet (Lei n. 12.965/2014) e as sugestões de alteração do CDC (PL 3.514/2015). São Paulo: Almedina, 2020.

[106] BRASIL. **Lei 13.853, de 8 de julho de 2019.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: mar. 2023.

[107] PINHEIRO, Patricia Peck**. Proteção de dados pessoais comentários à Lei n. 13.709/2018:** (LGPD). 3. ed.São Paulo: Saraiva Jur, 2021.

[108] DONDA, Daniel. **Guia prático de implementação da LGPD:** tudo que sua empresa precisa saber para estar em conformidade. São Paulo: Labrador, 2020.

Ainda que não adote padrões específicos para segurança dos dados, a LGPD estabelece sobre medidas gerais que podem ser adotadas, em seu artigo 50. Estabelece, desta forma, que os controladores e operadores podem formular regras de boas-práticas e governança, as estabelecendo em diversos aspectos do funcionamento da organização.[109] Em seu parágrafo 1º, ainda, coloca que, ao estabelecer estas regras, o controlador e o operador devem levar em consideração todo o escopo da operação, bem como balancear a gravidade dos riscos e os benefícios decorrentes do tratamento dos dados. Em seu parágrafo 2º, inciso I, estabelece diversas condições mínimas para o dito programa de governança em privacidade[110]:

> Art. 50., § 2º, 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;

Perceptível, desta forma, a intenção do legislador de prever estas medidas de auto-regulação dentro da LGPD, como coloca Patrícia Peck Pinheiro[111]. No entanto,

---

[109] 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. (BRASIL. **Lei n. 13.709 de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: jan. 2023.)

[110] BRASIL. **Lei n. 13.709 de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: jan. 2023.

[111] PINHEIRO, Patricia Peck**. Proteção de dados pessoais comentários à Lei n. 13.709/2018:** (LGPD). 3. ed.São Paulo: Saraiva Jur, 2021.

em seu inciso II do parágrafo 2º, bem como em seu parágrafo 3º, o artigo 50 prevê medidas de monitoramento para esta auto-regulação, na forma de autorização para a Autoridade Nacional de Proteção de Dados requisitar, a qualquer momento, que a organização demonstre a efetividade de seu programa de governança, bem como de publicar e atualizar regras de boas práticas e governança para proteção de dados e padrões técnicos mínimos para os operadores.

Se utilizando destes requisitos mínimos, a implementação de um programa de compliance deve envolver o manejo de indicadores que permitam calcular seu sucesso, bem como entender diversos aspectos de tecnologia da informação com relação a seus processos internos, como os softwares utilizados, os métodos de tratamento dos dados, entre outros. Desta forma, é possível alinhar o programa de compliance com as diretivas da Lei Geral de Proteção de Dados de maneira adequada, e com a criação dos controles internos necessários para tal, como estabelecem Márcio Cots e Ricardo Oliveira.[112]

[112] COTS, Márcio; OLIVEIRA, Ricardo. **Lei geral de proteção de dados pessoais comentada**. São Paulo: Thomson Reuters, 2019.

4 A IMPORTÂNCIA DA ADEQUAÇÃO DOS ESCRITÓRIOS DE ADVOCACIA À LGPD

4.1 A ADVOCACIA 4.0

Devido às transformações trazidas pela nova era digital, a sociedade em todos seus aspectos se viu obrigada a adaptar para o novo conceito. A advocacia, logo, também se viu diante de um impasse: como atualizar uma profissão com tantas raízes tradicionais para os tempos modernos? A advocacia 4,0, desta forma, procura identificar estas transformações afetando o direito contemporâneo, advindos da dita quarta revolução industrial.

Esta quarta revolução industrial, no caso, vem como uma sucessão dos movimentos de reforma da produção conhecidos como revoluções industriais, e a culminação de diversas tecnologias adentrando no campo da manufatura, especialmente nas questões de automação e troca de dados. Klaus Schwabb, fundador do Fórum Econômico Mundial, propõe em seu livro *A Quarta Revolução Industrial*[113] que esta revolução iria além da simples inovação da cadeia de produção e elementos informatizados aliados aos processos, mas sim um verdadeiro sistema interconectado que se estende além da manufatura para a criação de uma cadeia global e flexível, misturando desta forma sistemas físicos e virtuais.

Schwabb supõe, desta forma, que são três os principais fatores que nos permitem identificar esta nova etapa da industrialização: esta velocidade com que a inovação se difunde, acelerando o processo tecnológico e assim beneficiando a sociedade; a profundidade das novas mudanças trazidas por uma constante busca por inovação, sentidas por todo o sistema; e finalmente a enorme mudança sistêmica vivenciada pela população no geral, sem barreiras de fronteiras, idiomas e culturas, mudando completamente a organização social para a qual estamos evoluindo.

Desta forma, como coloca Alves[114], a advocacia 4.0 propõe identificar estas transformações causadas pelo impacto da quarta revolução industrial, que fundamentalmente modificou diversas atividades praticadas dentro do âmbito

[113] SCHWABB, Klaus. **A quarta revolução industrial**. São Paulo: Edipro, 2015.
[114] ALVES, Lucélia de Sena. Advocacia na quarta revolução industrial e a necessidade da presença digital. **Revista Direito, Tecnologia e Saúde,** v. 9, 2018.

jurídico, e em especial advocatício., Além das modificações legais em si, houve uma enorme modificação no modo de trabalho e atuação dos escritórios de advocacia, que devem atuar de maneira digitalizada, com softwares específicos, e aliar esta tecnologia com a produtividade do escritório, se adaptando a esta nova forma de trabalho.

A tecnologia, desta forma, se demonstra uma aliada do profissional, e não seu substituto, como coloca Fernanda Bragança[115]. Automatizar tarefas burocráticas manuais, deixando os profissionais envolvidos com a parte intelectual e estratética que envolva conhecimento jurídico, otimizando o tempo e potencialmente aumentando a qualidade dos serviços e redução de seus custos.

Ainda, é possível promover esta análise jurídica com precisão, estruturando informações por meio de algoritmos que tem como input a jurisprudência e analisando normas e súmulas, possivelmente prevendo desfechos de processos. Fausto de Martins[116] afirma que a inteligência artificial aplicada ao Direito caminha a passos crescentes, e que, especialmente com o chamado *machine learning*, a prática jurídica evoluirá em prol de todos os envolvidos, utilizando a tecnologia para tratamento de dados jurídicos com segurança.

Desta forma, é possível perceber que a advocacia 4.0 traz uma mudança de comportamento para os escritórios de advocacia, modificando de forma significativa as relações entre as partes envolvidas e revolucionando o mercado jurídico e advocatício como um todo. Com a automatização dos sistemas, realizando diversas tarefas que costumavam ser manuais, proporciona oportunidades para aprendizado profissional em tarefas estratégicas.

No entanto, com a quantidade de modificações trazidas por esta evolução digital, há também a necessidade de qualificação dos escritórios de advocacia com relação à utilização de toda a tecnologia, como estabelece Longhi.[117] A capacitação, neste caso, não apenas para utilização de inteligência artificial para auxílio nos processos, ou de novos softwares de acompanhamento e auxílio jurídico, mas em como transformar adequadamente o escritório em termos de processos internos

---

[115] BRAGANÇA, Fernanda; BRAGANÇA, Laurinda Fátima. Revolução 4.0 no poder judiciário: levantamento do uso de inteligência artificial nos tribunais brasileiros. **Revista da Seção Judiciária do Rio de Janeiro**, v. 23, n. 46, 2019.

[116] SANCTIS, Fausto M. **Inteligência artificial e direito.** São Paulo: Grupo Almedina, 2020.

[117] LONGHI, Maria Isabel Carvalho Sica; COSTA-CORRÊA, André. **Direito e novas tecnologias.** São Paulo: Almedina, 2020.

para atingir um padrão de segurança digital na utilização de todas estas ferramentas e tecnologias.

Assim, com este advento da advocacia 4.0, a questão da proteção e tratamento de dados dentro de escritórios de advocacia requer especial atenção. A virtualização dos processos judiciais, bem como dos próprios processos internos dos escritórios, abre margem para diversos riscos inexistentes anteriormente, como vazamentos de dados e ataques cibernéticos, bem como a própria brecha para erro humano dentro dos sistemas. Realizar a capacitação da equipe, e realizar um adequado planejamento com relação à segurança digital é essencial. Para isto, a própria regulação da profissão já fornece requisitos mínimos para esta atuação digital, como visto adiante.

4.2 A LGPD COMO FONTE DE REGULAÇÃO DA ATIVIDADE ADVOCATÍCIA

Dentro da atividade advocatícia, é especialmente desafiador se conformar com a nova regulação, pelo fato de dados pessoais serem utilizados em todas as atividades do cotidiano dos escritórios, independentemente da matéria que estes trabalhem. Se utilizam de dados de clientes, colaboradores, terceiros envolvidos, processos judiciais, empresas, entre tantos outros que participam da relação jurídica de atuação do escritório em questão. Como coloca Lima[118]:

> O exercício da advocacia lida com o tratamento de dados pessoais, seja pela coleta, tornando visível quando o cliente repassa suas informações para ser alocada em uma peça processual, pelo arquivamento, quando fica salva as informações em computadores pertencentes ao escritório, pela modificação, quando há mudanças cadastrais das informações, pela transferência, com o repasse de dados entre advogados parceiros, pela difusão aparente, quando é transmitida a peça para o poder judiciário quando contém as informações pessoais, além de outras formas que necessitam de consentimento pelo titular.

Há, ainda, uma relação única entre advogado e cliente, pautada pelo Código de Ética e Disciplina da Ordem dos Advogados do Brasil – OAB, que traz justamente a conduta adequada a ser tomada na prestação de serviços de cunho jurídico. Como

[118] LIMA, Vinícius Albuquerque**. A lei n° 13.709/18 (Lei Geral de Proteção aos Dados Pessoais – LGPD) e sua relação com a advocacia:** o advogado e seus deveres quanto ao tratamento dos dados pessoais. 2021. Disponível em: https://jus.com.br/artigos/94515/a-lei-n-13-709-18-lei-geral-de-protecao-aos-dados- pessoais-lgpd-e-sua-relacao-com-a-advocacia-o-advogado-e-seus-deveres-quanto- ao- tratamento-dos-dados-pessoais. Acesso em: dez. 2022.

coloca Kageyama[119], “A relação do advogado com o cliente é sempre permeada pela confiança, pois o cliente deposita no advogado todos os seus medos, anseios, rancores, conquistas, inclusive seu patrimônio”.

A atividade advocatícia utiliza os dados pessoais de maneira diversa ao comércio em geral. Enquanto empresas e a indústria em geral utiliza os dados justamente para aumentar suas vendas ou otimizar seus processos, os escritórios os utilizam para auxiliar seus clientes nas demandas jurídicas, pois são necessários para resolver as mesmas, como coloca Hallberg[120]. Ainda, é dever dos tribunais fazer o trâmite destas demandas de modo público, salvo eventual caso que requeira segredo de justiça, mas resguardando dados pessoais das partes.

De acordo com Colombo[121], os clientes dos escritórios de advocacia são os titulares deste direito fundamental à proteção de dados, devendo o advogado se pautar pela proteção dos mesmos através das novas normas, especialmente com relação ao princípio da necessidade, evitando utilizar dados desnecessários para a demanda de seu cliente. Ainda que o escritório não possua como finalidade o tratamento dos dados, deve fornecer a completa segurança e proteção dos mesmos.

Ainda, traz que o consentimento dado é atrelado à finalidade inicial, o que é corroborado pelo próprio Código de Ética e Disciplina da Ordem dos Advogados do Brasil, não podendo ser desvirtuado seu uso. No entanto, o mesmo código também permite a utilização dos dados no “interesse legítimo” do cliente, que seria justamente o de concluir a demanda para a qual foi contratado originalmente. Para este fim, deve agir com a devida presteza, tomando as medidas adequadas para esta proteção dos dados através de boas práticas, transparência e cuidado ao solicitar dados desnecessários.

O próprio sigilo é inerente à atividade advocatícia, sendo esta pautada pela boa-fé e confiança na relação entre advogado e cliente. O profissional, logo, deve

---

[119] KAGEYAMA, André. **Guia comentado do estatuto da advocacia e da OAB (Lei 8.906/94**). São Paulo: Aurum, 2020.

[120] HALLBERG, Fernando Bottega. **Gestão de arquivos em nuvem na era da LGPD com enfoque em um escritório de advocacia**. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/13546/1/FERNANDO_BOTTEGA_HALLBERG-%5b68352-685-5 953491%5dEstudo_de_Caso__GestAo_em_Ti_-_2021_-_Fernando_Bottega_Hallberg.pdf. Acesso em: jan. 2023.

