

MINISTÉRIO PÚBLICO DO ESTADO DO CEARÁ
ESCOLA SUPERIOR DO MINISTÉRIO PÚBLICO DO CEARÁ
CENTRO DE ESTUDOS E APERFEIÇOAMENTO FUNCIONAL

REVISTA ACADÊMICA ESCOLA SUPERIOR
DO MINISTÉRIO PÚBLICO DO CEARÁ

ANO 16, Nº 1 (JAN./JUN. 2024) SEMESTRAL
FORTALEZA-CE

ISSN FÍSICO: 2527-0206
ISSN ELETRÔNICO: 2176-7939



MPCE
Ministério Público
do Estado do Ceará



ESMP
ESCOLA SUPERIOR DO MINISTÉRIO
PÚBLICO DO ESTADO DO CEARÁ



CEAF
CENTRO DE ESTUDOS E
APERFEIÇOAMENTO FUNCIONAL

A ATUAÇÃO DO DIREITO NA PRIVACIDADE E PROTEÇÃO DOS DADOS PESSOAIS¹

THE ACT OF THE LAW IN PRIVACY AND PROTECTION OF PERSONAL DATA

*Antônia Ladymilla Tomaz Caracas Bandeira²
Jussara Suzi Assis Borges Nasser Ferreira³*

RESUMO

O aumento da disseminação da informação abriu portas para inúmeras pessoas acessarem uma variedade de serviços digitais. Para salvaguardar o direito à privacidade e à proteção de dados, surgiu a necessidade de regular essa questão, por meio de legislações e criação de autoridades reguladoras. Objetivou-se discorrer sobre a atuação do direito na privacidade e proteção dos dados pessoais. Trata-se de revisão de literatura, com recorte temporal dos últimos 10 anos. Concluiu-se que a proteção de dados e a preservação da privacidade não são apenas teorias, mas também questões práticas que afetam a elaboração de regulamentações, o funcionamento das economias e a cultura empresarial.

Palavras-chave: dados pessoais; direito; era digital; lei geral de proteção de dados; privacidade.

1 INTRODUÇÃO

A sociedade contemporânea, frequentemente denominada de “Sociedade da Informação”, é caracterizada pelo papel central que a informação desempenha em seu desenvolvimento econômico. Esse fenômeno é impulsionado pelo crescente uso das tecnologias de comunicação e informação, que permitem o processamento e tratamento de dados em uma escala e velocidade sem precedentes. Isso, por sua vez, é fundamental para a geração de riqueza e o progresso social.

1 Data de Recebimento: 23/04/2024. Data de Aceite: 06/08/2024.

2 Doutoranda em Direito, Empreendimentos Econômicos, Processualidade e Relações Jurídicas pela Universidade de Marília (Unimar). Mestre em Direito pelo Centro Universitário 7 de Setembro (Uni7). Titular de Serventia Extrajudicial no Estado do Ceará – 1º Ofício de Araripe. E-mail: mila18891@hotmail.com. Lattes: <http://lattes.cnpq.br/6710357621033651>. ORCID: 0009-0005-4240-9992.

3 Doutora em Direito das Relações Sociais pela Pontifícia Universidade Católica de São Paulo (PUC-SP). Mestre em Direito pela Universidade Estadual de Londrina (UEL). Professora titular do PPGD da Universidade de Marília (Unimar). E-mail: sarasuzi@unipar.br. Lattes: <http://lattes.cnpq.br/4193332125844267>. ORCID: 0000-0002-4919-6935.

Com o advento da economia digital nos anos 1990 e a globalização, a dependência dos fluxos internacionais de dados tornou-se mais evidente, destacando-se a necessidade de regulamentações para proteger dados pessoais. No Brasil, a Lei n. 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), busca garantir a proteção dos direitos fundamentais de liberdade, privacidade e desenvolvimento pessoal em um ambiente onde os dados pessoais desempenham um papel cada vez mais importante.

A definição de dados pessoais, de acordo com a LGPD, engloba informações relacionadas a pessoas identificáveis, que têm um impacto significativo na vida das pessoas e em suas relações. Proteger esses dados é essencial, pois sua coleta permite um mapeamento detalhado da personalidade dos titulares, o que, se mal utilizado, pode prejudicar o desenvolvimento da sua personalidade e manipular seus interesses.

A revolução tecnológica na comunicação originou a Sociedade da Informação, onde o acesso à informação em tempo real representa uma característica marcante. No entanto, essa facilidade de obtenção de dados também levanta questões sobre a privacidade dos indivíduos, criando conflitos entre garantias constitucionais e interesses sociais, como o direito à informação.

À medida que a influência digital se expande, os direitos à privacidade e à proteção de dados ganham uma importância ainda maior. O desequilíbrio de poder entre os controladores de dados e os indivíduos cujos dados estão envolvidos é evidente, exigindo regulamentações que garantam a eficácia desses direitos e, por extensão, o direito à liberdade.

Nesse contexto, o princípio da *privacy by design* emerge como um guia fundamental para a regulamentação, garantindo a proteção de dados desde o início do desenvolvimento de novas tecnologias. Esse princípio orienta a formulação de diretrizes normativas e metodologias de trabalho que assegurem a efetiva proteção dos dados pessoais em um mundo cada vez mais digitalizado.

Diante do exposto, este estudo foi desenvolvido a partir da temática que envolve a atuação do direito diante da privacidade de dados pessoais. Sendo assim, buscou-se responder ao seguinte questionamento: de que forma o direito pode atuar para garantir a privacidade dos dados de usuários frente à sociedade da informação?

Para responder ao questionamento proposto, esta pesquisa teve como objetivo geral destacar como o direito pode atuar para garantir a privacidade dos dados e como objetivos específicos, abordar a privacidade na contemporaneidade, discorrer acerca da necessidade da criação da LGPD, bem como esclarecer formas de proteção de dados pessoais.

