VI ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

FREDERICO THALES DE ARAÚJO MARTOS

JÉSSICA AMANDA FACHIN

AIRES JOSE ROVER

D597

Direito, governança e novas tecnologias I [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Aires Jose Rover; Frederico Thales de Araújo Martos; Jéssica Amanda Fachin – Florianópolis; CONPEDI, 2023.

Inclui bibliografia
ISBN: 978-65-5648-745-8
Modo de acesso: www.conpedi.org.br em publicações
Tema: Direito e Políticas Públicas na era digital

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias. VI Encontro Virtual do CONPEDI (1; 2023; Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

VI ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

Apresentação

O VI Encontro Virtual do CONPEDI, realizado em parceria com o Programa de Mestrado Profissional em "Direito, Sociedade e Tecnologias" das Faculdades Londrina e a Faculdade de Direito de Franca (FDF), ocorreu nos dias 20, 21, 22, 23 e 24 de junho de 2023. O evento teve como temática central "Direito e Políticas Públicas na Era Digital". As discussões realizadas durante o encontro, tanto nas diversas abordagens tecnológicas como nos Grupos de Trabalho (GTs), foram de grande relevância, considerando a atualidade e importância do tema.

Nesta publicação, os trabalhos apresentados como artigos no Grupo de Trabalho "Direito, Governança e Novas Tecnologias I", no dia 23 de junho de 2023, passaram por um processo de dupla avaliação cega realizada por doutores. A obra reúne os resultados de pesquisas desenvolvidas em diferentes Programas de Pós-Graduação em Direito, abordando uma parte significativa dos estudos produzidos no âmbito central do Grupo de Trabalho.

As temáticas abordadas refletem intensas e numerosas discussões que ocorrem em todo o Brasil. Elas destacam o aspecto humano da Inteligência Artificial, os desafios para a democracia e a aplicação do Direito no ciberespaço, bem como reflexões atuais e importantes sobre a regulação das plataformas digitais e as repercussões das novas tecnologias em diversas áreas da vida social.

Esperamos que, por meio da leitura dos textos, o leitor possa participar dessas discussões e obter um entendimento mais amplo sobre o assunto. Agradecemos a todos os pesquisadores, colaboradores e pessoas envolvidas nos debates e na organização do evento, cujas contribuições inestimáveis foram fundamentais, e desejamos uma leitura proveitosa!

Prof. Dr. Aires Jose Rover - Universidade Federal de Santa Catarina/SC

Profa. Dra. Jéssica Fachin - Faculdades Londrina/PR

Prof. Dr. Frederico Thales de Araújo Martos - Faculdade de Direito de Franca/SP e Universidade do Estado de Minas Gerais/MG

A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) – LEI Nº 13.709/2018 E SUA APLICABILIDADE NO SETOR PÚBLICO: A NECESSÁRIA BUSCA PELO COMPLIANCE DE DADOS

THE GENERAL DATA PROTECTION LAW (LGPD) - LAW NO. 13,709/2018 AND ITS APPLICABILITY IN THE PUBLIC SECTOR: THE NECESSARY SEARCH FOR DATA COMPLIANCE

Felipe dos Santos Gasparoto [1]
Carlos Henrique Gasparoto [2]
Frederico Thales de Araújo Martos [3]

Resumo

A Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei nº 13.709, promulgada em agosto de 2018, pelo então Presidente da República Michel Temer, veio à luz do direito brasileiro com o grande intuito de introduzir direitos aos titulares da de dados pessoais e deveres aos agentes de tratamento. Deste modo o presente artigo busca explorar as aplicabilidades da Lei Geral de Proteção de Dados (LGPD) – Lei nº 13.709/2018, na Administração Pública direta e indireta, investigando nuances e empenhando-se para esclarecer a quem a LGPD se aplica no setor público, os requisitos, agentes e quais dados que a Administração Pública terá liberdade de tratar, sendo sensíveis ou não sensíveis. Explorar as regras específicas de tratamento de dados para o setor público. Além de trazer proposta de boas práticas e governança para que não sofra as devidas sanções por não agir de acordo com a lei, buscando desta forma a melhor aplicação da LGPD, visando alcançar o compliance de dados, do setor público.

Palavras-chave: Lei geral de proteção de dados, Setor público, Boas práticas, Compliance de dados

Abstract/Resumen/Résumé

The General Law of Protection of Personal Data (LGPD) – Law No. 13,709, promulgated in August 2018, by the then President of the Republic Michel Temer, came to the light of Brazilian law with the great intention of introducing rights to the holders of personal data and duties to the processing agents. In this way, this article seeks to explore the applicability of the General Data Protection Law (LGPD) – Law No. 13,709/2018, in direct and indirect

[1] Pós-graduando em Direito Processual Civil Empresarial pela Faculdade de Direito de Franca – FDF. Advogado. Lattes: http://lattes.cnpq.br/0116392854798241. OrcID: https://orcid.org/0000-0002-9622-1304. E-mail: felipegasparoto.adv@gmail.com

[2] Doutorando em Direito pela FADISP. Mestrado em Direito pela Unifran. Professor Titular de Direito Penal na Faculdade de Direito de Franca.