[121] COLOMBO, Cristiano. Do sigilo profissional da advocacia à proteção de dados pessoais: princípios da lgpd e medidas concretas. *In:*I CONGRESSO INTERNACIONAL DA ADVOCACIA EXTRAJUDICIAL E DIGITAL, 1, 2021, São Paulo. VECCHIO, Fabrizio Bon; XIMENES, Raquel Letícia Cúrcio (Org.). **Caderno de resumos exandidos.** Porto Alegre: Instituto Ibero-americano de Compliance, 2021.

fornecer completo sigilo e confidencialidade para seus clientes, sendo a quebra deste apenas em situações extremas, determinadas por juiz competente. O próprio Estatuto da OAB[122] estabelece, em seu artigo 25: “O sigilo profissional é inerente à profissão, impondo-se o seu respeito, salvo grave ameaça ao direito à vida, à honra, ou quando o advogado se veja afrontado pelo próprio cliente e, em defesa própria, tenha que revelar segredo”.

Como medidas iniciais para esta adequação à Lei Geral de Proteção de Dados dentro de escritórios de advocacia, é recomendável a criação de um comitê interno próprio justamente para lidar com toda a questão da governança digital. Várias atividades, por sua vez, devem ser modificadas também de imediato, como processos internos que lidem com fornecedores e terceiros, eventuais estratégias de marketing, canais de comunicação com os clientes, entre diversos outros que se utilizam destes dados[123].

A elaboração de um *roadmap* de medidas a serem implementadas, traz Donda[124], se demonstra essencial para que organizações consigam adequadamente cumprir não apenas as exigências formais da nova regulação, mas também estrategicamente reduzir potenciais riscos já existentes de acordo com sua estrutura interna própria.

Dentro da área do direito, ainda, existem diversos ramos de atuação para escritórios de advocacia, com cada ramo possuindo suas peculiaridades. Desta forma, é essencial personalizar as medidas para as exigências de forma que todas estas peculiaridades estejam englobadas, especialmente no que tange ao termo de consentimento de uso de dados.

Para escritórios que lidam com matérias onde haja menores de dezoito anos envolvidos, há uma série de medidas adicionais a serem tomadas de forma preventiva, bem como em termos de consentimento. A própria Lei Geral de Proteção de Dados engloba proteção adicional a este público, inserindo em seu artigo 14 que os dados de menores devem ser utilizados apenas em seu “melhor interesse”. Deve,

---

[122] BRASIL. **Lei n. 8.906, de 4 de julho de 1994.** Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8906.htm. Acesso em: jan. 2023.

[123] QUAL O IMPACTO da LGPD no dia a dia dos escritórios? 2019. Disponível em: https://digital.fenalaw.com.br/2019/04/16/impacto-lgpd-escritorios/. Acesso em: fev. 2023.

[124] DONDA, Daniel. **Guia prático de implementação da LGPD:** tudo que sua empresa precisa saber para estar em conformidade. São Paulo: Labrador, 2020.

assim, ser feita esta adaptação, essencial para a proteção do menor de idade, como trazem Soares, Santos e Jesus.[125]

Dentro do campo previdenciário, há uma atuação comum dos escritórios, de maneira geral, centrado em uma demanda de pessoa física, no caso, o segurado, e dados utilizados de diversos de seus aspectos, como de saúde, do trabalho, financeiro, entre diversos outros próprios do ramo previdenciário, além do mesmo para seus dependentes, como coloca Veiga[126]. Há, justamente, alta demanda por dados altamente sensíveis, com elevado risco para a operação, e medidas adicionais devem ser tomadas para resguardar a integridade dos mesmos.

Tratando, também, com matérias relacionadas à saúde, a LGPD trouxe diversas considerações, elevando os dados dos pacientes a um patamar altamente elevado em relação à sua proteção, como a exigência de os dados serem apagados em certas condições.

Ainda, estabelece uma exigência de transparência única para o campo, para que haja o maior número de informações possível para os pacientes. Escritórios que atuam dentro do campo de direito da saúde devem estar atentos a todas estas questões próprias do ramo, especialmente em termos de adequação de seus processos internos, bem como do consentimento dos envolvidos, como coloca Rampazzo.[127]

Desta forma, com a advocacia englobando diversas matérias, e com diversas necessidades em termos de legislação de proteção de dados, é essencial que o planejamento das medidas a serem tomadas englobe ao máximo estes diferentes ramos, especialmente no que se relaciona ao termo de consentimento utilizado.

---

[125] SOARES, Ellen Aamanda Gomes; SANTOS, Pedro Otto Souza; JESUS, Tâmara Silene Moura de. LGPD e a Proteção de Dados pessoais das crianças e adolescentes no ordenamento jurídico brasileiro: o dilema da coleta de dados e a obrigatoriedade do consentimento dos pais. **Brazilian Jourrnal of Development,** v. 7, n. 8, 2021.

[126] VEIGA, T. M. A LGPD nos escritórios de advocacia previdenciária: o registo das operações de tratamento de dados e o conceito de escritório digital como medidas de base para a conformidade. **Revista Jurídica da Escola Superior de Advocacia OAB de Santa Catarina,** v. 1, n. 1, 2021.

[127] RAMPAZZO, F. **Consentimento do paciente no direito médico:** validade, interpretação e responsabilidade. São Paulo: Foco, 2021.

4.3 RELAÇÃO DE ESCRITÓRIOS DE ADVOCACIA COM CLIENTES E COLABORADORES

A atividade da advocacia está atrelada à Ordem dos Advogados do Brasil, ou OAB. Esta é uma instituição pública, com personalidade jurídica própria, que exerce papel fundamental na profissão, sendo responsável tanto pelo registro quanto pela fiscalização dos advogados. Possui um Código de Ética[128] próprio, que regula o comportamento profissional dos mesmos. Este código de ética estabelece justamente os deveres dos advogados, como defensores do Estado democrático de Direito, conforme art. 2º do mesmo.

Este código de ética e disciplina estabelece diversas orientações sobre as relações entre advogados e clientes. Esta relação é essencial para os serviços de advocacia, como coloca Kageyama: “A relação do advogado com o cliente é sempre permeada pela confiança, pois o cliente deposita no advogado todos os seus medos, anseios, rancores, conquistas, inclusive seu patrimônio”[129].

Esta ordem jurídica entre advogado e cliente, logo, deve pautar- se por uma confiança recíproca, sendo uma peça fundamental para a relação. A própria prestação de serviços jurídicos se dá por interesse público, sendo que o advogado desempenharia um papel essencial na administração da justiça. Com esta natureza jurídica, se demonstra essencial o exercício da ética profissional dos mesmos, como coloca Biela Jr.[130]

Em seu capítulo II, desta forma, o Código de Ética da OAB estabelece diretrizes a serem tomadas em suas relações com clientes. Seu artigo 8º prega pela transparência na relação, afirmando que o advogado deve sempre informar o cliente dos riscos e consequências de sua pretensão, bem como seu artigo 12 estabelece que o advogado não pode deixar o cliente em desamparo. Em suma, deve ser uma relação profissional e ética, onde o advogado venha a prestar seu serviço de maneira adequada, sempre com os melhores interesses do cliente.

---

[128] ORDEM DOS ADVOGADOS DO BRASIL. **Código de ética e disciplina da Ordem dos Advogados do Brasil**. Disponível em: https://www.oab.org.br/content/pdf/legislacaooab/codigodeetica.pdf. Acesso em: mar. 2023.

[129] KAGEYAMA, André. **Guia comentado do estatuto da advocacia e da OAB (Lei 8.906/94**). São Paulo: Aurum, 2020.

[130] BIELA JÚNIOR. **Curso de ética profissional para advogados:** de acordo com o novo código de ética, com o Novo CPC e com as súmulas do Conselho Federal da OAB. São Paulo: LTR, 2018.

Para isto, estabelece um adequado sigilo profissional, especificamente em seu capítulo III, artigo 25. Desta forma, se fortalece a relação, baseada em confiança, com uma segurança para o cliente de que o profissional não irá divulgar informações confidenciais, apenas em casos extremos, como grave ameaça à vida ou em defesa própria, de acordo com o mesmo artigo.

Esta confidencialidade é essencial por parte do advogado, em razão de seu exercício profissional. Coloca Paulo Lôbo[131] que é através dela que os clientes possuem a segurança de estarem amparados pelo advogado, independentemente daquilo que lhes informarem, e a garantia de que estas informações serão utilizadas com as melhores intenções por parte do profissional, e que o cliente não necessitará omitir fatos relevantes a seu pleito jurídico.

Desta forma, salienta-se a confiança recíproca que deve existir na relação entre advogado e cliente. O advogado, ao exercer seu mandato, atua justamente como o patrono da parte, devendo ser franco com relação a potenciais riscos e consequências, buscando sempre uma relação transparente e clara, relevando os interesses do cliente, mas o guiando por meio de seu conhecimento e experiência jurídicos, como coloca Nalini.[132]

Com relação à natureza da relação profissional entre advogado e cliente, esta é regida pelo Estatuto da Advocacia[133], a Lei 8.906, e não possui incidência do Código de Defesa do Consumidor, conforme entendimento do Superior Tribunal de Justiça[134]:

> INCIDÊNCIA DO CDC. DEFICIÊNCIA NA PRESTAÇÃO DOS SERVIÇOS.NEGATIVA DE QUE FORA EFETIVAMENTE CONTRATADO PELO CLIENTE. DANOS MORAIS. CARACTERIZAÇÃO. SÚMULA 7/STJ. PRESCRIÇÃO. NÃO OCORRÊNCIA. RECURSO ESPECIAL IMPROVIDO.1.- **As relações contratuais entre clientes e advogados são regidas pelo Estatuto da OAB, aprovado pela Lei n. 8.906/94, a elas não se aplicando o Código de Defesa do Consumidor**. Precedentes. [...] (REsp 1.228.104/PR, Rel. Ministro SIDNEI BENETI, TERCEIRA TURMA,julgado em 15/03/2012, DJe 10/04/2012
>
> RECURSO ESPECIAL. PROCESSUAL CIVIL. EMBARGOS DE DECLARAÇÃO. JULGAMENTO DA APELAÇÃO. INEXISTÊNCIA DE

[131] LÔBO, Paulo. **Comentários ao Estatuto da Advocacia e da OAB**. 14. ed. São Paulo: SaraivaJur, 2022.
[132] NALINI, Jose Renato. **Ética geral e profissional:** á ética do advogado. 13. ed. São Paulo: LTR, 2016.
[133] BRASIL. **Lei n. 8.906, de 4 de julho de 1994.** Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8906.htm. Acesso em: jan. 2023.
[134] BRASIL. Superior Tribunal de Justiça. REsp 1.228.104/PR. Terceira Turma. Relator: Ministro Sidnei Beneti. Julgado em: 15 mar. 2012. **DJe** 10 abr. 2012.

> VÍCIO. JULGAMENTO DE AGRAVO RETIDO. OMISSÃO. ART. 535, II, DO CPC. VIOLAÇÃO CONFIGURADA. CONTRATO DE SERVIÇOS ADVOCATÍCIOS. CDC. INAPLICABILIDADE. INTERPRETAÇÃO DE CLÁUSULA CONTRATUAL. SÚMULA N. 5/STJ. EFEITOS DA ADI N. 2.010-2. MATÉRIA VENTILADA APENAS NO VOTO VENCIDO. SÚMULA N. 320/STJ. FALTA DE PREQUESTIONAMENTO. [...] 3. **O CDC não se aplica à regulação de contratos de honorários advocatícios.** 4. A interpretação dada pelo acórdão recorrido a cláusulas contratuais deve ser mantida quando, apesar de mencionado, o CDC não tenha sido utilizado como critério interpretativo (Súmula n. 5/STJ). 5. "A questão federal somente ventilada no voto vencido não atende ao requisito do prequestionamento" (Súmula n. 320/STJ). 6. Recurso especial conhecido em parte e parcialmente provido. REsp 1123422/PR, Rel. Ministro JOÃO OTÁVIO DE NORONHA, QUARTATURMA, julgado em 04/08/2011, DJe 15/08/2011.

Desta forma, não é aplicável às relações contratuais entre clientes e advogados o Código de Defesa do Consumidor, sendo este regido pelo Estatuto da Ordem dos Advogados do Brasil, justamente pela natureza única desta relação, caracterizada pela notória confiança.

Quanto à relação entre o escritório de advocacia e colaboradores, esta é regida pela legislação trabalhista, majoritariamente pela Consolidação das Leis do Trabalho, o Decreto-Lei 5.452[135]. Desta forma, há a subordinação jurídica, onde o empregado deve subeter-se ao comando do empregador, e este deve observar todas as providências necessárias para a formação lícita desta relação contratual.

A Lei Geral de Proteção de Dados, por sua parte, não esboçou incidência dentro do Direito do Trabalho, no entanto, devido a esta relação entre as partes e suas peculiaridades, a mesma deve ser observada[136]:

> Sua incidência sobre o Direito do Trabalho é manifesta, uma vez que a relação jurídica desenvolvida entre empregado e empregador é repleta de coleta e processamento de dados pessoais, iniciando-se o tratamento mesmo antes do estabelecimento do vínculo empregatício, permanecendo o processo durante o curso da relação laboral e se estendendo para mesmo após o encerramento do contrato de trabalho.