A realização deste estudo justifica-se devido à relevância da proteção dos dados pes-

soais demandando-se, portanto, evitar que o fluxo de informações seja prejudicial ao livre desenvolvimento da personalidade humana ou à manipulação de seus interesses. Ressalta-se que, a análise da temática é importante devido aos diversos problemas que surgem em decorrência do conflito entre o direito à privacidade e outros interesses sociais, como o direito à informação. Assim, este estudo pode fornecer uma contribuição valiosa para a discussão dos desafios relacionados à privacidade, intimidade e superexposição na era digital, fornecendo elementos importantes sobre como equilibrar esses direitos e interesses em uma sociedade cada vez mais tecnológica.

Para o desenvolvimento deste estudo foi realizada uma revisão de literatura, tomando-se como base uma pesquisa bibliográfica a partir de autores de artigos científicos, publicações eletrônicas e livros que abordaram acerca da temática. Assim sendo, utilizou-se o recorte temporal referente aos últimos 10 anos, a fim de tornar o estudo o mais atual possível.

2 A PRIVACIDADE NA CONTEMPORANEIDADE

A concepção de privacidade tem evoluído desde a cunhagem do termo no final do século XIX, adaptando-se às diferentes situações e às demandas da sociedade ao longo do tempo. Com o avanço das tecnologias de informação e comunicação, houve uma expansão dos meios disponíveis, o que facilitou a coleta, o processamento e o uso de informações públicas e privadas. Isso desempenhou um papel fundamental na definição moderna de privacidade, centrada na ideia de autodeterminação informativa (Genso; Picoli; Luz, 2023, p. 24).

Conforme destacado por Genso, Picoli e Luz (2023, p. 24), inicialmente, o conceito de privacidade tem suas raízes no trabalho intitulado *The right to privacy*, escrito pelos advogados Samuel D. Warren e Louis D. Brandeis, e publicado em 1890 na revista jurídica da Universidade de Harvard, a *Harvard Law Review*. Esse artigo surgiu como resultado do desconforto causado pelo fato de a mídia americana expor e detalhar aspectos das vidas pessoais dos indivíduos, incluindo informações sobre a vida conjugal de Warren. Por meio desta obra, os autores tinham como objetivo estabelecer certos limites para a intrusão da imprensa na esfera privada das pessoas.

De acordo com Bioni (2021, p. 52), a partir da referida obra, é possível compreender o direito à privacidade como o direito de desfrutar de solidão, livre de qualquer intromissão externa, assim como o direito de determinar quais informações pessoais serão tornadas públicas. Isso se alinha com a lógica da privacidade, que implica na liberdade negativa de não sofrer interferência de terceiros.

Nesse contexto histórico, a privacidade era percebida como um privilégio vinculado

à propriedade, uma vez que apenas uma classe social, a burguesia, tinha a consciência e os meios para desfrutar desse direito. Ter a capacidade de isolar-se da sociedade, seja por escolha ou necessidade, a fim de desfrutar de total privacidade, era, portanto, um privilégio. Isso sugere que o surgimento da privacidade foi, na verdade, a aquisição de privilégios por parte de um grupo específico, em vez de uma necessidade intrínseca e natural de cada indivíduo (Machado, 2014, p. 32).

Ainda segundo Machado (2014, p. 33), embora a tecnologia traga benefícios evidentes para a sociedade, também suscita várias preocupações relacionadas aos direitos fundamentais que foram conquistados ao longo da história. Isso se torna especialmente relevante, quando a rápida transferência de informações e dados pessoais afeta, diretamente, o controle da privacidade individual. Portanto, hoje em dia, a tradicional definição de privacidade como o “direito de ser deixado em paz” mostra-se inadequada, uma vez que o debate sobre esse direito não se limita apenas à proteção da esfera privada contra intromissões externas, mas se expande para outras dimensões, como a capacidade de cada indivíduo controlar a utilização de suas próprias informações.

Percebe-se que o conceito de privacidade evoluiu substancialmente, e a concepção tradicional de privacidade como o “direito de ficar sozinho” difere, significativamente, da nova perspectiva de privacidade, que é vista como o “direito à autodeterminação informativa”. Essa última definição atribui a cada indivíduo o verdadeiro controle sobre suas informações e dados pessoais (Bioni, 2021, p. 17).

A noção de autodeterminação informativa foi introduzida pelo jurista Stefano Rodotà, que propôs esse novo conceito de privacidade como resposta à necessidade de afirmar a autonomia do indivíduo na era da sociedade da informação. Hoje, é evidente que o conjunto de dados pessoais desempenha um papel significativo no controle dos aspectos fundamentais da identidade de uma pessoa, funcionando como determinantes que definem a individualidade (Eler, 2016, p. 22).

É fundamental o controle individual sobre as informações pessoais na sociedade da informação. A proteção de dados é um direito fundamental significativo, que visa proteger a personalidade do indivíduo, não mais centrado na propriedade. Isso implica que a privacidade é o direito de controlar as próprias informações. Destaca-se a necessidade de o indivíduo ter poder legal para controlar as informações fornecidas, dado o aumento da dependência entre o fornecimento de informações e o uso de serviços, enquanto alerta sobre os perigos da coleta indiscriminada de dados, que pode resultar no surgimento de novas formas de poder sobre as pessoas (Eler, 2016, p. 22).

Como aponta Cancelier (2017, p. 47), a digitalização do cotidiano trouxe inúmeros benefícios, mas também tornou complexo o debate sobre privacidade. Na internet, o controle sobre nossas ações é mais desafiador, pois as ações digitais são profundas e o

seu alcance é vasto, com a viralização da informação sendo uma faceta atraente, mas perigosa. O anonimato virtual e a exposição deliberada se tornaram comuns, levando a uma evasão da privacidade. Legalmente, a proteção da privacidade concentra-se, principalmente, na invasão, negligenciando o mau uso de informações obtidas. É importante frisar que a Lei Carolina Dieckmann tipifica crimes informáticos, incluindo a invasão de dispositivos informáticos alheios.