[3] Doutor em Direito pela FADISP. Professor titular de Direito Civil e Coordenador da Pós-Graduação da FDF. Professor Efetivo de Direito Civil na UEMG. Advogado. frederico.martos@direitofranca.br.

Public Administration, investigating nuances and striving to clarify to whom the LGPD applies in the public sector, the requirements, agents and what data the Public Administration will be free to treat, whether sensitive or non-sensitive. Explore specific data processing rules for the public sector. In addition to bringing proposal of good practices and governance so that it does not suffer the due sanctions for not acting in accordance with the law, seeking in this way the best application of the LGPD, aiming to achieve data compliance, the public sector.

Keywords/Palabras-claves/Mots-clés: General data protection law, Public sector, Good practices, Data compliance

1. INTRODUÇÃO

A importância da internet para a sociedade moderna dispensa um longo arrazoado ou textos de alta complexidade, afinal, a realidade digital convive em simbiose com as relações interpessoais. Nesse contexto, a realidade virtual ganhou protagonismo nas mais diversas formas de relacionamento social, inclusive para o acesso, coleta e armazenamento de dados e informações diversas.

Dentre os diversos entraves existentes, a compreensão e estudo sobre a segurança da informação tangencia direitos fundamentais que merecem a atenção. Por exemplo, o monitoramento e a vigilância são instrumentos de controle importantes para a prevenção dos mais diversos tipos de incidentes e riscos do convívio em sociedade. Contudo, paralelamente, surge a preocupação da necessidade em se respeitar o direito à intimidade e à privacidade.

Para o recorte científico e delimitação desta investigação, pretende-se debruçar sobre a forma de acesso, coleta e armazenamento dos dados pessoais de forma virtual e seus reflexos ao setor público.

No mundo já existem mais de 125 países que possuem algum tipo de legislação de proteção de dados pessoais, muitas delas tendo inclusive legislações específicas sobre a coleta e o processamento desses dados. No Brasil, a primeira legislação nesse sentido foi o Marco Civil da Internet, por meio do Decreto Lei nº 8.771/15, que teve o intuito de complementar as diretrizes de privacidade e liberdade de expressão.

A Lei nº 13.709/2018 cria a Lei Geral de Proteção de Dados – LGPD que regula as atividades de tratamento de dados pessoais e que também altera os artigos 7º e 16 do Marco Civil da Internet.

A LGPD é considerada uma lei complexa de alto impacto, no mesmo nível que ocorreu quando do advento do Código de Defesa do Consumidor, por estabelecer uma série de procedimentos específicos, além de reafirmar princípios que já estavam presentes em outras legislações, como a Constituição Federal de 1988 e o próprio Marco Civil da Internet.

A LGPD aplica-se aos setores público e privado e tenta estabelecer um equilíbrio entre a proteção dos dados dos cidadãos e, no caso do setor público, a utilização desses dados para a elaboração e execução de políticas públicas e a correta prestação de serviços públicos.

Assim sendo, na esfera no setor público, intensifica-se a necessidade de realizar uma profunda harmonização da LGPD com as demais legislações em vigor em face das peculiaridades e formas de responsabilidade civil da Administração Pública.

Acerca deste ponto específico, cumpre observar a criação de um padrão de rotina no qual as medidas são elaboradas com o intuito do órgão da administração pública se "adequar à lei". Embora em uma visão superficial tal afirmação possa se mostrar totalmente normal o que se verifica na prática é um assunto de elevada complexidade, pois envolve a implantação de um sistema de gestão de *compliance* novo e integrado.

Assim sendo, cumpre observar que a organização do sistema de dados parte de diretrizes em comum com o *compliance.* Ou seja, os conceitos utilizados são os mesmos da área de *compliance*, tais como*: tone from the top*, Código de ética e de Conduta, Políticas, Procedimentos e Controles internos, Investigações Internas, Treinamentos, Canais de Denúncia, auditoria, *Due Diligence, risk assessment* etc.

O *Compliance* consiste em um estado dinâmico de conformidade a uma orientação normativa de comportamento com relevância jurídica por força de contrato ou lei, caracterizado pelo compromisso com a criação de um sistema complexo de políticas, de controles internos e de procedimentos, que demonstrem que a empresa está buscando "garantir", que se mantenha em um estado de *compliance*. Assim sendo, os elementos específicos de um *Compliance* de Dados devem ser entendido como parte de um sistema maior de gestão de *compliance*.