Já quanto à sua relação com terceiros, se demonstra necessário compreender a natureza da atividade advocatícia através duas regras deontológicas

---

[135] BRASIL. **Decreto-lei 5.452, de 1º de maio de 1943**. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm. Acesso em: fev. 2023.

[136] COLOMBO, Cristiano; BOCHI, Igor; BRONFMANN, José Leopoldo. Lei Geral de Proteção de Dados aplicada às relações de trabalho: ponderações quanto ao direito do esquecimento e o direito à informação. *In:* CONGRESSO ÍBERO-AMERICANO DE DOCENTES E INVESTIGADORES EM DERECHO E INFORMATICA, 22, 2022, Salta. Disponível em: https://drive.google.com/file/d/1lA2xawnGSwBM-cc-heRve4fjWBGAwiH4/view. Acesso em 2023. p. 37.

fundamentais, estabelecidas em regulamento através do próprio Código de Ética e Disciplina da Ordem dos Advogados do Brasil. Ainda, estas normas deontológicas se aplicam a todas as relações do advogado, e não apenas com terceiros com quem não possui relação direta, de acordo com Lôbo.[137]

Em seu Título I, “Da Ética do Advogado”, Capítulo I, “Das Regras Deontológicas Fundamentais”, o CED estabelece o que seria o eixo moral da profissão de advocacia, em seu artigo 2º, colocando que o principal objetivo de um advogado deve ser o de defender o Estado Democrático de Direito, os Direitos Humanos, as garantias fundamentais, a cidadania, moralidade, a justiça e a paz social.

Ainda, estabelece os deveres do advogado, ainda em seu artigo 2º, aqui elencados os mais relevantes para o tópico:

> Art. 2º Parágrafo único. São deveres do advogado:
> I – preservar, em sua conduta, a honra, a nobreza e a dignidade da profissão, zelando pelo seu caráter de essencialidade e indispensabilidade;
> II – atuar com destemor, independência, honestidade, decoro, veracidade, lealdade, dignidade e boa-fé;
> III – velar por sua reputação pessoal e profissional;
> V – contribuir para o aprimoramento das instituições, do Direito e das leis;
> IX – pugnar pela solução dos problemas da cidadania e pela efetivação dos seus direitos individuais, coletivos e difusos, no âmbito da comunidade.

Ainda, seu artigo 3º prega que o advogado deve ter consciência de que o Direito é apenas um meio de mitigar as desigualdades para o encontro de soluções justas, e que a lei é um instrumento para garantir a igualdade de todos. Desta forma, é perceptível que o advogado serve como instrumento para a proteção do interesse público, devendo servir à Justiça acima de tudo. Logo, a relação que os advogados possuem com terceiros, ainda que não relacionados diretamente, deve ser pautada em respeito e consideração, como coloca Nalini[138]. O profissional da advocacia deve se comportar com relação a estes de maneira profissional, sempre com boa-fé e dignidade,de forma a honrar sua classe.

---

[137] LÔBO, Paulo. **Comentários ao Estatuto da Advocacia e da OAB**. 14. ed. São Paulo: SaraivaJur, 2022.

[138] NALINI, Jose Renato. **Ética geral e profissional:** á ética do advogado. 13. ed. São Paulo: LTR, 2016.

Parte disto, coloca Nalini[139], é justamente a compreensão de que, atuando no ramo da advocacia, se entrará em contato com dados e informações confidenciais de diversos terceiros, e estes devem ser respeitados e tratados com a cautela exigida. Ainda, a atividade da advocacia é incompatível com a mercantilização, como estabelece o artigo 5º do Código de Ética e Disciplina da OAB. Logo, estes dados e informações de terceiros devem ser utilizados de maneira ética, apenas para alcançar os objetivos do cliente, e sempre dentro do que é legalmente permitido.

Além da natureza da relação, importante também relevar o modo como ocorre a responsabilização dentro da prática da advocacia. O advogado, sendo considerado profissional liberal, é responsabilizado por danos que vir a ocasionar ao longo do exercício de sua profissão, como coloca o artigo 32 do Estatuto da Ordem dos Advogados. Sua conduta, tanto comissiva quanto omissiva, gera consequências relevantes para seus clientes, e a partir destas que se releva sua responsabilidade, como colocam Cristiano de Farias e Felipe Braga Netto[140]:

> O advogado – assim como o médico, por exemplo – pode responder por ações ou omissões. O advogado que deixa de propor ação ou interpor recurso, que deixa de aconselhar o cliente quando o conselho se fazia absolutamente necessário, poderá incidir em hipótese de dano indenizável. Usamos o verbo condicional porque os dilemas que envolvem a responsabilidade civil não aceitam solução em abstrato. Só os casos concretos darão a chave hermenêutica adequada, e isso nem sempre é simples. Ademais, não basta que o advogado tenha agido mal: é preciso que a essa ação (ou omissão) desastrada se junte um dano indenizável. E mais: que o nexo causal cimente o dano à conduta.

Esta responsabilização civil do advogado advém de diversas legislações: do Código Civil, em seus artigos 186 e 197; do Estatuto da OAB, previamente citado, e do Código de Defesa do Consumidor, dependendo do caso concreto. Ainda, esta responsabilidade seria subjetiva, pois a averiguação da culpa é necessária para sua efetivação; Desta forma, os casos que envolvem a responsabilização do profissional são as que envolvem imprudência, negligência, imperícia ou atos ilícitos.

A Lei Geral de Proteção de Dados, no entanto, estabelece seu próprio regime de responsabilidade para operadores, intitulada “Da Responsabilidade e do

---

[139] NALINI, Jose Renato. **Ética geral e profissional:** á ética do advogado. 13. ed. São Paulo: LTR, 2016.

[140] NETTO, Felipe Braga; FARIAS, Cristiano de. **Manual de direito civil**. 2. ed. São Paulo: Saraiva Jur, 2022.

Ressarcimento de Danos", na seção III de seu capítulo VI. No entanto, dependendo da relação jurídica no caso concreto, ela deve ceder espaço a normas mais específicas, como, por exemplo, o Código de Defesa do Consumidor, como estabelece a LGPD em seu artigo 45.

Nesta seção que trata da responsabilidade, para configurar tal, é necessário que a atividade de tratamento viole especificamente a legislação de proteção de dados, tendo como base estrutural a própria LGPD. Em seu artigo 46, estabelece que os agentes de tratamento devem adotar as medidas adequadas de segurança, técnicas e administrativas, para assegurar a proteção dos dados pessoais. Desta forma, como coloca Capanema [141] , é possível detectar dois tipos de responsabilização civil na LGPD: violação de normas jurídicas, dentro do microssistema de proteção de dados, e violação de normas técnicas, voltadas à segurança e proteção dos dados pessoais. Caracteriza-se a responsabilidade civil, desta forma, se a violação possuir como consequência dano material ou moral.

O artigo 42, por sua vez, restringe a responsabilidade ao operador ou controlador. A responsabilidade será solidária apenas nos casos do parágrafo 1º, inciso I, que são quando há o descumprimento de legislação de proteção de dados, ou quando o operador não seguir as instruções do controlador. Ainda, seu inciso II estabelece que todos os controladores que estiverem envolvidos no tratamento responderão solidariamente.

Com relação à exclusão da responsabilidade civil, suas hipóteses se encontram em seu artigo 43. O inciso I estabelece que, caso o agente não tenha realizado o tratamento dos dados que foi atribuído ao titular, não será responsável. Esta hipótese se aproxima, desta forma, da figura da ilegitimidade passiva, onde não há vínculo entre o operador e o titular dos dados, como coloca Capanema.[142]

Já em seu inciso II, traz que não haverá responsabilidade em situações onde o agente realizou o tratamento, no entanto, não violou legislação de proteção de dados. Esta hipótese, ainda, deve ser considerada juntamente com a análise de possível violação de norma técnica. Por último, o inciso III estabelece a culpa exclusiva do titular ou de terceiro, caso o dano tenha sido causado por ingerência do titular ou de terceiro.

---

[141] CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. **Cadernos Jurídicos,** São Paulo, 2021.

[142] CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. **Cadernos Jurídicos,** São Paulo, 2021.

Com relação aos escritórios de advocacia, caracterizados legalmente como sociedade simples, de acordo com o artigo 15 do Estatuto da Advocacia[143], se aplica a responsabilização trazida pela Lei Geral de Proteção de Dados, que institui, em seu artigo 1º que a lei se aplica a qualquer tratamento de dados pessoais por pessoa jurídica de direito privado.

Desta forma, a responsabilidade civil trazida pela Lei Geral de Proteção de Dados atua de forma complementar à responsabilização na profissão da advocacia, respondendo civilmente nos termos da mesma apenas com relação a danos causados pelo tratamento dos dados pessoais.

4.4 REGULAÇÃO DO USO DE DADOS PARA ESCRITÓRIOS DE ADVOCACIA

Advogados devem sempre manter em mente o melhor interesse do cliente, essencial para a prestação de serviços de advocacia. Para alcançar esta excelência em prestação de serviços de advocacia, no entanto, é necessário utilizar os dados de seus clientes, sempre com o melhor interesse do mesmo em mente, como coloca Nalini.[144] Antes mesmo da digitalização dos processos, os dados dos clientes ainda eram necessários de serem armazenados para sua utilização.

Em uma sociedade virtual, ainda, com os processos tramitando de forma digitalizada, estes dados são essenciais de serem armazenados de maneira adequada e segura, se pautando por regras de governança corporativa para garanti-la, como coloca Lima:[145]

> O exercício da advocacia lida com o tratamento de dados pessoais, seja pela coleta, tornando visível quando o cliente repassa suas informações para ser alocada em uma peça processual, pelo arquivamento, quando fica salva as informações em computadores pertencentes ao escritório, pela modificação, quando há mudanças cadastrais das informações, pela transferência, com o repasse de dados entre advogados parceiros, pela difusão aparente, quando é transmitida a peça para o poder judiciário quando contém as informações pessoais, além de outras formas que necessitam de consentimento pelo titular.

---

[143] BRASIL. **Lei n. 8.906, de 4 de julho de 1994.** Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8906.htm. Acesso em: jan. 2023.

[144] NALINI, Jose Renato. **Ética geral e profissional:** á ética do advogado. 13. ed. São Paulo: LTR, 2016.

[145] LIMA, Vinícius Albuquerque**. A lei n° 13.709/18 (Lei Geral de Proteção aos Dados Pessoais – LGPD) e sua relação com a advocacia:** o advogado e seus deveres quanto ao tratamento dos dados pessoais. 2021. Disponível em: https://jus.com.br/artigos/94515/a-lei-n-13-709-18-lei-geral-de-protecao-aos-dados- pessoais-lgpd-e-sua-relacao-com-a-advocacia-o-advogado-e-seus-deveres-quanto- ao- tratamento-dos-dados-pessoais. Acesso em: dez. 2022.

De forma a englobar boas práticas, ainda que com relação a bens digitais, advogados devem pautar sua conduta pelo Código de Ética da Ordem dos Advogados do Brasil. Acerca deste, se estabelecem diversas diretrizes que devem ser seguidas também com relação à proteção de dados nos escritórios, de maneira complementar a legislações diversas, como a própria Lei Geral de Proteção de Dados. Ainda, há deveres por parte dos advogados que complementam os deveres da LGPD, como o próprio sigilo profissional.

O Código de Ética, desta forma, prevê em seu capítulo III que deve haver um sigilo profissional adequado por parte do advogado. Seu artigo 25 estabelece que o sigilo profissional é inerente à profissão, e suas únicas exceções são ameaças à integridade física e mental do advogado, e sempre se limitando ao interesse da causa, bem como seu artigo 26 proíbe que advogados testemunhem em processos que possua relação, direta ou indireta.

Este sigilo profissional não apenas é um dever do advogado, como também um direito, como coloca Paulo Lobo[146]. Ostenta, logo, natureza pública, pois é estabelecido por interesse geral, garantindo a plenitude de defesa do direito do cidadão, indo além do simples interesse do cliente imediato. Logo, este dever de sigilo se estende não apenas à confidência do cliente, mas também às do adversário, colaboradores, terceiros, ou qualquer outro envolvido no caso. Este pode apenas ser revisto em casos onde haja perigo imediato, estado de necessidade, ou ainda quando acusado pelo próprio cliente. Logo, são exceções extremas, dada sua importância para a profissão.

O dever de sigilo, logo, precede a legislação específica de proteção de dados, sendo a principal proteção concedida aos dados utilizados na atividade de advocacia, buscando justamente evitar o vazamento de informações confidenciais e que possam causar prejuízo ou dano a seus titulares, sejam eles clientes, colaboradores ou terceiros, postula Lobo.[147]

Ainda, o próprio Conselho Federal da Ordem dos Advogados do Brasil lançou, em 2015, uma resolução que proíbe divulgar, ou permitir a divulgação, de listas de clientes e demandas. Desta forma, já vedando de maneira anterior à Lei Geral de

[146] LÔBO, Paulo. **Comentários ao Estatuto da Advocacia e da OAB**. 14. ed. São Paulo: SaraivaJur, 2022.
[147] LÔBO, Paulo. **Comentários ao Estatuto da Advocacia e da OAB**. 14. ed. São Paulo: SaraivaJur, 2022.