3 FUNDAMENTOS DA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL: ALÉM DA LGPD

A partir da metade do século XX, a sociedade passou por uma série de transformações em sua estrutura, impulsionadas pelos avanços tecnológicos originados nos Estados Unidos, que agora constituem as maiores empresas de tecnologia globalmente conhecidas como *big techs* (Genso; Picoli; Luz, 2023, p. 37). Segundo Bioni (2021, p. 21), neste novo paradigma social, a informação desempenha um papel fundamental, sendo o elemento que reestrutura e reorganiza a sociedade. De acordo com Doneda (2021, p. 64), à medida que o volume de informações cresceu, ou seja, com o aprimoramento das capacidades técnicas de coletar, processar e aplicar dados, a relevância dessas informações também se elevou.

No passado, o Estado era o principal detentor e usuário das informações pessoais da população. No entanto, com avanços tecnológicos recentes, que tornaram mais fácil e acessível a coleta e o processamento de informações pessoais, as entidades privadas também passaram a aproveitar esses dados (Doneda, 2021, p. 64). O acesso a informações como os hábitos de consumo dos cidadãos permitiu ao setor empresarial aprimorar suas estratégias de mercado, segmentar produtos e serviços e melhorar a abordagem publicitária, aumentando as chances de sucesso junto ao público-alvo (Bioni, 2021, p. 21). Isso evidencia a importância dos dados pessoais dos cidadãos como um elemento importante para impulsionar a economia da informação. Além disso, a difusão da tecnologia e a ampla digitalização se tornaram ubíquas, impactando todas as esferas da vida a nível global, incluindo os aspectos sociais, econômicos e culturais, como destacado por Genso, Picoli e Luz (2023, p. 38).

O debate sobre a proteção de dados não se limita ao Brasil, e a criação de regulamentações para o tratamento de dados pessoais não é uma novidade local. No entanto, a sociedade atualmente demanda proteção legal eficaz para os indivíduos. No Brasil, a Constituição Federal (CF) de 1988 inicialmente abordava a questão da informação por intermédio de garantias como a liberdade de expressão, o direito à informação e à inviolabilidade da vida privada. Além disso, a legislação incluiu medidas específicas, como

a proibição da invasão de domicílio e a violação de correspondência, para proteger a privacidade conforme a concepção clássica (Doneda, 2021, p. 64).

O direito à privacidade é mencionado no art. 5º, inciso X, da CF/88, onde é considerado um bem que não pode ser violado. Adicionalmente, a proteção do sigilo de dados, estabelecida no art. 5º, inciso XII, da CF/88, complementa a garantia da intimidade e vida privada (Brasil, 1988). Ambas as disposições, que visam proteger a privacidade, são governadas pelo princípio da exclusividade, com o objetivo de assegurar esse direito a todos os cidadãos (Barreto Junior; Sampaio; Gallinaro, 2018, p. 35).

Para Ferraz Júnior (1993, p. 13), o que é exclusivo diz respeito às escolhas pessoais, que são influenciadas pela subjetividade do indivíduo e não estão sujeitas a normas ou padrões objetivos. Diante da esfera da privacidade, encontra-se a intimidade. A intimidade não requer exposição pública, pois não afeta os direitos de outras pessoas. No contexto da privacidade, a intimidade é o direito mais exclusivo.

Na concepção de Silva (2011, p. 18), o extenso sistema de informações digitais resulta em uma fragmentação das identidades das pessoas, expondo completamente sua individualidade. O risco aumenta à medida que o uso da tecnologia da informação possibilita a interligação de bancos de dados, que podem revelar a vida dos indivíduos sem sua autorização, e, em alguns casos, mesmo sem seu consentimento. Ressalta-se o perigo gerado pela internet, tendo em vista que a CF oferece a devida proteção a esses direitos, porém, lamentavelmente, a implementação dessas salvaguardas ainda não ocorreu de maneira eficaz.

Mendes e Branco (2014, p. 19) ressaltam a importância da privacidade na vida individual, destacando-a como essencial para a saúde mental e o desenvolvimento da personalidade. Os autores comparam a abordagem brasileira e americana, argumentando que, no contexto brasileiro, a privacidade deve ser interpretada de forma mais restritiva, embora reconheça a forte ênfase na liberdade e privacidade nos Estados Unidos. Ademais, também destacam a natureza *erga omnes* do direito à privacidade, que se aplica tanto contra o Estado quanto contra os indivíduos, com base na experiência americana de proteção contra divulgações excessivas pela imprensa. Enfatizam ainda que, embora o interesse público seja importante, a Constituição brasileira protege os direitos e liberdades individuais, com limitações apenas na interpretação consistente com o conjunto da Constituição, incluindo princípios como o direito à informação e à liberdade de imprensa.

Na busca por orientações na interpretação dos valores fundamentais, Moraes (1999, p. 25) aponta os interesses sociais protegidos pelo direito à privacidade, que se alinham com os meios de comunicação e a sociedade da informação. Essa proteção da privacidade envolve aspectos como a não interferência na vida privada, familiar e doméstica, a

preservação da integridade física e mental, bem como da liberdade intelectual e moral, e a salvaguarda da honra, reputação e intimidade, entre outros elementos.

Além disso, ao considerar os princípios constitucionais da razoabilidade e proporcionalidade, o Marco Civil da Internet levanta a questão de se os princípios, por si só, seriam suficientes. Parece haver uma tendência legislativa no Brasil de incluir direitos adicionais, mesmo que não possam ser completamente efetivados, especialmente para atender às necessidades da população, principalmente as mais vulneráveis (Barreto Junior; Sampaio; Gallinaro, 2018, p. 36).

No entanto, existe um consenso de que os direitos fundamentais constitucionalmente previstos, como o direito à vida, segurança, saúde e acesso responsável à internet, muitas vezes não são, efetivamente, implementados, criando um problema social a ser resolvido. Isso ressalta a necessidade de inovação jurídica no contexto da sociedade da informação, reconhecendo que a falta de efetividade desses direitos é um desafio a ser enfrentado no Brasil (Barreto Junior; Sampaio; Gallinaro, 2018, p. 36).

Assim sendo, o estudo da Regulamentação e Efetividade Jurídica da Sociedade da Informação assume um papel estratégico, uma vez que as novas interações sociais, interpessoais e institucionais, frequentemente ocorrendo em âmbito internacional, requerem uma reavaliação dos paradigmas, teorias e aplicação do Direito. Como uma realidade social em evolução, o Direito não pode permanecer alheio aos novos arranjos e características desse modelo de sociedade em constante transformação (Barreto Junior, 2012, p. 17).