Destarte, a ideia de "proteção" visa à assegurar que o cidadão tenha a seu dispor meios para exercer efetivo controle sobre seus dados e, também, que todo o ecossistema em torno do tratamento de dados pessoais tenha contrapesos e incentivos para que danos aos cidadãos sejam evitados. Isto sem, contudo, impedir a inovação a partir do tratamento de tais dados, elemento fundamental da sociedade da informação.

Para o desenvolvimento deste estudo, foi utilizada a metodologia com abordagem qualitativa, método dedutivo e técnicas bibliográfica e documental, por meio de estudos de artigos científicos, livros e doutrinas civilistas, além da própria legislação.

Dessa forma, a escolha do tema justifica-se pela importância em analisar como a LGPD se aplica ao setor público e as implicações dessa regulamentação para o funcionamento das instituições governamentais de uma forma efetiva e coerente com a legislação vigente.

O resultado almejado com a presente pesquisa volta-se para uma reflexão sobre a necessidade de mudança cultural. Afinal, as estratégias necessárias orbitam no campo ética e jurídico.

Por fim, importante salientar que o presente trabalho não teve por objetivo esgotar o debate, mas sim ampliar os espaços acadêmicos de discussão a respeito de uma situação que demanda preocupação jurídica.

2. A LEI DE PROTEÇÃO DE DADOS, SEUS PRINCÍPIOS E SEUS AGENTES

Ao estudar a Lei Geral de Proteção de Dados deve-se entender o que são dados pessoais, partindo-se da premissa que eles podem ser definidos como qualquer informação que tenha relação com pessoa natural identificada ou ao menos identificável. É evidente que se trata de uma definição bastante ampla, visto que abrange desde informações mais públicas como o nome até as senhas ou mensagens destinadas para uma determinada pessoa (MARTOS, FRATTARI, FURLAN, 2022, p. 297)

O perfil atual da proteção de dados está fortemente ligado aos marcos regulatórios adotados na Europa e nos Estados Unidos. A realidade brasileira adotou as tendências de outros países, facilitando a harmonizações das legislações e regramentos existentes.

A Emenda Constitucional nº 115/2022 introduziu importantes mudanças na Constituição Federal em busca de ampliar a proteção de dados dos indivíduos. O emblemático artigo 5º, mais especificamente no recente inciso LXXIX, consigna que "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais" dentro os direitos e garantias fundamentais.

Outra alteração constitucional que merece ser apontada é a inclusão do inciso XXVI no artigo 21 da Constituição Federal, consignando a competência da União para "organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei". Assim sendo, de forma expressa o Estado declara e reconhece a sua importância em se criar instrumentos garantidores de proteção dos dados e sua forma de circulação.

Nesse contexto foi criada a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, e tem o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (art. 1º).

Ainda guarda ares de "novidade" a incorporação do termo "proteção de dados pessoais" ao glossário jurídico brasileiro. A LGPD é considerada uma lei complexa e de alto impacto, por estabelecer uma série de procedimentos específicos, além de reafirmar princípios que já estavam presentes em outras leis, como a nossa carta magna de 1988 e o próprio Marco Civil da Internet.

Além disso, existe a demanda de realizar uma profunda harmonização com legislações vigentes, como a Lei de Acesso à Informação, que requer um trabalho de adequação minucioso e de alta complexidade, especialmente no setor público.

A LGPD estabelece diferentes princípios norteadores do tratamento de dados pessoais. Esses princípios reforçam o fato de que a nova lei busca modificar completamente a cultura e a tutela jurídica de dados pessoais na era da informação, merecendo destaque o teor do art. 6º da lei:

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

Merece destaque, também, os conceitos e definições presentes no art. 5º da lei, em especial relacionado a 3 (três) figuras: o "controlador", o "operador" e o "encarregado", apresentando o seguinte:

> [...]
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.
> [...]

Nessa jornada de adequações, de acordo com a visão de Doneda, deve-se considerar que:

> A LGPD, apesar de, como verificado, procurar sistematizar a problemática relacionada ao tratamento de dados pessoais e proporcionar um eixo em torno do qual a disciplina passa a se estruturar, não cumpre essa tarefa meramente com a absorção de elementos já presentes na nossa ordem jurídica. Na verdade, a lei apresenta diversos elementos novos que, por si sós, causaram certo impacto, o fato de consolidarem em uma normativa toda a matéria foi somente o primeiro deles: com a LGPD, passa a integrar o ordenamento toda uma nova série de institutos próprios da disciplina da proteção de dados, de direitos do titular, um enfoque novo de tutela dos titulares é proporcionado pelas regras de demonstração e prestação de contas (*accountability*), são considerados elementos que levam em conta o risco em atividades de tratamento de dados pessoais e muitas outras (DONEDA; MENDES; CUEVA; 2020, p.254-255).