Proteção de Dados que se espalhem informações sobre clientes, ou sobre suas demandas, de forma pública.[148]

Com relação à Ordem dos Advogados do Brasil, com a promulgação da Lei Geral de Proteção de Dados, diversos conselhos seccionais criaram guias para auxiliar escritórios de advocacia a implementar a lei adequadamente. Não havendo legislação ou regulação específica para escritórios de advocacia, estes devem realizar adaptações para se conformar como qualquer outra organização, embora existam diversas situações específicas à atividade que merecem atenção especial.

Estes guias, logo, estabelecem orientações não-vinculantes, com o objetivo de educar e orientar escritórios de advocacia a respeito da proteção de dados, bem como conscientizar a comunidade de advogados com relação à importância do tópico. Os principais conselhos seccionais do Brasil, desta forma, criaram seus próprios guias de auxílio a escritórios de advocacia através de suas Comissões responsáveis pela proteção de dados.

A Ordem dos Advogados do Brasil é dividida em diferentes conselhos seccionais, e estes, divididos em subsecções, conforme artigo 44, parágrafo 2º, da Lei 8.906, o Estatuto da Advocacia[149]. Este estabelece que estes conselhos seccionais são dotados de personalidade jurídica própria, e possuem jurisdição sobre os respectivos territórios de seus Estados-Membros, bem como do Distrito Federal e eventuais territórios.

A Comissão de Privacidade e Proteção de Dados do Conselho Seccional da OAB de São Paulo, desta forma, lançou um Guia da Lei Geral de Proteção de Dados na advocacia[150], bem como uma cartilha de boas práticas de proteção de dados na advocacia[151]. Com relação a esta, foi baseada em materiais de organizações internacionais, e observando especialmente as práticas estabelecidas na própria LGPD, em seu capítulo VI, de segurança e boas-práticas. Desta forma, seu objetivo

---

[148] ORDEM DOS ADVOGADOS DO BRASIL. Conselho Federal. **Resolução n. 02/2015.** Disponível em: https://www.oab.org.br/arquivos/resolucao-n-022015-ced-2030601765.pdf. Acesso em: mar. 2023.

[149] BRASIL. **Lei n. 8.906, de 4 de julho de 1994.** Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8906.htm. Acesso em: jan. 2023.

[150] ORDEM DOS ADVOGADOS DO BRASIL, SP. **Guia da Lei Geral de Proteção de Dados na Advocacia**. 2020. Disponível em: https://www.conjur.com.br/dl/guia-lgpd-escritorios.pdf. Acesso em: jan. 2023.

[151] ORDEM DOS ADVOGADOS DO BRASIL, SP. **Boas práticas de proteção de dados na advocacia**. 2021. Disponível em: https://jornaldaadvocacia.oabsp.org.br/wp-content/uploads/2021/09/CPPD-OAB-SP-Coordenadoria-de-Educacao-Cartilha-de-Boas-Praticas-rev-2_compressed.pdf. Acesso em: jan. 2023.

é justamente o de estabelecer um protocolo de conduta que escritórios de advocacia possam seguir, para operações que envolvam o tratamento de dados pessoais ao longo de sua duração.

As principais etapas de implementação sugeridas pelo guia de boas-práticas [152] são: a criação de um comitê (ou nomeação de um colaborador) responsável pelo acompanhamento de todas as tarefas relacionadas a proteção de dados, como mapeamento de dados, classificação das informações tratadas e escolha de provedores; compartilhamento de responsabilidades entre todas as áreas envolvidas do escritório; avaliação da maturidade dos processos internos que já existam e lidem com tratamento de dados; a realização de treinamento com todos os colaboradores que exercem atividades de tratamento com dados; e, finalmente, a atualização das políticas de compliance já existentes.

Para isto, certas precauções devem ser tomadas, como registrar todas as operações de tratamento de dados, a seleção dos dados que serão armazenados de forma a eliminar os desnecessários, a criação de uma política de privacidade alinhada com os tratamentos realizados, e a adaptação das minutas contratuais, com o estabelecimento da responsabilidade dos agentes de tratamento, por exigência da própria LGPD.

Estabelece que o compartilhamento dos dados pessoais com tribunais e com correspondentes deve obedecer o artigo 7º, incisos II a X da LGPD, que trata do compartilhamento sem a necessidade de consentimento do titular. Lima[153], por sua vez, estabelece que devem ser avaliados para tal a necessidade dos dados para o efetivo exercício dos direitos pleiteados no processo, bem como que o titular dos dados será informado quando a hipótese do tratamento for aplicada, de forma a assegurar um adequado controle dos dados. Isto possibilitará responder aos titulares quando questionado com relação a seus dados.

Por fim, o guia de boas práticas traz importantes orientações com relação à gestão de dados armazenados em mídia física, pois estes também são protegidos

---

[152] ORDEM DOS ADVOGADOS DO BRASIL, SP. **Boas práticas de proteção de dados na advocacia**. 2021. Disponível em: https://jornaldaadvocacia.oabsp.org.br/wp-content/uploads/2021/09/CPPD-OAB-SP-Coordenadoria-de-Educacao-Cartilha-de-Boas-Praticas-rev-2_compressed.pdf. Acesso em: jan. 2023.

[153] LIMA, Vinícius Albuquerque**. A lei n° 13.709/18 (Lei Geral de Proteção aos Dados Pessoais – LGPD) e sua relação com a advocacia:** o advogado e seus deveres quanto ao tratamento dos dados pessoais. 2021. Disponível em: https://jus.com.br/artigos/94515/a-lei-n-13-709-18-lei-geral-de-protecao-aos-dados- pessoais-lgpd-e-sua-relacao-com-a-advocacia-o-advogado-e-seus-deveres-quanto- ao- tratamento-dos-dados-pessoais. Acesso em: dez. 2022.

pela Lei Geral de Proteção de Dados: mapear e estabelecer padrões de arquivamento dos dados; estabelecer uma política de uso e uma hierarquia de acesso ao local dos dados; garantir medidas de segurança ao local de acesso, como cadeados e trancas; eliminar os dados periodicamente, e de maneira segura e final; e revisar periodicamente a política de gestão destes documentos, sempre a atualizando quando necessário.

Com relação ao Guia da LGPD na Advocacia[154], traz seus aspectos gerais, fundamentos e princípios de forma generalizada, bem como diversas definições técnicas. Lista, ainda, os agentes de tratamento, as hipóteses de tratamento, e os direitos dos titulares. Por fim, em sua parte geral, o guia postula sobre as medidas de segurança elencadas na lei, e suas sanções administrativas.

Em sua parte específica, começa estabelecendo diversos cuidados que escritórios de advocacia devem ter em suas atividades do dia-a-dia, para melhor se adequar à nova legislação: adotar medidas de transparência na etapa de prospecção de clientes; criar um aviso interno de privacidade, bem como realizar treinamento de todos os colaboradores e advogados, por estes serem também titulares de dados; incluir cláusulas de proteção de dados e procedimentos para definir os diversos papéis dos agentes de tratamento, bem como redobrar a atenção dada aos contratos celebrados com clientes, sempre ressaltando a transparência com relação ao tratamento de dados; realizar o saneamento dos arquivos de maneira periódica, evitando acúmulo de dados desnecessários e ultrapassados; e, por último, observar o consentimento de terceiros ao estabelecer boletins e newsletters por e-mail, sempre estabelecendo mecanismos de *opt*-in ou *opt-out* adequados.

O guia cria, desta forma, nove etapas para um processo de adequação para a Lei Geral de Proteção de Dados em escritórios de advocacia, aqui parafraseados:[155]

1) Implementar uma estrutura de governança em privacidade e proteção de dados que atenda às necessidades do escritório, incluindo a criação de um comitê de privacidade em nome de um encarregado.

[154] ORDEM DOS ADVOGADOS DO BRASIL, SP. **Guia da Lei Geral de Proteção de Dados na Advocacia**. 2020. Disponível em: https://www.conjur.com.br/dl/guia-lgpd-escritorios.pdf. Acesso em: jan. 2023.

[155] ORDEM DOS ADVOGADOS DO BRASIL, SP. **Guia da Lei Geral de Proteção de Dados na Advocacia**. 2020. Disponível em: https://www.conjur.com.br/dl/guia-lgpd-escritorios.pdf. Acesso em: jan. 2023.

2) Mapear as atividades de tratamento de dados, identificando pontos de desconformidade com a legislação e atribuindo as bases legais que autorizam o tratamento dos dados para as atividades. Para tal, é necessário identificar as áreas internas do escritório que realizem o tratamento de dados pessoais, bem como as que possivelmente lidam ou possuem interesse em lidar com os mesmos.

3) Avaliar o nível de maturidade dos processos internos existentes em relação ao cumprimento da LGPD. Ao realizar a análise preliminar dos processos, se torna possível identificar o nível de adequação dos mesmos, e realizar esta avaliação.

4) Identificar os riscos apurados em todas as atividades de tratamento dos dados, bem como avaliar o nível de maturidade do programa de governança em privacidade estabelecido no escritório.

5) Criar/revisar as políticas e procedimentos para formalizar um programa de privacidade dos dados, sempre considerando as características do escritório e das atividades que necessitem dos mesmos. Para tal, se deve revisar também os contratos firmados com terceiros e clientes, e registrá-los em base de dados apropriada. Este programa de privacidade de dados deve conter normas gerais sobre proteção de dados, bem como um código de conduta para os colaboradores, uma política de retenção ou eliminação de dados, e uma política de resposta a incidentes.

6) Criar canais de comunicação para servir aos titulares dos dados, bem como a órgãos reguladores. Estes canais de comunicação devem ser específicos para tratar de questões referentes à proteção de dados e privacidade. Ainda, firmar termos de confidencialidade com os mesmos, de forma a garantir o sigilo em relação aos dados pessoais com os quais entrarão em contato.

7) Criar materiais orientativos e de conscientização para sócios, advogados e colaboradores.

8) Treinar e capacitar colaboradores que estejam incumbidos do tratmento de dados. As sessões de treinamento devem ser realizadas de forma periódica. Estas sessões devem ter como escopo, no curto prazo, orientar os colaboradores sobre seu papel ao longo do processo de adequação, e, a longo prazo, instruí-los a respeito das novas políticas que serão implementadas devido à LGPD.

9) Estabelecer um roteiro de monitoramento constante, de forma a atualizar o programa de governança e privacidade, sempre reavaliando o nível de maturidade do mesmo.

Ainda, em sua 3ª subsecção, localizada em Campinas, a OAB/SP lançou um segundo guia da Lei Geral de Proteção de Dados aplicada aos escritórios de advocacia[156]. Além de recapitular a legislação, também instrui escritórios a criar sua própria política de privacidade. Esta, colocam, é o documento que apresenta todas as regras aplicáveis para o tratamento de dados pessoais realizado pelo escritório, podendo este ser tanto de clientes, colaboradores ou terceiros.

Desta forma, o guia estabelece que esta política de privacidade demonstrará diversos aspectos do tratamento dos dados: quais dados serão coletados; como serão utilizados; por quanto tempo ficam retidos; quais as bases legais de sua utilização; qual a forma que os dados serão descartados após sua utilização; e quais os requisitos necessários para construir um programa de proteção de dados pessoais que esteja em conformidade com a legislação. Ainda, deve conter o compromisso do escritório com relação ao tratamento dos dados de todos os envolvidos.

Esta política de privacidade, desta forma, serviria para cobrir a exigência prevista no artigo 52, parágrafo 1º, inciso IX da Lei Geral de Proteção de Dados, que estabelece que a adoção de política de boas práticas e governança pelas organizações será utilizada como critério para julgar a gravidade de sanções administrativas impostas pela lei.

---

[156] ORDEM DOS ADVOGADOS DO BRASIL, SP. **Guia da LGPD aplicada aos escritórios de advocacia**. 2021. Dispponível em: https://oabcampinas.org.br/wp-content/uploads/2021/12/Guia-LGPD_Advocacia.pdf. Acesso em: jan. 2023.

As atividades desenvolvidas pelo escritório, logo, devem assegurar, através do desenvolvimento da política de privacidade, que conformam com suas obrigações legais em relação ao tratamento de dados trazido pela LGPD, dado que os escritórios de advocacia lidam com a manipulação de dados pessoais. Esta traz a dispensa de consentimento em duas hipóteses relevantes para o exercício da advocacia, em seu artigo 7º[157]:

> Artigo 7º:
> [...] 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).

Esta política de privacidade, desta forma, deve garantir que todos os envolvidos no escritório (advogados, sócios, colaboradores, etc.) estejam comprometidos integralmente com a proteção dos dados, sempre que o escritório atuar como controlador dos mesmos. Desta forma, se fortalece a transparência nas diversas relações do escritório, colocando em evidência a preocupação do escritório com a proteção dos dados.