Ainda com base no autor, ressalta-se a importância de atender às exigências legais desse novo modelo de sociedade, destacando o papel do Marco Civil da Internet como uma tentativa do legislador de exercer esse controle. Ele também destaca a falta de observância dos direitos humanos em países como o Brasil, mesmo que esses direitos sejam devidamente abordados na CF/88.

4 A LEI GERAL DE PROTEÇÃO DE DADOS

A finalidade da LGPD é dispor quanto às normas relacionadas ao tratamento de “[...] dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (Brasil, 2018, art. 1º).

A LGPD visa proteger a privacidade dos cidadãos, garantindo transações transparentes e seguras, promovendo o desenvolvimento tecnológico e a livre concorrência. Ela se aplica a todas as empresas, públicas ou privadas, que lidam com dados pesso-

ais, estabelecendo definições e papéis importantes, como o controlador, o operador e o encarregado. O conceito central é que dados pessoais são informações relacionadas a pessoas identificáveis (Carvalho, 2019, p. 31).

Ainda com base em Carvalho (2019, p. 31), além disso, a lei também introduz uma categoria de informações pessoais que requer atenção especial, conhecidas como dados pessoais sensíveis, conforme estipulado pelo art. 5º, inciso II, da LGPD:

[...] 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. (Brasil, 2018, art. 5º, II).

A lei proíbe o uso de dados pessoais sensíveis, como orientação sexual, raça, religião, opinião política, dados genéticos, biométricos e de saúde, para processamento, a menos que haja consentimento explícito do titular, ou em situações excepcionais, como para proteger a vida ou a integridade física. Além disso, a legislação reconhece a categoria de dados anonimizados, que são informações sobre o titular, que não podem ser identificadas por meios técnicos razoáveis disponíveis na época do tratamento (Carvalho, 2019, p. 31).

Para Doneda (2014, p 23), o termo “dado” se refere à sua forma mais básica e abstrata, assemelhando-se a uma informação em estado inicial, quase como uma pré-informação. Por outro lado, a “informação” em seu sentido completo engloba o que pode ser apresentado para além da representação abstrata e fragmentada encontrada nos dados, chegando ao ponto de ser compreendida cognitivamente. Isso está diretamente relacionado ao direito à privacidade, onde a equação básica é que quanto menor for a disseminação de informações, maior será o nível de privacidade.

De acordo com Carvalho (2019, p. 33), infere-se que os dados desempenham um papel significativo na aquisição de informações, uma vez que é por meio de sua interpretação que as informações são extraídas. Portanto, os dados permanecem como informações em potencial, até que alguém compreenda a mensagem que eles contêm e que está sendo transmitida. Portanto, a intenção da LGPD vai além de apenas distinguir os tipos de dados, pois ela também busca estabelecer limites para como esses dados podem ser tratados. Nesse sentido, o art. 5 evidencia:

(...) tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamen-

to, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, 19 modificação, comunicação, transferência, difusão ou extração. (Brasil, 2018, art. 5º, X).

A LGPD atribui ao controlador um papel fundamental, exigindo a elaboração do Relatório de Impacto à Privacidade (RIPD), para analisar a gravidade e a extensão do tratamento de dados pessoais. A empresa também deve comunicar, imediatamente, o titular em caso de interferências graves em seus dados, alinhando-se ao princípio da prevenção para reduzir riscos. Os princípios estabelecidos no art. 6º da referida lei, juntamente com a boa-fé, funcionam como medidas de segurança para proteger os dados. Para assegurar o cumprimento dos princípios e das regras da lei, foi criada a Autoridade Nacional de Proteção de Dados (ANPD), por meio da Lei n. 13.853, de 8 de julho de 2019 (Brasil, 2019), aprovada pelo Congresso Nacional (Carvalho, 2019, p. 34).

A autora reforça que a ANPD tem como atribuições zelar pela proteção dos dados pessoais, conforme a legislação elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e Privacidade, bem como fiscalizar e impor sanções em casos de tratamento inadequado de dados, ou seja, em desacordo com a LGPD. Esta autoridade terá uma natureza transitória, podendo ser transformada em uma entidade da administração pública federal indireta, com regime autárquico especial vinculado à Presidência da República, após um período de dois anos, conforme estabelecido no art. 55-A, §§ 1º e 2º, da Lei n. 13.709/2018 (Brasil, 2018).

Ressalta-se, ainda, que a ANPD seguirá uma estrutura organizacional delineada pelo art. 55-C da Lei, incluindo Conselho Diretor, Conselho Nacional de Proteção de Dados, Corregedoria, Ouvidoria, assessoria jurídica própria e unidades administrativas necessárias. Conforme a LGPD, o *Data Protection Officer* (DPO) é responsável por planejar e implementar medidas de proteção de dados, servindo como ponto de comunicação entre o controlador, os titulares de dados e a ANPD, podendo ser uma pessoa física ou jurídica, com ênfase no conhecimento avançado em proteção de dados. Ademais, o DPO também assume o papel de receber comunicações da ANPD e interagir com os titulares de dados, para esclarecer questões e resolver problemas, conforme estabelecido no art. 41, incisos, da Lei n. 13.709/2018 (Carvalho, 2019, p. 38).

5 MEDIDAS LEGAIS PAUTADAS NA LGPD PARA A PRESERVAÇÃO DA PRIVACIDADE

As pessoas podem ser identificadas por meio de informações pessoais, que desempenham o papel de criar uma identidade única para cada indivíduo. Atualmente, devido ao

avanço das Tecnologias de Informação e Comunicação (TICs), e à ampla utilização de plataformas online para comunicação e obtenção de informações, é comum que dados pessoais sejam fornecidos ao realizar cadastros, compras pela internet e acordos contratuais. No entanto, é importante observar determinados requisitos ao coletar e tratar esses dados pessoais por parte das entidades solicitantes (Genso; Picoli; Luz, 2023, p. 35).