Também chamado de DPO, o encarregado de dados deve, primeiramente, ser alguém com autonomia para exercer uma função fiscalizatória interna. Mas também possui prerrogativas de interlocutor com a AND.

Sendo recomendável que o DPO seja um profissional multidisciplinar, com conhecimentos das legislações vigentes, conhecimentos sobre governança de base de dados pessoais, de segurança da informação, mas que tenha habilidade para se relacionar como porta-voz da instituição perante as autoridades e também perante os titulares de dados, principalmente nos caso aonde houver necessidade de reportar incidentes de violações de dados pessoais.

Insta salientar que os titulares são as pessoas naturais a quem se referem os dados pessoais que são objeto de tratamento. Titular será o contribuinte, servidor ou empregado público, gestor público, pessoa física com a qual o órgão ou entidade pública possui alguma relação contratual.

3. A ORGANIZAÇÃO DA ADMINISTRAÇÃO PÚBLICA

Antes de adentrar nos aspectos legais e regulamentares da LGPD, mostra-se relevante compreender alguns pontos que envolvem a Administração Pública, na qual o sistema de informação e os programas de integridade serão implementados. Esse panorama inicial se faz importante em face das diferenças que envolvem as pessoas privadas e públicas quanto ao limites e autonomia e forma de atuação

Castro (2018, p. 16) explique que "a administração pública deve ser vista como contraponto da administração privada. Lá tudo é permitido, exceto o que a lei proíbe. Na área pública nada é permitido, somente o que a legislação autoriza.”. Assim sendo, o administrador público possui uma função muito mais limitada e restrita, pois o seu comportamento está pautado nos permissivos da lei.

A Administração Pública se divide em direta: envolvendo os poderes Legislativo, Executivo e Judiciário, disposto no artigo 2° da Constituição Federal; e indireta, a qual engloba as autarquias, empresas públicas, sociedades de economia mista e fundações públicas, tendo em vista o Decreto-lei 200/67, e o disposto no caput do artigo 37 da Constituição Federal. Acerca da segunda categoria, adiante apresenta-se alguns conceitos para a melhor compreensão dos institutos.

Castro (2018, p.16) ensina que as autarquias são as entidades criadas por lei, possuindo personalidade jurídica, patrimônio e receita próprias. Apesar de desempenharem atividades da Administração Pública, possuem gestão financeira autônoma e descentralizada.

Acerca das empresas públicas ou estatais, importante destacar que possuem personalidade jurídica de direito privado, patrimônio próprio e capital exclusivo da União. O objetivo de sua criação é a exploração de uma atividade que o governo entende ser conveniente aos objetivos do próprio Estado (CASTRO, 2018, p. 16).

No que concerne às fundações públicas, elas podem ser classificadas como atividades que são do interesse coletivo, nas áreas da educação, cultura e pesquisa, são autorizadas e estruturadas por Decreto (CASTRO, 2018, p. 16).

Já as sociedades de economia mista são pessoas jurídicas de direito privado com seu capital e administração compostos pelo Poder Público e por particulares. São responsáveis pela execução de atividades de interesse coletivo, as quais são delegadas pelo próprio Estado (CASTRO, 2018, p. 17).

A compreensão básica da estrutura do Estado com relação a Administração Pública Direta e Indireta permite constatar a complexidade que se estrutura o próprio Estado, tornando desafiador (e indispensável!) a criação de um sistema de informação e coleta de dados em conformidade com as particularidades de cada órgão, setor, departamento da administração pública e a legislação vigente.

4. DA APLICAÇÃO DA LEI AO SETOR PÚBLICO

A Lei Geral de Proteção de Dados (LGPD) também tem impacto significativo no setor público, uma vez que as instituições públicas também coletam e tratam dados pessoais. A LGPD estabelece que os órgãos e entidades da administração pública devem adotar medidas para garantir a proteção dos dados pessoais que coletam, inclusive por meio de nomeação de um Encarregado de Proteção de Dados (DPO).

Além disso, a lei também estabelece regras específicas para o tratamento de dados pessoais por parte do setor público, como a necessidade de consentimento explícito dos titulares dos dados para o tratamento de informações sensíveis e a possibilidade de compartilhamento de dados pessoais entre órgãos da administração pública apenas em situações específicas e mediante autorização legal.