O guia da subsecção de Campinas[158] ainda traz um manual de elaboração de uma política de incidentes para o escritório de advocacia, através do estabelecimento de respostas padronizadas a incidentes de segurança. Ainda que a LGPD não traga uma definição específica do que seria um incidente de segurança, a Autoridade Nacional de Proteção de Dados a complementou, definindo-o como um "evento adverso confirmado, relacionado à violação, na segurança de dados pessoais, tais como acessos não-autorizados, acidentais ou ilícitos, que resultem na destruição, perda, alteração, vazamento, ou, ainda, qualquer forma de tratamento de dados inadequado que possa ocasionar risco para os direitos e liberdades do titular dos dados pessoais".[159]

---

[157] BRASIL. **Lei n. 13.709 de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: jan. 2023.

[158] ORDEM DOS ADVOGADOS DO BRASIL, SP. **Guia da LGPD aplicada aos escritórios de advocacia**. 2021. Dispponível em: https://oabcampinas.org.br/wp-content/uploads/2021/12/Guia-LGPD_Advocacia.pdf. Acesso em: jan. 2023.

[159] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Comunicação de incidentes de segurança**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca. Acesso em: mar. 2023.

Desta forma, a resposta a estes incidentes de segurança é justamente a maneira como o escritório irá lidar com estas situações, e como agirá para mitigar os riscos decorrentes delas, devendo sempre ser formalizado através de um plano de ação. Ele orienta os envolvidos sobre como agir, reduzindo o tempo de ação e diminuindo os custos de recuperação. O guia elenca, assim, os elementos que devem ser contidos na política de incidentes de segurança, aqui parafraseados:

1) A definição de incidente de segurança.
2) A descrição dos procedimentos que serão executados, caso exista suspeita de um incidente de segurança, ou que este seja confirmado.
3) A indicação de pessoas que serão acionadas em caso de suspeita ou confirmação de um incidente de segurança, bem como as ações que devem ser tomadas.
4) Ferramentas e recursos tecnológicos que devem ser utilizados no caso de um incidente de segurança ser confirmado.
5) Qual tempo de resposta seria razoável para o incidente em questão.
6) Quais critérios de análise de criticidade do incidente, bem como os critérios para comunicação à Autoridade Nacional de Proteção de Dados e para titulares dos dados.
7) Procedimentos internos de registro e monitoramento de eventual incidente de segurança.
8) Como será realizado o gerenciamento de terceiros que possam fazer parte do incidente.

Ainda, o artigo 48 da Lei Geral de Proteção de Dados[160] determina que a comunicação à Autoridade Nacional e aos titulares apenas é necessária em caso onde exista risco ou dano relevante para os mesmos. Logo, os incidentes de segurança devem passar por uma análise no momento que ocorrerem, para averiguar a possibilidade de causar danos.

[160] BRASIL. **Lei n. 13.709 de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: jan. 2023.

Como sugestão, o guia[161] traz que incidentes de segurança de risco mediano são os que apresentam pelo menos uma das características a seguir, e alto caso possua duas ou mais: previsão de consequências de médio e longo prazo; envolvimento de dados sensíveis; envolvimento de categorias especiais de titulares, como crianças e adolescentes, idosos ou incapazes; capacidade de provocar riscos ou violação a direitos fundamentais dos titulares; e a capacidade de o incidente trazer riscos à segurança do titular ou exposição a fraudes.

Por fim, fornece sugestões de boas-práticas para escritórios de advocacia, no que tange à proteção de dados, aqui parafraseados:

- Usar uma conexão VPN (Virtual Private Network), que estabelece um túnel criptografado para seu tráfego de dados, bem como disfarça seu endereço de rede, criando um ambiente mais seguro para os dados.

- Criar *backups* de todos os dados armazenados, tanto fisicamente quando em nuvem, e ativar criptografia nos mesmos.

- Criar senhas fortes, contendo combinações diversas de caracteres, sempre evitando utilizar informações pessoais como senhas.

- Habilitar a verificação de senha em duas etapas em todos os sistemas de armazenamento e aplicativos de mensagens.

- Sempre apagar os dados armazenados em todas as mídias que forem descartadas.

- Contratar um serviço de certificação digital, que funciona como uma identidade eletrônica para o escritório. Desta forma, se fortalece a segurança ao lidar com documentos digitais, e acessos a portais governamentais.

- Tomar precauções ao digitalizar processos e documentos, sempre priorizando a segurança dos dados encontrados nestes, escolhendo opções seguras de armazenamento digital.

- Garantir que advogados correspondentes tomem os mesmos cuidados que qualquer colaborador do escritório, adotando as medidas de segurança e sigilo, podendo este ser responsabilizado caso ocorra um incidente de segurança.

- Evitar utilizar aplicativos de mensagens instantâneas para enviar documentos que contenham dados pessoais sensíveis, pois é comum ocorrerem

[161] BRASIL. **Lei n. 13.709 de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: jan. 2023.

falhas de segurança nestes, ou até mesmo erro humano, ao enviar para pessoa terceira não envolvida.

- Por fim, evitar o uso de redes sociais para compartilhamento de dados, ainda que os ditos dados sejam públicos.

Percebe-se, logo, a importância de implementar o compliance digital dentro dos escritórios de advocacia, atuando em conformidade com as leis e normas que lidam com a proteção de dados digitais. Esta, ainda, deve ser planejada de acordo com as necessidades de cada escritório, sendo estas definidas durante o mapeamento inicial dos processos internos e estrutura do mesmo.

Ainda, com relação aos dados de seus colaboradores, os escritórios de advocacia devem seguir orientações gerais a respeito da Lei Geral de Proteção de Dados aplicadas às relações trabalhistas, pois possuem a mesma relação com os mesmos que qualquer tipo de sociedade empresarial, como coloca Kirschner[162]. A comissão de privacidade e proteção de dados pessoais do conselho seccional do Distrito Federal, desta forma, criou um guia da LGPD nas relações de trabalho[163].

Trazem que o tratamento de dados pessoais está presente durante toda a execução do contrato trabalhista, começando em sua fase pré-contratual, e se estendendo até mesmo após o término do contrato de trabalho, na forma de armazenamento das informações dos trabalhadores para fins de legislação trabalhista e previdenciária. Desta forma, é importante que o escritório, toda vez que fizer a coleta de qualquer dado, estabelecer a base legal correspondente, e sempre descarte de maneira adequada os dados que não forem mais relevantes.

Importante relevar que isto sempre deve ser feito através da coleta do consentimento expresso do trabalhador, sempre informando de forma clara e transparente a finalidade dos dados. Ainda, se devem criar cláusulas específicas nos contratos de trabalho que lidem com a matéria do tratamento e armazenamento dos dados, e termos de confidencialidade e sigilo entre o empregador e o empregado. Este documento garante que informações estratégicas e confidenciais não sejam repassados a terceiros, ou utilizadas para fins alheios aos originais.

---

[162] KIRSCHNER, Ana. Responsabilidade social corporativa em escritórios de advocacia. **Revista Processus de Estudos de Gestão, Jurídicos e Financeiros**, v. 4, n. 9, 2013.

[163] ORDEM DOS ADVOGADOS DO BRASIL. **LGPD nas relações de trabalho**. 2021. Disponível em: https://oabdf.org.br/wp-content/uploads/2021/08/eBook_LGPD-nas-Relacoes-de-Trabalho-1-1.pdf. Acesso em: mar. 2023.

Ainda, a cultura de proteção de dados deve vir da gestão do escritório, e ser repassada a todos os colaboradores, fortalecendo a cultura da organização e provocando a equipe a refletir sobre o tema e incorporar atitudes em suas tarefas rotineiras voltadas para a proteção dos dados, como coloca Veiga[164]. Devem, também, receber treinamento adequado em boas-práticas no tema, de forma que se habituem com as novas normas, e sejam capazes de implementar boas-práticas.

Deve-se, também, realizar investimentos em segurança digital para a prática do trabalho remoto, pois as redes domésticas dos trabalhadores podem apresentar maior potencial de invasões e riscos em geral, de acordo com o próprio Comitê Central de Governança de Dados do Brasil.[165] Por último, é importante abrir um canal de comunicação para que colaboradores se sintam confortáveis para exercer seus direitos como titulares dos dados coletados pelo escritório.

Desta forma, a partir desta análise da legislação de proteção de dados, da regulação da profissão da advocacia, e destas guias e cartilhas emitidas pela Ordem dos Advogados do Brasil, logo, é possível planejar e implementar medidas de adequação para a Lei Geral de Proteção de Dados dentro de escritórios de advocacia, sempre mantendo as medidas atualizadas e com o melhor interesse dos titulares dos dados como prioridade.

[164] VEIGA, T. M. A LGPD nos escritórios de advocacia previdenciária: o registo das operações de tratamento de dados e o conceito de escritório digital como medidas de base para a conformidade. **Revista Jurídica da Escola Superior de Advocacia OAB de Santa Catarina,** v. 1, n. 1, 2021.

[165] BRASIL. Ministério da Gestão e da Inovaçãoem Serviços Públicos. **Guia de boas práticas:** Lei Geral de Proteção de Dados (LGPD). 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas-praticaslei-geral-de-protecao-de-dados-lgpd. Acesso em: maio 2023.

5 PROPOSTA DE TERMO DE CONSENTIMENTO DE USO DE DADOS

Inicialmente, se trará um modelo de termo de consentimento de uso de dados pessoais, com foco em escritórios de advocacia. Este modelo busca englobar as diversas modalidades de dados pessoais que possam ser utilizados na profissão, sempre visando o melhor interesse do cliente com relação à finalidade do tratamento dos dados.

Após a criação do modelo, se passará a uma exposição de motivos acerca das cláusulas elencadas, de acordo com as diversas áreas de atuação profissionais dentro do campo da advocacia, bem como uma visão geral sobre o termo de consentimento em si.

5.1 MODELO DE TERMO DE CONSENTIMENTO DE USO DE DADOS

TERMO DE CONSENTIMENTO PARA USO DE DADOS PESSOAIS

O presente documento objetiva registrar a livre e inequívoca manifestação por parte do titular dos dados pessoais, pela concordância com o tratamento dos mesmos para a finalidade especificada neste documento, se pautando a partir da Lei Geral de Proteção de Dados, Lei 13.709, e com fundamentação jurídica em seu artigo 5º, inciso XII.

Ao assinar o presente termo, o titular de nome, nacionalidade, estado civil, profissão, portador da cédula de identidade, inscrito no Cadastro de Pessoa Física, residente e domiciliado, aqui denominado “**Titular**”, consente que o Escritório de Advocacia, com o Cadastro Nacional de Pessoa Jurídica, registro na Ordem dos Advogados do Brasil, com endereço comercial, telefone, aqui denominado “**Controlador**”, utilize seus dados pessoas para tratamento, sempre dentro da finalidade e dos termos estabelecidos neste documento, e em conformidade com a Lei Geral de Proteção de Dados.

Por tratamento, se entende as seguintes ações, conforme artigo 5º, inciso X da Lei Geral de Proteção de Dados: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

CLÁUSULA PRIMEIRA: DADOS PESSOAIS

O controlador fica, desta forma, autorizado a tomar decisões e realizar as ações previamente estabelecidas com relação ao tratamento dos dados pessoas aqui elencados, quando aplicáveis para as finalidades previstas neste termo:

- Nome completo, estado civil, nível de Instrução ou escolaridade, profissão, endereço completo, número de telefone, endereço de e-mail;

- Número da carteira de identidade (RG), número da Carteira Nacional de Habilitação (CNH), número do Cadastro de Pessoas Físicas (CPF) ou número do Cadastro Nacional de Pessoas Jurídicas (CNPJ), número do PIS, número do Passaporte, número da Carteira de Trabalho e Previdência Social (CTPS);

- Nome fantasia, razão social, inscrição municipal e estadual, Classificação Nacional de Atividade Econômica (CNAE), registros no Instituto Nacional da Propriedade Intelectual (INPI);

- Endereço de IP (Internet Protocol), localização geográfica genérica, horário de acesso, fonte de referência, tipo de navegador, duração da visita, páginas visitadas, bem como qualquer comunicação mantida entre titular e controlador em seu website;

Estes dados terão seu tratamento sempre pautado pela legislação de proteção de dados.

CLÁUSULA SEGUNDA: DADOS SENSÍVEIS

Para atingir as finalidades elencadas, é possível que seja necessária a coleta de dados sensíveis, nos termos do artigo 5º da Lei Geral de Proteção de Dados. Entre eles, se elencam os seguintes, entre outros: etnia, cor, religião, opção sexual. Desta forma, o titular consente na utilização destes dados sensíveis para atingir as finalidades presentes neste termo de consentimento, conforme artigo 11, inciso I, da mesma.

CLÁUSULA TERCEIRA: DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES

O titular confirma que é o responsável legal legítimo de qualquer menor de idade cujos dados forneça, e consente expressamente com o tratamento de seus dados pessoais para atingir as finalidades descritas neste termo de consentimento, nos termos do artigo 14 da Lei Geral de Proteção de Dados, em seu parágrafo 1º.

Ainda, o controlador irá manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício de seus direitos, conforme parágrafo 2º do mesmo artigo. O tratamento dos dados do menor de idade, desta forma, seguirá os parâmetros gerais estabelecidos no Estatuto da Criança e do Adolescente com relação à proteção aos mesmos.