Os autores reforçam que a LGPD tem como finalidade estabelecer um ambiente de segurança jurídica em todo o país nesse assunto. Entretanto, para alcançar esse objetivo, é importante que haja uma fiscalização rigorosa sobre como os responsáveis pelo tratamento de dados estão implementando as medidas de conformidade. Isso implica que a aplicação das regras legais deve ser respaldada por meios coercitivos, que são fundamentais para o correto funcionamento da legislação. Portanto, a legislação inclui disposições que estabelecem sanções e medidas punitivas para aqueles que não a cumprirem.

O Capítulo VIII, da Lei nº 13.709/2018, trata da fiscalização e, a partir do art. 52, apresenta as possíveis sanções para aqueles que violarem a LGPD. É fundamental compreender a quem se aplicam essas sanções, quem as impõe e os critérios para sua aplicação. Em termos gerais, de acordo com o art. 3º, da LGPD, as normas são aplicáveis a todos que realizam o tratamento de dados pessoais, sejam pessoas físicas ou jurídicas, de organizações públicas ou privadas. No entanto, a lei estabelece exceções, como quando o tratamento é realizado, por exemplo, por uma pessoa física para fins estritamente pessoais e não econômicos, para fins exclusivamente jornalísticos e artísticos, ou para tratamentos relacionados à segurança pública e defesa nacional, conforme estipulado no art. 4º, I, II, III e IV, entre outros. Nessas situações excepcionais, não há imposição de sanções nem medidas coercitivas.

Em relação à aplicação das sanções e medidas de coerção, estas se destinam aos agentes de tratamento, conforme estabelecido no art. 52, da LGPD. A própria lei define esses agentes como o controlador e o operador, ambos descritos no art. 5º, incisos VI e VII, respectivamente, da LGPD. Para Genso, Picoli e Luz (2023, p. 38), embora a distinção entre o controlador e o operador seja fundamental com base no critério da autonomia, ainda existem incertezas em relação à classificação dos responsáveis pelo tratamento de dados dentro dessas categorias.

Conforme a LGPD, sobre a entidade encarregada de impor sanções administrativas e medidas coercitivas, essas serão aplicadas por uma autarquia de natureza especial, a ANPD, que possui autonomia técnica e poder decisório, conforme estabelecido no art. 52, parágrafo inicial, da mencionada Lei. A ANPD tem sua própria regulamentação, como especificado a partir do art. 55, da mesma lei.

A LGPD estabelece sanções de forma exaustiva, conforme apontado por Oliveira (2021, p. 18), o que limita a Autoridade de Proteção de Dados a aplicar penalidades

diferentes das previstas na lei. Nesse sentido, as sanções incluem advertência, multa simples de até 2% do faturamento anual da empresa, limitada a 50 milhões de reais, multa diária nos mesmos moldes, publicização da infração, bloqueio e eliminação dos dados pessoais relacionados à infração, suspensão parcial do funcionamento do banco de dados, suspensão da atividade de tratamento de dados pessoais, e proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados (Brasil, 2018).

Conforme Oliveira (2021, p. 32) e com base na relação acima, fica evidente que existem sanções de natureza financeira, medidas restritivas de atividades e advertências. A ANPD tem a responsabilidade de aplicar a sanção mais apropriada para cada situação específica, visando assegurar a proteção dos direitos fundamentais. Nota-se, portanto, a presença de sanções destinadas a incentivar o cumprimento das regras estabelecidas, bem como aquelas que têm o propósito de repreender o infrator, desempenhando um papel educativo.

6 FORMAS DE PROTEÇÃO DOS DADOS PESSOAIS

Consideradas como instrumentos para salvaguardar dados pessoais, as *Privacy Enhancing Technologies* (PETs) representam tecnologias cujo objetivo é fortalecer e/ou aprimorar a privacidade dos usuários. Entre essas tecnologias, encontra-se o *Privacy by Design* (PbD) (Bioni, 2021, p. 64).

Como destaca Bioni (2021, p. 64), o PbD foi desenvolvido nos anos 90 pela Comissão de Informação e Privacidade de Ontário, Canadá, a Dra. Ann Cavoukian. Essa é uma metodologia que prioriza a proteção de dados pessoais como ponto central durante o desenvolvimento de produtos ou serviços, com a ideia fundamental de que esses produtos ou serviços devem ser integrados com tecnologias que simplifiquem a gestão e a segurança das informações pessoais. Sobre o assunto, Simonette (2021, p. 1) afirma que:

Na prática, as iniciativas das empresas devem garantir que a privacidade e a proteção de dados sejam consideradas desde a idealização de qualquer iniciativa que envolva dados pessoais, seja por iniciativa da área de TI ou de qualquer outra área da empresa. Projetos internos, desenvolvimento de produtos, desenvolvimento de software e sistemas de TI são alguns exemplos de iniciativas de empresas.

Simonette (2021, p. 1) reforça que a aplicação da abordagem PbD evidencia os benefícios recíprocos tanto para as empresas quanto para os titulares de dados, pois, além

de proporcionar maior segurança e privacidade dos dados por parte das empresas, os titulares obtêm a capacidade de gerenciar seus próprios dados, determinando quais serão compartilhados e quais não, enquanto também compreendem a necessidade e o propósito da coleta dessas informações.

Com o propósito de orientar a aplicação do PbD em tecnologias específicas, operações empresariais, arquiteturas físicas e infraestruturas de rede, Ann Cavoukian desenvolveu sete princípios de gestão de informações conhecidos como os Princípios Fundamentais do *Privacy by Design*. São eles: adoção de abordagem pró-ativa em vez de reativa, foco na prevenção em vez de correção, implementação da privacidade como configuração padrão, incorporação da privacidade desde a concepção, busca da funcionalidade completa com impacto positivo, em vez de impacto nulo, garantia de segurança abrangente em todo o ciclo de vida e manutenção do enfoque centrado no usuário com visibilidade e transparência (Genso; Picoli; Luz, 2023, p. 48).