A LGPD busca, assim, garantir a proteção dos dados pessoais também no âmbito das instituições públicas, garantindo a privacidade e os direitos dos cidadãos brasileiros.
A lei abrange todas as empresas do setor público? Conforme o artigo 3º da lei se aplica a todo e qualquer órgão ou entidade pública, empresas públicas e sociedades de economia mista.

No seu artigo 4º, o legislador explica o que está de fora da aplicação da lei, sendo os casos de tratamentos de dados realizados para fins exclusivamente: jornalísticos e artísticos; acadêmicos; fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais. E casos de tratamentos de dados provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado à LGPD.

O Controlador no setor público será o órgão público, entidade pública, empresa pública ou sociedade de economia mista que toma as decisões a respeito do tratamento de dados pessoais. O órgão público que mantém um banco de dados de seus servidores ou empregados públicos também se enquadraria nesta definição. Será o Operador que irá realizar o tratamento dos dados pessoais em nome do Controlador.

O órgão ou entidade pública, empresa pública ou sociedade de economia mista, quando atuar na qualidade de controlador, deverá indicar encarregado pelo tratamento de dados pessoais.

A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

Devendo este ficar responsável por aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências. Além de receber comunicações da autoridade nacional e adotar providências e orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais. Podendo ainda executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

A Autoridade Nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

Porém, até que sejam definidas tais regras pela Autoridade, todos os órgãos públicos, entidades públicas, empresas públicas e sociedades de economia mista que atuarem como controladores terão que nomear um encarregado pelo tratamento de dados pessoais.

O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do Artigo 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

Desde que, sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos

Estas devem apresentar o consentimento do titular, sendo este uma manifestação livre, informada e inequívoca que autoriza o tratamento de dados pessoais para uma finalidade determinada.

Não é admitido um consentimento implícito. Esse consentimento, diferente das demais bases legais autorizativas do tratamento de dados pessoais, pode ser revogado a qualquer momento.

Ou quando estiver presente alguma das seguintes situações: Cumprimento de obrigação legal ou regulatória pelo controlador. Pela Administração Pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.

Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais. Nessa hipótese se enquadra, por exemplo, a pesquisa realizada por universidade públicas e, também, por institutos de pesquisa públicos.

Quando é 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. É o caso, por exemplo, de contratos celebrados pela administração pública com fornecedores de produtos ou serviços, assim como concessões de serviços públicos e de uso de bens públicos, contratos de parcerias público-privadas e outros instrumentos contratuais da Administração Pública.

Para o exercício regular de direitos em processo judicial, administrativo ou arbitral. Essa hipótese se aplicaria, por exemplo, ao tratamento de dados pessoais de servidores ou empregados públicos para fins de defesa dos interesses da administração pública em processos judiciais ou mesmo administrativos, o mesmo valendo para o tratamento de dados pessoais de contribuintes nas mesmas hipóteses.

Para a proteção da vida ou da incolumidade física do titular ou de terceiro. O tratamento de dados pessoais no âmbito da atuação da Defesa Civil, com vistas a proteger a vida e a incolumidade física do titular ou de terceiros se enquadraria nessa hipótese.

Para a tutela da saúde, em procedimento a ser realizado por profissionais da área da saúde ou por entidades sanitárias. Hospitais públicos e demais entidades sanitárias públicas estão autorizadas a tratar dados dos respectivos pacientes, sem seu consentimento, para fins de tutela da saúde.

Quando é necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

5. DO COMPLIANCE DE DADOS

A tendência que se nota nas mais variadas iniciativas é tratar a área de “adequação à lei geral de proteção de dados” como se fosse algo completamente diferente da implementação de um sistema de gestão de *compliance*. No entanto, quando se observa mais de perto o que a legião de “novos especialistas” entende por “adequação à lei geral de proteção de dados”, os conceitos utilizados são os mesmos da área de *compliance.*

Em tradução livre, *compliance*, significa “estar em conformidade”, “cumprir”, “estar de acordo”. Todavia a compreensão que se busca ao termo *Compliance* e muito mais ampla, pois pretende-se estabelecer uma relação, entre o “estado de conformidade “e uma determinada “orientação de comportamento”.

Desta forma, o *compliance* consiste em um estado dinâmico de conformidade a uma orientação normativa de comportamento com relevância jurídica por força de contrato ou lei, caracterizado pelo compromisso com a criação de um complexo sistema de políticas, de controles internos e de procedimentos, que demostrem que a empresa está buscando “certificar”, que se mantenha em um estado de *compliance*.

Compliance de dados é o conjunto de práticas e políticas que visam garantir que as empresas e organizações estejam em conformidade com as leis e regulamentos relacionados ao uso, armazenamento e proteção de dados. Isso inclui uma série de medidas de segurança e privacidade para proteger os dados contra acessos não autorizados, perda ou roubo.