CLÁUSULA QUARTA: DADOS DE IDOSOS

O titular consente com relação ao tratamento de dados pessoais de idosos, nos termos da legislação de proteção de dados. Ainda, o controlador garante que o tratamento de dados de idosos será efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, conforme artigo 55-J da Lei Geral de Proteção de Dados, e seguindo as diretrizes gerais da Lei 10.741, o Estatuto do Idoso.

CLÁUSULA QUINTA: DADOS DE TERCEIROS

O titular concorda em compartilhar apenas os dados de terceiros que sejam necessários para o cumprimento de suas obrigações legais, como para atuação em processos judiciais ou administrativos, e para o cumprimento de obrigações legais ou regulatórias. Ainda, consente que irá apenas compartilhar dados pessoais de terceiros que não se encaixam nestas categorias quando tiverem o consentimento expresso dos mesmos para tal.

Ainda, dados pessoais de colaboradores se enquadram nesta categoria, logo, deve se obter o consentimento dos mesmos para casos onde não seja permitida a dispensa de consentimento para o tratamento dos dados.

CLÁUSULA SEXTA: FINALIDADE DO TRATAMENTO DOS DADOS

Os dados pessoais elencados neste termo de consentimento apenas poderão passar por tratamento para atingir as seguintes finalidades, sempre respeitando os limites da legislação de proteção de dados:

- Para representar em Juízo o titular, bem como para praticar todos os atos necessários para tal, patrocinando a defesa de seus direitos e interesses, seja como Autor, Réu, Assistente, Requerente ou por qualquer outra, sendo esta postulação em qualquer órgão do Poder Judiciário, juizados especiais ou em matéria administrativa, sempre visando o melhor interesse do mesmo;

- Para representar os interesses em geral do titular em matéria de advocacia extrajudicial, englobando as atividades de consultoria, assessoria e direção jurídicas, estabelecidas como atividades privativas da advocacia no artigo 1º, inciso II do Estatuto da Advocacia, Lei 8.906/94;

- Para cumprimento pelo controlador de obrigações impostas por órgãos de fiscalização;

- Quando for necessário para adequadamente atender aos interesses legítimos do controlador ou mesmo de terceiros, exceto em casos onde prevaleçam direitos do titular que exijam a proteção de seus dados pessoais;

- Quando necessário para a execução de contrato no qual o titular seja parte, e o controlador seu mandatário;

- Por ordem do titular dos dados;

- Para a proteção da vida e da incolumidade física do titular ou de terceiros.

CLÁUSULA SÉTIMA: COMPARTILHAMENTO DOS DADOS

O controlador fica, desta forma, autorizado para compartilhar os dados pessoais do titular com outros agentes de tratamento de dados, no de caso este compartilhamento for necessário para atingir as finalidades listadas neste documento, sempre com a observância da legislação de proteção de dados pessoais.

Em caso do compartilhamento de dados com terceiro que esteja em desacordo com as finalidades listadas neste termo de consentimento, o controlador

deve comunicar o titular, que poderá revogar o consentimento, bem como ajustar novo termo de consentimento para este compartilhamento.

CLÁUSULA OITAVA: SEGURANÇA DOS DADOS

O controlador fica responsável por manter medidas de segurança, tanto técnicas quanto administrativas, de maneira a garantir a proteção dos dados pessoais de qualquer risco, como acessos não-autorizados e situações acidentais ou ilícitas, como destruição, perda, alteração, comunicação ou qualquer tipo de ação inadequada.

O controlador, desta forma, confirma que adota medidas de prevenção contra riscos, bem como orienta os que atuam em seu nome com relação à melhores práticas de proteção de dados, bem como que seus colaboradores, sócios e associados conhecem e cumprem integralmente o disposto na legislação de proteção de dados, e utiliza programas de proteção e segurança de informações que busquem evitar qualquer tipo de acesso não-autorizado.

Ainda, o controlador notificará o titular, seu responsável legal, e a Autoridade Nacional de Proteção de Dados, ou ANPD, caso ocorra incidente de segurança que venha a acarretar risco ou dano relevante para o mesmo, conforme artigo 48 da Lei Geral de Proteção de Dados.

CLÁUSULA NONA: TÉRMINO DO TRATAMENTO DOS DADOS

Ao controlador é permitido manter e utilizar os dados pessoais fornecidos pelo titular durante o período de cumprimento das finalidades elencadas neste termo de consentimento, enquanto os dados forem pertinentes para alcançar as mesmas. Ainda, o controlador poderá permanecer com seus dados mesmo após o encerramento das mesmas, restringindo seu uso posterior ao cumprimento de seus próprios objetivos legais.

Caso os dados passem por um processo de anonimização, onde cesse a possibilidade de serem associados ao titular, poderão ser mantidos por tempo indeterminado, cessando, desta forma, o vínculo entre as partes presentes neste termo de consentimento.

Ainda, é permitido ao titular solicitar ao controlador, a qualquer momento, a eliminação de seus dados pessoais que não tenham sido anonimizados, através de e-mail ou correspondência. O titular, no entanto, fica ciente de que, caso ocorra a eliminação de seus dados, os serviços oferecidos pelo controlador podem ser inviabilizados.

CLÁUSULA DÉCIMA: DIREITOS DO TITULAR

Com relação ao titular, este possui direito a obter, do controlador, amparado pelo artigo 18 da Lei Geral de Proteção de Dados, mediante requisição e a qualquer momento:

- Confirmação da existência do tratamento;
- Acesso aos dados;
- Correção de dados incompletos,
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei 13.709;
- Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa;
- Eliminação dos dados pessoais tratados com o consentimento do titular;
- Informação das entidades, públicas ou privadas, com a qual o controlador realizou uso compartilhado dos dados.
- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- Revogação de seu consentimento, a qualquer momento, mediante solicitação via e-mail ou correspondência ao controlador; salvo em hipóteses de obrigatoriedade do tratamento de dados para cumprimento de obrigação legal ou regulatória pelo mesmo.

5.2 EXPOSIÇÃO DE MOTIVOS

Escritórios de advocacia lidam com diversas demandas de natureza multidisciplinar. Seus clientes são titulares deste direito fundamental à proteção de dados, logo, o advogado deve pautar pela proteção destes, sempre se utilizando apenas de dados que sejam estritamente necessários para suas demandas, e garantindo a segurança e proteção dos mesmos, conforme o próprio Guia da LGPD na Advocacia[166]. Assim, é importante relevar a necessidade de o termo de consentimento de uso de dados utilizado pelo escritório englobar as hipóteses de consentimento que o escritório irá requerer para uma prestação de serviços adequada.

A cláusula primeira estabelece quais seriam os dados pessoais necessários para se atingir as finalidades elencadas na cláusula sexta. Esta cláusula deve listar a maior quantidade de dados possíveis, sempre dentro do escopo das finalidades pretendidas com o tratamento. Escritórios de advocacia necessitam, por vezes, não apenas de informações pessoais dos clientes, mas também de dados relativos ao caso concreto sendo tratado.[167] Desta forma, não há como prever com exatidão a totalidade dos dados que seriam necessários. Logo, listam-se dados gerais, e se estabelece que o tratamento será feito em todos os dados que forem cedidos para alcançar a finalidade pretendida.

Já na cláusula segunda, se tem o consentimento para os dados sensíveis, que necessitam de consentimento especial, conforme artigo 11 da Lei Geral de Proteção de Dados. Estes dados, como traz Patrícia Pinheiro[168], possuem risco considerável para o titular em casos de vazamentos, por darem margem a discriminação. Ainda, a atividade advocatícia lida de maneira constante com dados considerados sensíveis, como religião, etnia, ou opção sexual, em especial com relação à atuação em matérias de direito civil. Desta forma, obter consentimento expresso para o tratamento de dados sensíveis é essencial.

Com relação aos dados pessoais de idosos, bem como os dados pessoais de crianças e adolescentes, que se encontram nas cláusulas terceira e quarta do termo de consentimento, estes possuem amparo em seus estatutos. Embora estes não

---

[166] ORDEM DOS ADVOGADOS DO BRASIL, SP. **Guia da Lei Geral de Proteção de Dados na Advocacia**. 2019. Disponível em: https://www.conjur.com.br/dl/guia-lgpd-escritorios.pdf. Acesso em: jan. 2023.

[167] ORDEM DOS ADVOGADOS DO BRASIL, SP. **Guia da Lei Geral de Proteção de Dados na Advocacia**. 2019. Disponível em: https://www.conjur.com.br/dl/guia-lgpd-escritorios.pdf. Acesso em: jan. 2023.

[168] PINHEIRO, Patricia Peck**. Proteção de dados pessoais comentários à Lei n. 13.709/2018:** (LGPD). 3. ed.São Paulo: Saraiva Jur, 2021.

trabalhem diretamente com a proteção de dados, estabelecem diretrizes gerais que devem ser seguidas ao lidar com os mesmos, que devem ser obedecidas também em termos da mesma, como coloca Veiga.[169]

Ainda, a própria Lei Geral de Proteção de Dados estabelece maior proteção aos dados destes, em seu artigo 14, limitando as finalidades possíveis para tratamento dos mesmos, e aumentando o nível de consentimento requerido para tal. Desta forma, é essencial possuir cláusula específica no termo de consentimento de tratamento de dados que lide com os dados de ambos, como exposto nas cláusulas terceira e quarta do termo de consentimento.

Com relação à cláusula quinta, que trata de direitos de terceiros, esta é particularmente relevante para escritórios que lidam com clientes empresariais. Dentro da área de direito empresarial e trabalhista patronal, é importante ressaltar que as preocupações tomam outra figura, com relação a seus dados corporativos. Em especial, ainda, suas bases de dados que contém informações de terceiros, como de seus colaboradores e consumidores, dados estes por vezes sensíveis.

Desta forma, as empresas necessitam observar se possuem o consentimento destes titulares para compartilhar seus dados, como pode ser observado na cláusula quinta do termo de consentimento. Caso não possuam o consentimento, como qualquer organização, coloca Lóssio [170], estes dados devem apenas ser compartilhados com o escritório de advocacia em casos onde haja a necessidade da utilização dos mesmos para cumprimento de dever legal, ou exercício regular de seus direitos, conforme artigo 8, incisos III e IV da Lei Geral de Proteção de Dados.

O próprio direito do trabalho, ainda, estabelece diversas considerações com relação à proteção dos trabalhadores, em razão de sua hipossuficiência na relação, que perdura até mesmo nas fases pré e pós-contratual, de acordo com Perregril. [171] Desta forma, incluir nesta cláusula a responsabilidade do cliente de apenas compartilhar os dados de colaboradores caso possua seu consentimento previne situações indesejadas de terceiros interferindo na relação advogado-cliente.

---

[169] VEIGA, T. M. A LGPD nos escritórios de advocacia previdenciária: o registo das operações de tratamento de dados e o conceito de escritório digital como medidas de base para a conformidade. **Revista Jurídica da Escola Superior de Advocacia OAB de Santa Catarina,** v. 1, n. 1, 2021.

[170] LÓSSIO, Claudio Joel Brito. **Proteção de dados e compliance digital.** São Paulo, Almedina, 2021.

[171] PERREGRIL, Fernanda; CALCINI, Ricardo (Org.). **LGPD e compliance trabalhista:** os desafios atuais do direito do trabalho empresarial. São Paulo: Mizuno, 2021.

A cláusula sexta estabelece quais seriam as finalidades do tratamento dos dados por parte do escritório. Desta forma, é necessário listar quais seriam as atividades típicas de um escritório de advocacia, estabelecidos pelo próprio Estatuto da Ordem dos Advogados do Brasil[172], além das finalidades estabelecidas na própria Lei Geral de Proteção de Dados, em seu artigo 7º, que estabelece hipóteses lícitas para o tratamento de dados.

Com relação ao compartilhamento de dados, presente na cláusula sétiima, esta estabelece que este compartilhamento, caso seja necessário para atingir as finalidades elencadas, deve ser consentido pelo titular dos dados. Esta previsão é elencada no artigo 7º, parágrafo 5º da Lei Geral de Proteção de Dados, que requer consentimento específico para tal, necessitando de uma cláusula própria para destaque.

A cláusula oitava estabelece a responsabilidade do controlador com relação aos dados e sua segurança. Isto inclui medidas técnico-administrativas que visem a garantir a proteção dos dados, bem como o manejo de processos internos de forma a reduzir potenciais riscos, essencial para o compliance interna de qualquer organização, como coloca Cavalari[173]. Esta cláusula se encontra pautada pelo artigo 6º da LGPD, inciso X, que estabelece o princípio da responsabilização e prestação de contas, que é justamente a demonstração pelo agente de adoção de medidas eficazes para a proteção dos dados. Desta forma, é do melhor interesse do escritório de colocar esta cláausula como medida de transparência no termo de consentimento.