O princípio da abordagem proativa prioriza a prevenção em vez de reação, antecipando e solucionando potenciais problemas de privacidade antes que surjam, enfatizando a gestão de riscos em vez de uma abordagem de gerenciamento de crise. O princípio da privacidade por padrão estabelece a adoção da privacidade como o padrão em todos os sistemas e operações da empresa, garantindo que a proteção de dados seja incorporada de forma automática, sem exigir ação adicional por parte do titular dos dados. Já o princípio da privacidade incorporada ao *design* destaca a necessidade de integrar a privacidade desde a fase inicial do desenvolvimento de produtos ou serviços, tornando-a uma parte intrínseca do projeto (Genso; Picoli; Luz, 2023, p. 48).

O princípio da funcionalidade completa com ganhos mútuos propõe um equilíbrio entre os interesses das empresas e dos titulares de dados, harmonizando objetivos legítimos e garantindo que ambas as partes se beneficiem. O da segurança de ponta a ponta coloca a segurança como elemento orientador em todas as etapas do ciclo de vida dos dados, desde a coleta até a exclusão, bem como em situações de compartilhamento de dados. O princípio da visibilidade e transparência garante que todos os envolvidos tenham acesso a informações claras sobre como os dados estão sendo tratados, permitindo a verificação independente pelos titulares. Por fim, o princípio do respeito pela privacidade do usuário prioriza os interesses individuais em relação à privacidade, oferecendo medidas que beneficiem os titulares de dados, respeitando suas preferências e direitos (Genso; Picoli; Luz, 2023, p. 49).

Apesar de a LGPD não abordar, explicitamente, os princípios mencionados do *Privacy by Design*, as empresas têm a liberdade de aplicar os conceitos da Privacidade por *Design* e Privacidade por Padrão, para assegurar a máxima segurança dos dados de seus clientes. Isso contribui para fortalecer o compromisso com a proteção de dados

personais, mesmo que esses princípios não estejam detalhados na legislação, promovendo assim a efetiva segurança das informações dos indivíduos (Simonette, 2021, p. 33).

Para Venosa (2013, p. 47):

Deve haver sempre posição firme do jurista no sentido de defender a preservação da intimidade, tantos são os ataques que modernamente. Não se pode permitir que a tecnologia, os meios de comunicação e a própria atividade do Estado invadam um dos bens mais valiosos do ser humano, que é seu direito à intimidade, seu direito de estar só ou somente na companhia dos que lhe são próximos e caros. As fotografias e imagens obtidas à socapa, de pessoas no recôndito de seu lar, em atividades especialmente privadas, são exemplos claros dessa invasão de privacidade, que deve ser coibida e pode gerar direito à indenização. Os fatos comezinhos da vida privada de cada um não devem interessar a terceiros. Tanto mais será danosa a atividade quanto mais renomada e conhecida socialmente for a vítima, mas todos, independentemente de seu nível de projeção social ou cultural, gozam da proteção.

Como destacam Freitas, Saikali e Reis (2022, p. 54), a criação da ANPD enfrenta o desafio de regular diferentes setores econômicos e promover uma abordagem de regulação baseada na arquitetura, focando na forma como o código de software relacionado ao tratamento de dados pessoais é desenvolvido. Isso resulta na aplicação dos princípios já estabelecidos na LGPD, como medidas de proteção de dados desde a concepção até a execução de produtos e serviços, reduzindo riscos relacionados à privacidade e tecnologia. Assim, a ANPD busca incentivar o modelo PbD, que incorpora princípios de segurança e privacidade desde o início do desenvolvimento de produtos e serviços que envolvem dados pessoais, tornando-os mais seguros e acessíveis. Além disso, a ANPD visa estimular a adoção de padrões que facilitem o controle dos titulares sobre seus dados pessoais, promovendo uma abordagem proativa para proteger a privacidade e mitigar riscos sob a LGPD.

Dessa forma, Freitas, Saikali e Reis (2022, p. 54) afirmam que *Privacy by Design* é a concepção de sistemas de informação que, desde o código-fonte, incorporam as tecnologias necessárias para proteger os dados pessoais e a privacidade do usuário. Isso envolve a definição de padrões rigorosos para a coleta de dados, seguindo o princípio do mínimo necessário. De acordo com Lemos e Branco (2021, p. 42), o conjunto de normas estabelecidas durante a criação do software ou produto, com foco na segurança de dados, pode ser chamado de *Privacy by Design*.

Os autores destacam outra prática fundamental, além de incorporar princípios de proteção de dados durante o desenvolvimento de sistemas. Trata-se da adoção do *Privacy by Default*. Esse modelo requer que organizações, em seus processos, produtos e serviços, considerem sempre uma configuração, que ofereça a máxima proteção aos titulares de dados, tanto em relação à quantidade de dados coletados quanto ao período de armazenamento. Portanto, é essencial determinar a quantidade mínima de dados necessária para alcançar a finalidade do tratamento, estabelecendo, como padrão, a configuração menos invasiva para o titular. Nesse sentido, a LGPD orienta a ANPD a promover a eficácia da legislação não apenas por meio de normas, mas também pela adoção de padrões de mercado que regulamentem o tratamento de dados pessoais em âmbitos público e privado.

Conforme reforçam Lemos e Branco (2021, p. 43), é responsabilidade da ANPD promover e incentivar o mercado a adotar padrões, já que a LGPD não detalha explicitamente quais medidas técnicas devem ser implementadas.

7 MARCO NORMATIVO DA LGPD

A LGPD brasileira, sancionada em 2018, e em vigor desde setembro de 2020, representa um marco significativo na proteção dos dados pessoais no Brasil. Sua estrutura e princípios foram fortemente influenciados pelo Regulamento Geral sobre a Proteção de Dados (GDPR, na sigla em inglês) da União Europeia, que entrou em vigor em maio de 2018. A inspiração nas normativas europeias é evidente em diversos aspectos da LGPD, tanto em seus fundamentos quanto em suas práticas regulatórias (Lemos; Branco, 2021, p. 49).