Um dos principais regulamentos de *compliance* de dados é a Lei Geral de Proteção de Dados (LGPD) no Brasil, que entrou em vigor em 2020. A LGPD estabelece regras claras, em seu capitulo VII, quando trata da segurança e das boas praticas dos artigos 46 ao 51, para o uso de dados pessoais, incluindo informações de clientes, funcionários e fornecedores. As empresas que não estão em conformidade com a LGPD podem enfrentar multas significativas.

Outros regulamentos de *compliance* de dados incluem a Lei de Proteção de Dados Pessoais da União Europeia (GDPR), o Ato de Proteção de Informações Pessoais do Japão (APPI) e a Lei de Privacidade do Consumidor da Califórnia (CCPA).

Avaliação de dados, ou *data assessments*, é um processo de avaliação sistemática e crítica das práticas e processos de gerenciamento de dados de uma organização, com o objetivo de identificar pontos fortes e áreas de melhoria.

A doutrina, trata de diferentes tipos de *data assessments*, dando um especial atenção aos a) *Risk Assessment* (Análise de risco); b) *Data Mapping* (Inventário e registro de dados); c) *Privacy Impact Assessement* (PIA) e d) *Data Protection Impact Assessmene* (DPIA).

A avaliação de risco é elemento essencial de qualquer sistema de gestão de *compliance.* Sendo a razão de sua existência, analisar e gerenciar riscos de sistemas de gestão de *compliance*.

Existem duas metodologias aceitas mundialmente como referência de melhores práticas de gestão de riscos; 1) *COSO Enterprise Risk Management* (COSO-ERM) e 2) ISO 31.000.

As referidas metodologias são constituídas de algumas etapas fundamentais, como conhecer a empresa, seu ambiente legal e suas obrigações de *compliance*, realizar entrevistas e análises de documentos, fazer testes e checagens dos dados levantados, identificar riscos e fatores de riscos, deve também realizar avaliações de probabilidade, além de desenvolver matriz de risco e por fim realizar o monitoramento.

O inventário de dados, ou *data map*, é um dos elementos fundamentais, de um sistema de gestão de *compliance* de dados e tem como principal função apontar os dados que transitam vários sistemas e serve para indicar como os dados são compartilhados.

Um PIA é uma análise dos riscos de privacidade e proteção de dados associada ao "processamento de informação pessoal em relação a um projeto, produto ou serviço". Do mesmo modo, serve para reconhecer ou prover medidas atenuantes necessárias para evitar os riscos identificados. Sendo essa metodologia, uma facilitadora para a implementação da *privacy by design*, exigido pela GPDR.

Por fim, quando uma organização ou empresa coleta ou faz uso de dados pessoais, quem os utiliza está exposto a risco, A DPIA expõe "o processo designado para identificar riscos, que surge do processamento de dados pessoais e para minimizar esses riscos o máximo e o mais rápido possível". Sendo desta forma o DPIA uma das metodologias utilizadas para a implantação de um sistema de gestão de *compliance* de dados.

Porém as legislações vigentes determinam que uma determinada metodologia seja aplicada, na iminência da implementação do *Compliance* de dados, o *Privacy by Design*.

Essa metodologia expõe que privacidade e proteção de dados estão intrinsecamente ligadas com todo o ciclo de vida das tecnologias, do desenho inicial até o seu lançamento no mercado. O seu conceito fundamental implica que as organizações devem sempre criar produtos e serviços estejam de acordo com as diretrizes de um sistema de gestão de *compliance* dados, assim como as melhores práticas e medidas a serem aplicadas diretamente nas tecnologias, nos sistemas e nas práticas vinculadas a todo o ciclo de vida dos produtos e serviços das organizações e empresas.

Outra metodologia exigida pelas leis vigentes é o Código de Ética e de Conduta, devendo esse ter um capítulo reservado para os valores e princípios da área de proteção de dados e privacidade. Este deve ainda refletir os valores da empresa, a criação de um comitê interno de dados e informações sobre o canal de denúncias da empresa.

Martos e Frattari (2019, p. 76) destacam que

> É de significativa relevância que o conteúdo do Código de Ética seja o reflexo das práticas empresariais e condutas realizadas pelas pessoas relacionadas, inclusive pelo alto escalão da empresa, pois, para comprovar a efetividade de seus mandamentos, o comportamento de todos precisa estar em sintonia com tais diretrizes, principalmente dos que exercem cargos superiores.
> [...]
> Cumpre ressaltar que o Código de Ética precisa resultar do consenso entre as pessoas envolvidas, e que nele deve haver participantes de todas as classes relacionadas ao desenvolvimento da atividade empresarial. Logo, tal normativa não pode se originar da vontade e do envolvimento de um único sujeito.
> Ainda sobre a elaboração do Código de Ética, deve-se observar que, para gerar amplo comprometimento, deve ser, preferencialmente, desenvolvido por um comitê representativo de todos os grupos e níveis funcionais e gerenciais.