O término do tratamento dos dados é trazido na cláusula nona, que estabelece que os dados podem ser guardados pelo controlador durante todo o período necessário para o cumprimento das finalidades elencadas no termo, mas também garante o direito do controlador permanecer com os dados mesmo após o encerramento destas caso para quando houver necessidade de cumprir seus próprios objetivos legais, como estabelece o artigo 15 da LGPD. Ainda, abre a possibilidade de os dados passarem por um processo de anonimização, onde possam ser mantidos por tempo indeterminado.

---

[172] BRASIL. **Lei n. 8.906, de 4 de julho de 1994.** Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8906.htm. Acesso em: jan. 2023.

[173] CAVALARI, Ana Paula França. **O compliance digital como ferramenta de gestão**. Porto Alegre: OAB/RS, 2020.

Por fim, a cláusula décima elenca os direitos que o titular possui ao consentir com o tratamento de seus dados pelo escritório. Os dados presentes na cláusula são os elencados no Capítulo III da Lei Geral de Proteção de Dados, e são reforçados no termo de consentimento para garantir um melhor entendimento por parte do titular para sua própria proteção, buscando a transparência na relação, princípio norteador da LGPD.

6 CONCLUSÃO

Tendo abordado a Lei Geral de Proteção de Dados, exposto seu contexto histórico, tanto nacional quanto internacional, sua estrutura, seus princípios norteadores e seus principais aspectos no que tange à profissão da advocacia, ficou demonstrado sua importância para o cenário digital, que se encontra em constante evolução. A promulgação do Regulamento Geral sobre Proteção de Dados da União Européia providenciou uma importante iniciativa internacional sobre o importante tema e assim abrindo as portas para que a LGPD viesse a ser criada, justamente pela necessidade de o direito acompanhar a evolução tecnológica considerável que vem acontecendo.

Foram listadas, desta forma, diversas medidas possíveis para escritórios de advocacia adequarem seus processos internos às normas estabelecidas pela Lei Geral de Proteção de Dados. A Ordem dos Advogados do Brasil, ainda, com a edição de diversos materiais propícios para a implementação de governança em termos de proteção de dados em escritórios de advocacia, criou um ambiente propício para orientação e auxílio da categoria com relação à matéria.

A importância da proteção de dados para o exercício da advocacia precede a Lei Geral de Proteção de Dados, dando especial atenção à segurança das informações de clientes na forma do sigilo profissional estabelecido no Estatuto da Ordem dos Advogados do Brasil, Lei 8.906, bem como na própria relação entre advogado e cliente, que deve ser pautada pela confiança e integridade entre as partes, dentro disto incluso, logo, a proteção de suas informações.

Ainda, com relação ao tratamento de dados por escritórios de advocacia, estes necessitam de um adequado termo de consentimento para o tratamento dos mesmos, que englobe não apenas a atividade advocatícia como um todo, mas também as especificidades dentro de cada área de atuação possível da profissão, como em atuação em direito empresarial, trabalhista, previdenciário, entre outros, bem como cláusulas gerais que englobem a possibilidade de tratamento de dados de diversos clientes que possuam necessidades especiais com relação aos dados, como de crianças e adolescentes, e de clientes idosos, onde o Estatuto da Criança e do Adolescente e o Estatuto do Idoso oferecem proteção adicional, conjugada com a própria Lei Geral de Proteção de Dados.

O termo de consentimento elencou diversos dados pessoais que possam vir a ser compartilhados pelo titular em sua cláusula primeira, bem como garantiu seu consentimento em dados diversos que possam servir para suas finalidades, sempre visando garantir a transparência para o titular, e obter seu consentimento de maneira detalhada a diversas etapas do tratamento dos dados, para não ser necessário obter consentimento de cada dado individualmente ao longo do tratamento.

Estabeleceu também as finalidades possíveis dos dados para escritórios de advocacia em seu capítulo sexto, elencando as hipóteses de tratamento de acordo com as atividades listadas nom Estatuto da Ordem dos Advogados do Brasil, bem como as hipóteses elencadas na própria Lei Geral de Proteção de Dados, e estabeleceu a responsabilização pela segurança dos dados como medida protetiva para o titular, com o fim de aumentar a transparência na relação, bem como listou seus direitos de acordo com o capítulo III da mesma.

Retoma-se, aqui, o problema de pesquisa, elaborado com a seguinte questão: Que providências, então, devem ser tomadas por escritórios para realizar a adequação de seus processos internos à Lei Geral de Proteção de Dados, observando as diversas áreas de atuação profissional dentro do campo da advocacia?

A hipótese de trabalho formulada para tal problema, desta forma, foi a de que a LGPD traz uma série de regulamentos e requisitos que demandam a atenção dos escritórios, sendo necessário reconhecer as peculiaridades de cada área de atuação da advocacia. Devem, então, fazer uma readequação em seus processos internos para conciliá-los com as novas demandas regulatórias, através das práticas de compliance jurídica, e estabelecer termos de consentimento de uso de dados para suas áreas específicas de atuação dentro da advocacia.

Possível, desta forma, realizar que a hipótese de trabalho veio a se confirmar. A Lei Geral de Proteção de Dados de fato elencou diversos requisitos legais que escritórios de advocacia devem observar, estando estes sob o leque de proteção da mesma. Uma readequação de seus processos internos se demonstrou crítico para tal, se utilizando das diversas ferramentas trazidas pelo compliance digital. A análise dos diversos materiais produzidos pela Ordem dos Advogados do Brasil sobre tal tópico fortalece a necessidade de adequação dos mesmos, e oferece uma importante divertida para a profissão.

Ainda, o termo criado atende a estas especificidades da profissão de advocacia, e fornece um panorama geral das atividades realizadas por escritórios, bem como engloba as diversas possibilidades específicas de diferentes áreas de atuação, trabalhando com suas necessidades e possibilitando um tratamento adequado dos dados com o adequado consentimento do cliente. A complementação deste, logo, traz transparência para a relação entre advogado e cliente, fortalecendo sua relação.

REFERÊNCIAS

ADACHI, Tomi. **Comitê gestor da internet no Brasil (CGI.br):** uma evolução do sistema de informação nacional moldada socialmente. Tese (Doutorado) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2011. Disponível em: https://www.teses.usp.br/teses/disponiveis/12/12139/tde-10102011-165732/pt-br.php. Acesso em: mar. 2023.

AGENCIA BRASIL. **Brasil tem 24,3 milhões de crianças e adolescentes que usam internet.** 2019. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2019-09/brasil-tem-243-milhoes-de-criancas-e-adolescentes-utilizando-internet. Acesso em Janeiro de 2023.

ALVES, Lucélia de Sena. Advocacia na quarta revolução industrial e a necessidade da presença digital. **Revista Direito, Tecnologia e Saúde,** v. 9, 2018.

ARAÚJO, Jeferson. **A História Brasileira de Proteção aos Dados: O Advento da LGPD e a sua Influência No Acesso aos Dados Médicos no Brasil**. Disponível em: https://www.nucleodoconhecimento.com.br/lei/advento-da-lei Acesso em Junho de 2023.

ASSI, Marco. **Compliance:** como implementar. São Paulo: Trevisan, 2018.

ATTARD, Judie *et al*. A systematic review of open government data initiatives. **Science Direct,** v. 32, n. 4, p. 399-418, oct. 2015. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0740624X1500091X. Acesso em: mar. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Comunicação de incidentes de segurança**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca. Acesso em: mar. 2023.

BIELA JÚNIOR. **Curso de ética profissional para advogados:** de acordo com o novo código de ética, com o Novo CPC e com as súmulas do Conselho Federal da OAB. São Paulo: LTR, 2018.

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

BITTAR, Carlos Alberto. **Os contratos de adesão e o controle de cláusulas abusivas**. São Paulo: SaraivaJur, 1991.

BLOCK, Marcella. **Compliance e governança corporativa**. São Paulo: Freitas de Bastos, 2020.

BRAGANÇA, Fernanda; BRAGANÇA, Laurinda Fátima. Revolução 4.0 no poder judiciário: levantamento do uso de inteligência artificial nos tribunais brasileiros. **Revista da Seção Judiciária do Rio de Janeiro**, v. 23, n. 46, 2019.

BRASIL. **Blog do marco civil da internet**. 2012. Disponível em: <http://arquivo.edemocracia.camara.leg.br/web/marco-civil-da-internet/inicio#.YJybE6Fv-Uk>. Acesso em: jan. 2023.

BRASIL. **Constituição da República Federativa do Brasil**. 1988. Disponível em: em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: jan. 2023.

BRASIL. **Decreto-lei 5.452, de 1º de maio de 1943**. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm. Acesso em: fev. 2023.

BRASIL. **Lei n. 8.906, de 4 de julho de 1994.** Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8906.htm. Acesso em: jan. 2023.

BRASIL. **Lei n. 10.406, de 10 de janeiro de 2002**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: mar. 2023.

BRASIL. **Lei n. 11.111, de 5 de maio de 2005.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/lei/l11111.htm. Acesso em: mar. 2023.

BRASIL. **Lei 12.527, de 18 de novembro de 2011.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: jan. 2023.

BRASIL. **Lei n. 12.965, de 23 de abril de 2014.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: dez. 2022.

BRASIL. **Lei n. 13.709 de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: jan. 2023.

BRASIL. **Lei n. 13.853, de 8 de julho de 2019**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: jan. 2023.

BRASIL. **Medida Provisória no 869, de 27 de dezembro de 2018**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm. Acesso em: jan. 2023.

BRASIL. **Projeto de Lei 4060/2012**. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=54806. Acesso em: jan. 2023.

BRASIL. **Projeto de Lei 6291/2016**. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2113796. Acesso em jan. 2023.

BRASIL. **Proposta de Emenda à Constituição - PEC 17/2019.** Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757. Acesso em: jan. 2023.

BRASIL. Câmara dos Deputados. Sancionada, com nove vetos, lei que cria Autoridade Nacional de Proteção de Dados **Agência Câmara de Notícias**, 2019. Disponível em: https://www.camara.leg.br/noticias/561908-SANCIONADA,-COM-NOVE-VETOS,-LEI-QUE-CRIA-AUTORIDADE-NACIONAL-DE-PROTECAO-DE-DADOS. Acesso em: jan. 2023.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Guia de boas práticas:** Lei Geral de Proteção de Dados (LGPD). 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas-praticaslei-geral-de-protecao-de-dados-lgpd. Acesso em: maio 2023.

BRASIL. Superior Tribunal de Justiça. REsp 1.228.104/PR. Terceira Turma. Relator: Ministro Sidnei Beneti. Julgado em: 15 mar. 2012. **DJe** 10 abr. 2012.

CALIFORNIA. **California consumer privacy act**. 2018. Disponível em: https://oag.ca.gov/-privacy/ccpa. Acesso em: jan. 2023.

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. **Cadernos Jurídicos,** São Paulo, 2021.

CAVALARI, Ana Paula França. **O compliance digital como ferramenta de gestão**. Porto Alegre: OAB/RS, 2020.

COLOMBO, Cristiano. Do sigilo profissional da advocacia à proteção de dados pessoais: princípios da lgpd e medidas concretas. *In:*I CONGRESSO INTERNACIONAL DA ADVOCACIA EXTRAJUDICIAL E DIGITAL, 1, 2021, São Paulo. VECCHIO, Fabrizio Bon; XIMENES, Raquel Letícia Cúrcio (Org.). **Caderno de resumos exandidos.** Porto Alegre: Instituto Ibero-americano de Compliance, 2021.

COLOMBO, Cristiano; BOCHI, Igor; BRONFMANN, José Leopoldo. Lei Geral de Proteção de Dados aplicada às relações de trabalho: ponderações quanto ao direito do esquecimento e o direito à informação. *In:* CONGRESSO ÍBERO-AMERICANO DE DOCENTES E INVESTIGADORES EM DERECHO E INFORMATICA, 22, 2022, Salta. Disponível em: https://drive.google.com/file/d/1lA2xawnGSwBM-cc-heRve4fjWBGAwiH4/view. Acesso em 2023.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei geral de proteção de dados pessoais comentada**. São Paulo: Thomson Reuters, 2019.

CRIADOR da Web divulga apoio ao marco civil da internet no Brasil. **G1 Globo**. 24 mar. 2014. Disponível em: http://g1.globo.com/tecnologia/noticia/2014/03/criador-da-web-divulga-apoio-ao-marco-civil-da-internet-no-brasil.html. Acesso em: mar. 2023.

DE LA TORRE, Lydia. **A guide to the California consumer privacy act of 2018**. Santa Clara: Santa Clara University, 2018. Disponível em:

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3275571. Acesso em: abr. 2023.
DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord**.). Direito e internet**. São Paulo: Quartier Latin, 2015. T. 1: Marco civil da Internet (Lei n. 12.965/2014).

DONDA, Daniel. **Guia prático de implementação da LGPD:** tudo que sua empresa precisa saber para estar em conformidade. São Paulo: Labrador, 2020.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 3. ed. São Paulo: Thomson Reuters, 2021.

DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. **Revista dos Tribunais**, São Paulo, v. 998, 2018.

ESTADOS UNIDOS DA AMÉRICA. **Foreign corrupt practices act**. 1977. Disponível em https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act. Acesso em: jan. 2023.