A proteção de dados, na Europa, começou a ganhar forma na década de 1970, quando alguns países começaram a reconhecer a importância de regulamentar o uso de dados pessoais. A primeira legislação de proteção de dados surgiu na Alemanha, em 1970, com a Lei de Proteção de Dados do Estado de Hessen. Posteriormente, em 1981, o Conselho da Europa adotou a Convenção 108, que estabeleceu princípios para a proteção das pessoas em relação ao processamento automatizado de dados pessoais. Estes desenvolvimentos iniciais criaram a base para um esforço europeu mais coordenado na proteção de dados pessoais, culminando na Diretiva 95/46/CE da União Europeia, em 1995. A diretiva estabelecia um quadro comum para a proteção de dados em todos os Estados-Membros da UE, mas permitia variações nacionais significativas, o que resultava em diferentes níveis de proteção e complexidade para as empresas que operavam em vários países da União (Lemos; Branco, 2021, p. 51).

Os referidos autores apontam que a necessidade de harmonização e atualização das

normas de proteção de dados levou à criação do GDPR, aprovado em 2016, e efetivamente aplicado a partir de maio de 2018. O GDPR estabeleceu-se como a legislação mais abrangente e rigorosa sobre proteção de dados no mundo. Ele se baseia em princípios fundamentais como transparência, segurança e direitos dos titulares dos dados.

Os principais pontos do GDPR incluem: consentimento, os dados pessoais só podem ser processados com o consentimento claro e explícito do titular dos dados; transparência, as organizações devem informar aos titulares dos dados como seus dados serão utilizados; direitos dos titulares, incluem o direito ao acesso, retificação, apagamento (direito ao esquecimento), restrição de processamento, portabilidade dos dados e objeção; segurança, implementação de medidas técnicas e organizacionais adequadas para proteger os dados pessoais; e responsabilidade e conformidade, as organizações devem demonstrar conformidade com o GDPR e são responsabilizadas por violações (Noain-Sánchez, 2016, p. 24).

Ainda segundo o autor, a LGPD segue uma estrutura similar, adotando princípios e direitos inspirados diretamente pelo GDPR. Entre os fundamentos da LGPD, destacam-se: consentimento, onde o tratamento de dados pessoais requer o consentimento explícito do titular, com exceções específicas claramente definidas; transparência, onde as organizações devem ser transparentes sobre o uso dos dados pessoais; direitos dos titulares, que garantem direitos como acesso, correção, exclusão, portabilidade dos dados e objeção ao tratamento; segurança, estabelecendo a necessidade de medidas técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados; e responsabilização e prestação de contas, onde as empresas devem demonstrar conformidade e são responsabilizadas por incidentes de segurança e violações.

A LGPD não é uma cópia direta do GDPR, mas sim uma adaptação aos contextos jurídico, cultural e econômico do Brasil. No entanto, a influência do GDPR é clara em vários aspectos: estrutura legal, onde ambos os regulamentos possuem uma estrutura robusta que define direitos, responsabilidades e princípios que devem ser seguidos pelas organizações que tratam dados pessoais; amplitude, aplicando-se a todas as organizações que processam dados pessoais, independentemente do tamanho ou do setor; e sanções, onde as penalidades por não conformidade são severas em ambas as leis, com a LGPD prevendo multas significativas, similarmente às do GDPR (Noain-Sánchez, 2016, p. 27).

A adoção de princípios semelhantes ao GDPR pela LGPD reflete um movimento global em direção à harmonização das normas de proteção de dados. Isso é importante num mundo cada vez mais globalizado, onde dados pessoais frequentemente atravessam fronteiras internacionais. A compatibilidade entre as leis facilita o comércio internacional e a cooperação entre empresas e governos em matéria de proteção de dados (Marrafon; Coutinho, 2020, p. 33).

A implementação da LGPD, como a do GDPR, apresenta desafios significativos para as organizações. Estas precisam ajustar suas práticas, políticas e sistemas para garantir conformidade. No Brasil, isso implicou na criação da ANPD, responsável pela fiscalização e regulamentação da LGPD, similarmente à função do European Data Protection Board (EDPB) na Europa (Machado, 2014, p. 61).

A LGPD brasileira é um reflexo do avanço global na proteção de dados pessoais, fortemente inspirada pelo GDPR europeu. Essa inspiração não apenas ajudou a moldar uma legislação robusta e moderna, mas também alinhou o Brasil às melhores práticas internacionais em proteção de dados, facilitando a integração do país na economia digital global. Ao adotar e adaptar os princípios do GDPR, a LGPD fortaleceu a defesa dos direitos dos titulares de dados no Brasil, promovendo maior transparência, segurança e responsabilidade no tratamento dos dados pessoais (Machado, 2014, p. 61).

8 ESTUDOS ANTERIORES

O estudo realizado por Willis (2014, p. 24) destacou que experiências anteriores com inadimplências indicam problemas de rigidez no *Track-Me* e excessiva flexibilidade no *Do-Not-Track*, questionando sua eficácia. Isso impacta as políticas “*Do-Not-Track*” em discussão nos Estados Unidos, União Europeia e *World Wide Web Consortium*, além de levantar dúvidas sobre estratégias comportamentais, para aprimorar a privacidade do consumidor.

O estudo desenvolvido por Noain-Sánchez (2016, p. 37) apontou a importância de unir a configuração padrão de privacidade com a obtenção de consentimento esclarecido como medidas conjuntas para proteger a privacidade dos usuários de TIC. Além disso, foi desenvolvida uma abordagem adequada para administrar esse “consentimento informado” com os usuários.

Com base na pesquisa desenvolvida por Carvalho (2019, p. 29), a demanda por uma regulamentação precisa no manejo de dados pessoais conduziu à promulgação de uma lei específica que trouxe alterações significativas no cenário online. Inspirada em princípios do GDPR europeu e na filosofia de “privacidade por *design*”, os acordos digitais serão agora supervisionados por recém-introduzidos profissionais denominados agentes de tratamento, sob a supervisão de autoridades legais, potencialmente moldando uma nova dinâmica no mercado virtual.

Tomando-se como base o estudo realizado por Marrafon e Coutinho (2020, p. 35), ficou evidente que a aplicação do princípio “*privacidade desde o início*” é fundamental para concretizar de maneira prática tanto o direito à proteção de dados quanto o direito fundamental à privacidade.