Vale destacar, a presença do DPO (*Data Protection Officer*) uma vez mais apontado como exigência legal, para se gerenciar o sistema de gestão de dados, como uma das metodologias de *compliance* de dados.

Ademias, duas políticas são de suma importância para se alcançar o *Compliance*, a Política de Privacidade e Proteção de Dados, sendo essa um compilado de descrições de todas as medidas atenuantes, procedimentos, controles internos, que deverão ser adotados na empresa. Apenas uma apropriada avaliação de riscos pode auxiliar a compreender quais são as informações, riscos e medidas mitigatórias que devem se adotados para evitar ou atenuar riscos de dados.

Da mesma forma, outra política a ser adotada é a Política de Terceiros, deve ser considerado a revisão dos contratos com fornecedores para inserir cláusulas específicas relacionadas ao tratamento de dados. Cláusulas essas que vão reforçar ao fornecedor ou terceiro controlador dos dados a importância do mesmo manter os mesmos níveis de segurança e proteção de dados adotados pelo contratante.

Para garantir o *compliance* de dados, as empresas devem implementar medidas de segurança e privacidade, incluindo a criptografia de dados, a autenticação de usuários, o gerenciamento de acessos e a segurança física dos equipamentos. As empresas também devem estabelecer políticas claras para o uso de dados e treinar seus funcionários sobre as práticas de segurança de dados.

Além disso, é suma importância que as empresas realizem auditorias regulares para garantir que suas práticas de segurança e privacidade estejam em conformidade com as leis e regulamentos aplicáveis. Em caso de violações de dados, as empresas devem notificar as

autoridades competentes e os indivíduos afetados o mais rápido possível, a fim de minimizar os danos potenciais.

6. CONCLUSÃO

A LGPD tem implicações significativas para a gestão das informações governamentais e para a privacidade dos indivíduos. A aplicação da lei no setor público é essencial para garantir que as informações pessoais sejam coletadas e tratadas de acordo com as diretrizes estabelecidas pela lei.

A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, representa um marco importante na regulamentação da proteção de dados pessoais no Brasil, estabelecendo direitos e obrigações tanto para o setor público quanto para o setor privado.

A LGPD busca assegurar a privacidade e proteção dos dados pessoais dos cidadãos, garantindo que seu tratamento seja feito de forma adequada, segura e transparente.

No contexto do setor público, a LGPD tem uma aplicabilidade específica, considerando que órgãos e entidades governamentais também tratam uma grande quantidade de dados pessoais em suas atividades cotidianas. Nesse sentido, a busca pelo *compliance* de dados, ou seja, a conformidade com as disposições da LGPD, é essencial para garantir que os órgãos e entidades do setor público cumpram com as obrigações previstas na legislação.

Uma das principais mudanças trazidas pela LGPD é a necessidade de obtenção de consentimento expresso e específico do titular dos dados para o tratamento de suas informações pessoais, exceto em casos de cumprimento de obrigação legal, execução de políticas públicas, proteção à vida, entre outras situações previstas na lei. Isso implica em uma mudança cultural no setor público, que deve se preocupar em obter o consentimento adequado dos cidadãos antes de coletar e tratar seus dados pessoais.

Além disso, a LGPD estabelece princípios importantes para o tratamento de dados pessoais, tais como a: finalidade, adequação, necessidade, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas. Esses princípios devem ser observados pelos órgãos e entidades do setor público em todas as suas atividades relacionadas ao tratamento de dados pessoais, desde a coleta até o descarte dessas informações.

A LGPD também prevê a obrigação de realizar a Avaliação de Impacto à Proteção de Dados (AIPD) em determinadas situações, como em casos de tratamento de dados sensíveis,

realização de decisões automatizadas com base em dados pessoais, transferência internacional de dados, entre outros.

A AIPD é uma ferramenta importante para identificar e mitigar riscos à privacidade e proteção de dados, permitindo que o setor público adote medidas adequadas de segurança e conformidade.

Outro aspecto relevante é a obrigatoriedade de nomeação de um encarregado de proteção de dados (DPO) pelo setor público, que será o responsável por monitorar a conformidade com a LGPD, orientar os funcionários e atuar como ponto de contato com os titulares dos dados e com a Autoridade Nacional de Proteção de Dados (ANPD). A figura do DPO é fundamental para garantir uma abordagem proativa e efetiva na implementação das medidas de *compliance* de dados no setor público.