FIORILLO, Celso Antonio Pacheco. **O marco civil da internet e o meio ambiente digital na sociedade da informação:** comentários à Lei 12.965/2014. São Paulo: SaraivaJur, 2015.

FRAZÃO, Ana *et al.* **A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters, 2019.

GALINDO, Hercília. A “constituição da internet” brasileira requer atenção. **Folha de Pernambuco**, 26 jun. 2017. Disponível em: https://www.folhape.com.br/noticias/a-constituicao-da-internet-brasileira-requer-atencao/25427/. Acesso em: mar. 2023.

GARCIA, Sheila. **A tutela da privacidade e dos dados pessoais na er a da vigilância**. [*s.l.*]: Processo, 2022.

HALLBERG, Fernando Bottega. **Gestão de arquivos em nuvem na era da LGPD com enfoque em um escritório de advocacia**. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/13546/1/FERNANDO_BOTTEGA_HALLBERG-%5b68352-685-5 953491%5dEstudo_de_Caso__GestAo_em_Ti_-_2021_-_Fernando_Bottega_Hallberg.pdf. Acesso em: jan. 2023.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das melhores práticas de governança corporativa**. São Paulo: IBGC, 2015.

KAGEYAMA, André. **Guia comentado do estatuto da advocacia e da OAB (Lei 8.906/94**). São Paulo: Aurum, 2020.

KAUER, Gisele. **Anonimização, pseudonimização e criptografia:** perguntas frequentes, definições e o que diz a LGPD. InfraNews Telecom, 2023. Disponível em: https://www.infranewstelecom.com.br/anonimizacao-pseudonimizacao-e-

criptografia-perguntas-frequentes-definicoes-e-o-que-diz-a-lgpd/. Acesso em: mar. 2023.
KIRSCHNER, Ana. Responsabilidade social corporativa em escritórios de advocacia. **Revista Processus de Estudos de Gestão, Jurídicos e Financeiros**, v. 4, n. 9, 2013.

KREMER, Bianca. **Os agentes de tratamento de dados pessoais**. São Paulo: Arquipélago, 2020.

LAMBERT, Paul. **The data protection officer:** profession, rules and role. New York: CRC Press, 2017.

LAMBOY, Christian Karl de. **Manual de compliance**. São Paulo: Instituto ARC, 2017.

LEITE, George Salomão; LEMOS, Ronaldo (Coord.). **Marco civil da internet**. São Paulo: Atlas, 2014.

LIMA, Cíntia Rosa de (Coord.). **ANPD e LGPD desafios e perspectivas.** São Paulo: Almedina, 2021.

LIMA, Cíntia Rosa Pereira de. **Autoridade nacional de proteção de dados e a efetividade da Lei Geral de Proteção de Dados:** de acordo com a Lei Geral de Proteção de Dados (Lei n. 13.709/2018 e as alterações da Lei n. 13.853/2019), o Marco Civil da Internet (Lei n. 12.965/2014) e as sugestões de alteração do CDC (PL 3.514/2015). São Paulo: Almedina, 2020.

LIMA, Cintia Rosa Pereira de (Coord.). **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020.

LIMA, Vinícius Albuquerque**. A lei n° 13.709/18 (Lei Geral de Proteção aos Dados Pessoais –LGPD) e sua relação com a advocacia:** o advogado e seus deveres quanto ao tratamento dos dados pessoais. 2021. Disponível em: https://jus.com.br/artigos/94515/a-lei-n-13-709-18-lei-geral-de-protecao-aos-dados-pessoais-lgpd-e-sua-relacao-com-a-advocacia-o-advogado-e-seus-deveres-quanto-ao- tratamento-dos-dados-pessoais. Acesso em: dez. 2022.

LIMBERGER, Têmis. **O direito à Intimidade na era da informática:** a necessidade de proteção de dados pessoais. Porto Alegre: Livraria do Advogado, 2007.

LÔBO, Paulo. **Comentários ao Estatuto da Advocacia e da OAB**. 14. ed. São Paulo: SaraivaJur, 2022.

LONGHI, Maria Isabel Carvalho Sica; COSTA-CORRÊA, André. **Direito e novas tecnologias.** São Paulo: Almedina, 2020.

LÓSSIO, Claudio Joel Brito. **Proteção de dados e compliance digital.** São Paulo, Almedina, 2021.

MARTINS-COSTA, Judith. **A boa-fé no direito brasileiro**. São Paulo: Revista dos Tribunais, 1999.

MENDES, Gilmar; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. **Direito, inovação e tecnologia**. São Paulo: Saraiva, 2015.

MONCAU, Luiz Fernando *et al.* **Contribuição do Centro de Tecnologia e Sociedade da FGV DIREITO RIO ao debate público sobre o Anteprojeto de Lei de Proteção de Dados Pessoais**. Rio de Janeiro:FGV, 2015. Disponível em: https://bibliotecadigital.fgv.br/dspace/handle/10438/17472. Acesso em: abr. 2023.

NALINI, Jose Renato. **Ética geral e profissional:** á ética do advogado. 13. ed. São Paulo: LTR, 2016.

NETTO, Felipe Braga; FARIAS, Cristiano de. **Manual de direito civil**. 2. ed. São Paulo: Saraiva Jur, 2022.

ORDEM DOS ADVOGADOS DO BRASIL. **LGPD nas relações de trabalho**. 2021. Disponível em: https://oabdf.org.br/wp-content/uploads/2021/08/eBook_LGPD-nas-Relacoes-de-Trabalho-1-1.pdf. Acesso em: mar. 2023.

ORDEM DOS ADVOGADOS DO BRASIL. Conselho Federal. **Resolução n. 02/2015.** Disponível em: https://www.oab.org.br/arquivos/resolucao-n-022015-ced-2030601765.pdf. Acesso em: mar. 2023.

ORDEM DOS ADVOGADOS DO BRASIL, SP. **Boas práticas de proteção de dados na advocacia**. 2021. Disponível em: https://jornaldaadvocacia.oabsp.org.br/wp-content/uploads/2021/09/CPPD-OAB-SP-Coordenadoria-de-Educacao-Cartilha-de-Boas-Praticas-rev-2_compressed.pdf. Acesso em: jan. 2023.

ORDEM DOS ADVOGADOS DO BRASIL, SP. **Guia da Lei Geral de Proteção de Dados na Advocacia**. 2019. Disponível em: https://www.conjur.com.br/dl/guia-lgpd-escritorios.pdf. Acesso em: jan. 2023.

ORDEM DOS ADVOGADOS DO BRASIL, SP. **Guia da Lei Geral de Proteção de Dados na Advocacia**. 2020. Disponível em: https://www.conjur.com.br/dl/guia-lgpd-escritorios.pdf. Acesso em: jan. 2023.

ORDEM DOS ADVOGADOS DO BRASIL, SP. **Guia da LGPD aplicada aos escritórios de advocacia**. 2021. Dispponível em: https://oabcampinas.org.br/wp-content/uploads/2021/12/Guia-LGPD_Advocacia.pdf. Acesso em: jan. 2023.

PERREGRIL, Fernanda; CALCINI, Ricardo (Org.). **LGPD e compliance trabalhista:** os desafios atuais do direito do trabalho empresarial. São Paulo: Mizuno, 2021.

PHILIPS, Mark. International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR). **Human Genetics,** n. 137, p. 575–582, 2018. Disponível em: https://doi.org/10.1007/s00439-018-1919-7. Acesso em: jan. 2023.

PINHEIRO, Patricia Peck. **Direito digital**. São Paulo: Saraiva Jur, 2021.

PINHEIRO, Patricia Peck**. Proteção de dados pessoais comentários à Lei n. 13.709/2018:** (LGPD). 3. ed.São Paulo: Saraiva Jur, 2021.

QUAL O IMPACTO da LGPD no dia a dia dos escritórios? 2019. Disponível em: https://digital.fenalaw.com.br/2019/04/16/impacto-lgpd-escritorios/. Acesso em: fev. 2023.

QUEIROZ, João Quinelato. **Responsabilidade civil na rede:** danos e liberdades à luz do marco civil da internet. Rio de Janeiro: Processo, 2019.

RAMPAZZO, F. **Consentimento do paciente no direito médico:** validade, interpretação e responsabilidade. São Paulo: Foco, 2021.

REZENDE, Pedro Antônio Dourado de. **Lei Azeredo, AI-5 digital e a cultura da História.** 2009. Disponível em: https://cic.unb.br/~rezende/trabs/azeredo3.html. Acesso em: jan. 2023.

ROBINSON, Neil *et al.* **Review of the european data protection directive**. Pittsburg: Rand Corporation, 2009. Disponível em: https://www.huntonak.com/files/webupload/PrivacyLaw_review_of_eu_dp_directive.pdf. Acesso em: abr. 2023.

SANCTIS, Fausto M. **Inteligência artificial e direito.** São Paulo: Grupo Almedina, 2020.

SAXENIAN, Annalee. The genesis of silicon valley. **Built Environment**, v. 9, n. 1, 1983.

SCHWABB, Klaus. **A quarta revolução industrial**. São Paulo: Edipro, 2015.

SIBILE, Daniel; SERPA, Alexandre; FARIA, Felipe. **Os pilares do programa de compliance:** uma breve discussão. LEC, 2020. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/BibliotecaDigital/BibDigitalLivros/TodosOsLivros/Os-pilares-do-programa-de-compliance.pdf. Acesso em: jan. 2023.

SOARES, Ellen Amanda Gomes; SANTOS, Pedro Otto Souza; JESUS, Tâmara Silene Moura de. LGPD e a Proteção de Dados pessoais das crianças e adolescentes no ordenamento jurídico brasileiro: o dilema da coleta de dados e a obrigatoriedade do consentimento dos pais. **Brazilian Jourrnal of Development,** v. 7, n. 8, 2021.

STINCO, M. (Coord.) **Compliance à luz da governança corporativa**. São Paulo, InstitutoBrasileiro de Governança Corporativa, 2017.

STRAHUS, Rodrigo. **Direito digital:** o marco civil brasileiro da internet e as inovações jurídicas no ciberespaço. Curitiba: FASP Universitária, 2018.

TEIXEIRA, Tarcísio; GUERREIRO, Ruth Maria. **Lei geral de proteção de dados pessoais (LGPD):** comentada artigo por artigo. São Paulo: SaraivaJur, 2022.
TILT UOL. **Proteção de dados:** conheça os indicados por Bolsonaro para comandar a ANPD. 2020. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/10/17/conheca-os-indicados-por-bolsonaro-para-comandar-a-anpd.htm. Acesso em: jan. 2023.

TOMASEVICIUS FILHO, Eduardo. **Marco civil da internet:** uma lei sem conteúdo normativo. São Paulo: Faculdade de Direito, Universidade de São Paulo, São Paulo, 2015.

UNIÃO EUROPEIA. **Convenção 108, para a Proteção das Pessoas Relativamente ao Tratamento de Dados de Caracter Pessoal**. Conselho Europeu, 1981.

UNIÃO EUROPEIA. **Diretiva de proteção de dados pessoais (95/46/CE**). 1995. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046. Acesso em: jan. 2023.

UNIÃO EUROPEIA. **General data protection regulation 679/2016.** Disponível em https://gdpr-info.eu/. Acesso em: fev. 2023.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679.** Regulamento Geral sobre a Proteção deDados (RGPD). 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=PT. Acesso em: jan. 2023.

UNIÃO EUROPÉIA. **Regulamento 679, de 14 de abril de 2016.** Regulamento Geral sobre a Proteção de Dados. Disponível em: https://gdpr-info.eu/. Acesso em: nov. 2022.

VEIGA, T. M. A LGPD nos escritórios de advocacia previdenciária: o registo das operações de tratamento de dados e o conceito de escritório digital como medidas de base para a conformidade. **Revista Jurídica da Escola Superior de Advocacia OAB de Santa Catarina,** v. 1, n. 1, 2021.

VOIGT, Paul. **The EU general data protection regulation (GDPR):** a practical guide. [*s.l.*]: Springer, 2017.

WIKILEAKS. **Blog WikiLeaks**. Disponível em: https://wikileaks.org/. Acesso em: jan. 2023.

UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS

UNIDADE ACADÊMICA DE PESQUISA E PÓS-GRADUAÇÃO

PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO DA EMPRESA E DOS NEGÓCIOS

NÍVEL MESTRADO PROFISSIONAL

O Trabalho de Conclusão de Curso intitulado: **Adequação de Escritórios de Advocacia à Lei Geral de Proteção de Dados**, elaborado pelo mestrando **Arthur Cravo Battesini,** foi julgado adequado e aprovado por todos os membros da Banca Examinadora para a obtenção do título de MESTRE EM DIREITO DA EMPRESA E DOS NEGÓCIOS - Profissional.

Porto Alegre, 23 de maio de 2023

Prof. Dr. **Fabiano Koff Coulon**

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

Apresentada à Banca integrada pelos seguintes professores:

Presidente: Dr. Cristiano Colombo

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

Membro: Dr. Wilson Engelmann (Participação por webconferência)

Membro externo: Guilherme Damásio Goulart (Participação por webconferência)