A falta de conformidade com a LGPD pode resultar em sanções administrativas significativas, como multas, advertências, bloqueio ou eliminação de dados, além de outras consequências jurídicas, financeiras e na sua reputação. Portanto, é fundamental que os órgãos e entidades do setor público busquem a conformidade.

Desta forma, se mostra cada dia mais presente e fundamental a adequação das empresas públicas, nas normas da Lei Geral de Proteção de Dados, seja para estar em conformidade com o *compliance* de dados, seja para proteger seus titulares, quanto para se proteger das possíveis sanções que podem ser impostas contra a empresa.

REFERENCIAS

BACHUR, João Paulo. **Proteção de Dados Pessoais na Educação.** In: DONEDA, Danilo. Et al. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021

BARRETO, Maurício L; ALMEIDA, Bethânia & DONEDA, Danilo. **Uso e Proteção de Dados na Pesquisa Científica**. In: DONEDA, Danilo. Et al. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021

BELLI, Luca. **Como Implementar a LGPD por Meio da Avaliação de Impacto Sobre Privacidade e Ética de Dados (AIPED).** In: DONEDA, Danilo. Et al. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021

BRASIL. **LEI Nº 12.965, DE 23 DE ABRIL DE 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela & PONCE, Paula Pedigoni. **Boas Práticas e Governança na LGPD**. In: DONEDA, Danilo. Et al. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021

CASTRO, Domingos Poubel de. **Auditoria, Contabilidade e Controle Interno no Setor Público**. 7ª ed. São Paulo: Atlas. 2018.

DAL POZZO, Augusto Neves & MARTINS, Ricardo Marcondes, Cood. **Compliance no Direito Administrativo.** São Paulo: Thomson Reuters Brasil, 2020.

DONDA, Daniel. **Guia Prático de Implementação da LGPD.** São Paulo: Labrador, 2020.

DONEDA, Danilo. **Panorama Histórico da Proteção de Dados Pessoais**. *in*: DONEDA, Danilo. Et al. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021

GARCIA, Lara Rocha, AGUILEIRA-FERNANDES, Edson, GONÇALVES, Rafael Augusto Moreno & PEREIRA-BARRETTO, Marcos Ribeiro. **Lei Geral de Proteção de Dados (LGPD): Guia de implementação.** São Paulo: Blucher, 2020

LEMOS, Ronaldo; BRANCO, Sérgio. **Privacy By Design: Conceito, Fundamentos e Aplicabilidade na LGPD.** In: DONEDA, Danilo. Et al. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021

LÓSSIO, Claudio Joel Brito. **Manual Descomplicado de Direito Digital: Guia para profissionais do Direito e da Tecnologia.** 3ª ed. rev., atual e ampl. São Paulo: Editora Juspodivm, 2022

MARINHO, Fernando. **Os 10 mandamentos da LGPD: Como implementar a Lei Geral de Proteção de Dados em 14 passos.** 1 ed. São Paulo: Atlas 2020.

MARTOS, F. T. A.; FRATTARI, M. B. ; FURLAN, H. A. P. . Lei Geral de Proteção de Dados e a Tutela dos Dados Pessoais de Crianças e Adolescentes: A Importância da Proteção do Vulnerável e o Consentimento Parental. *in*: V Encontro Virtual do CONPEDI, 2022. direito de família e das sucessões. Florianópolis: CONPEDI, 2022. p. 293-310. Disponível em: http://site.conpedi.org.br/publicacoes/465g8u3r/u24i7du9/B5Kd9r4Fio6Qu8U8.pdf. Acesso em 24 abr. 2023.

MARTOS, F. T. A.; FRATTARI, M. B. **A Empresa Estrategista: A Revitalização da Ética nas Relações Empresariais e os Códigos de Conduta**. Revista Eletrônica da Faculdade de Direito de Franca, [S. l.], v. 14, n. 1, p. 65–83, 2019. DOI: 10.21207/1983.4225.721. Disponível em: https://www.revista.direitofranca.br/index.php/refdf/article/view/721. Acesso em: 24 abr. 2023.

PINHEIRO, Patrícia Peck. **Direito Digital**. 7 ed. São Paulo: Saraiva Educação, 2021

SAAVREDA, Giovani Agostine. **Complice de Dados**. *In*: DONEDA, Danilo. Et al. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021

SARLET, Ingo Wolfgang. **Fundamentos Constitucionais: O Direito Fundamental à Proteção de Dados.** In: DONEDA, Danilo. Et al. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021

TEIXEIRA, Tarcisio. **Direito Digital e Processo Eletrônico.** São Paulo: Saraiva Educação, 2020.

WIMMER, Miriam. **Os Desafios do Enforcement na LGPD: Fiscalização, Aplicação de Sanções Administrativas e Coordenação Intergovernamental**. *in*: DONEDA, Danilo. Et al. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021