A pesquisa realizada por Freitas, Saikali e Reis (2022, p. 30) realçou o impacto da

Sociedade da Informação diante da proteção de dados, examinou os princípios subjacentes à intervenção estatal na economia do Brasil, e recomendou a adoção do modelo regulatório baseado na arquitetura como uma alternativa eficaz para o papel desempenhado pela ANPD.

O estudo de Genso, Picoli e Luz (2023, p. 38) apontou que a integração do conceito “privacidade desde o início” com as leis pertinentes pode promover a eficácia da cultura de proteção de dados.

A discussão baseada nos estudos mencionados revela a crescente importância da proteção de dados e da privacidade na era digital. Cada pesquisa aborda aspectos distintos relacionados a essas questões e oferece informações importantes para a compreensão das complexidades envolvidas na proteção dos dados dos usuários de TICs.

Primeiramente, os estudos de Willis (2014, p. 24) e Noain-Sánchez (2016, p. 37) chamam a atenção para a necessidade de equilibrar a rigidez e a flexibilidade nas políticas de proteção de dados. Isso destaca a importância de encontrar um ponto de equilíbrio que respeite os direitos dos indivíduos sem sufocar a inovação e o desenvolvimento tecnológico. Além disso, a ênfase em obter consentimento informado e em configurar padrões de privacidade pode ser uma abordagem eficaz para proteger a privacidade dos usuários.

Por outro lado, o estudo de Carvalho (2019, p. 29) destacou a evolução das regulamentações relacionadas à proteção de dados, especialmente no contexto da União Europeia com o GDPR. Isso ilustra como a legislação está se adaptando às demandas da era digital e como a privacidade está se tornando um aspecto cada vez mais importante nas políticas governamentais e na regulamentação.

Já a pesquisa de Marrafon e Coutinho (2020, p. 35) enfatizou a importância do princípio “privacidade desde o início” como uma abordagem proativa para a proteção de dados o que implica que a privacidade deve ser considerada desde a concepção de produtos e serviços, em vez de ser uma reflexão tardia. Isso pode ser fundamental para garantir que a privacidade seja efetivamente incorporada às soluções tecnológicas.

No estudo de Freitas, Saikali e Reis (2022, p. 30) destacada a interseção entre a proteção de dados e a economia, ressaltando como a regulamentação pode influenciar o mercado virtual. A introdução de agentes de tratamento e a supervisão legal sugerem uma mudança significativa na forma como as empresas abordam a proteção de dados.

O estudo de Genso, Picoli e Luz (2023, p. 38) abordou a ideia de que a integração de práticas de “privacidade desde o início” com a legislação pode ser fundamental para uma cultura eficaz de proteção de dados.

De forma geral, esses estudos evidenciaram que a proteção de dados e a privacidade não são apenas preocupações teóricas, mas questões práticas e em constante evolução

que afetam a regulamentação, a economia e a cultura das empresas. A abordagem multidisciplinar e a cooperação entre diferentes partes interessadas, incluindo governos, empresas e sociedade civil, são essenciais para lidar com esses desafios de maneira eficaz e responsável.

9 CONCLUSÕES

O desenvolvimento desta pesquisa teve como objetivo discorrer a atuação do direito na privacidade de dados. Para fundamentar a temática abordada, foi realizada uma revisão de literatura onde foram apontadas as concepções dos autores acerca do assunto para o alcance do objetivo proposto.

A partir dos resultados apurados foi possível concluir que:

1. Os estudos mencionados destacam a crescente importância da proteção de dados e da privacidade na era digital, ressaltando a necessidade de equilibrar rigidez e flexibilidade nas políticas de proteção de dados para promover inovação e respeitar os direitos individuais;
2. A evolução das regulamentações, exemplificada pelo GDPR na União Europeia, demonstra como a legislação está se adaptando às demandas da era digital, tornando a privacidade um aspecto central nas políticas governamentais e regulamentações;
3. O princípio “privacidade desde o início” emerge como uma abordagem proativa fundamental para a proteção de dados, enfatizando a importância de incorporar a privacidade desde a concepção de produtos e serviços;
4. A interseção entre a proteção de dados e a economia, conforme destacado em um dos estudos, revela como a regulamentação pode influenciar o mercado virtual, introduzindo agentes de tratamento e supervisão legal;
5. A integração de práticas de “privacidade desde o início” com a legislação é fundamental para criar uma cultura eficaz de proteção de dados.

A LGPD brasileira é um reflexo do avanço global na proteção de dados pessoais, fortemente inspirada pelo GDPR europeu. Essa inspiração não apenas ajudou a moldar uma legislação robusta e moderna, mas também alinhou o Brasil às melhores práticas internacionais em proteção de dados, facilitando a integração do país na economia digi-

tal global. Ao adotar e adaptar os princípios do GDPR, a LGPD fortaleceu a defesa dos direitos dos titulares de dados no Brasil, promovendo maior transparência, segurança e responsabilidade no tratamento dos dados pessoais.

De maneira geral, os estudos ressaltam que a proteção de dados e a privacidade não são apenas questões teóricas, mas preocupações práticas que impactam regulamentações, economias e culturas empresariais. Abordar esses desafios requer uma abordagem multidisciplinar e a colaboração entre governos, empresas e sociedade civil, para garantir uma proteção de dados eficaz e responsável na era digital em constante evolução.

THE ACT OF THE LAW IN PRIVACY AND PROTECTION OF PERSONAL DATA

ABSTRACT

The increased dissemination of information has opened doors for numerous individuals to access a variety of digital services. To safeguard the right to privacy and data protection, there arose the need to regulate this issue through legislation and the establishment of regulatory authorities. The objective was to discuss the role of law in privacy and protection of personal data. This constitutes a literature review, focusing on the past 10 years. It was concluded that data protection and the preservation of privacy are not merely theoretical concepts, but also practical issues that impact the development of regulations, the functioning of economies, and corporate culture.

Keywords: personal data; law; digital age; general data protection law; privacy.

REFERÊNCIAS

BARRETO JUNIOR, I. F. Dignidade da pessoa humana na sociedade da informação. *In: SIMÃO FILHO, A. et al. (org.). Direito da sociedade da informação: temas jurídicos relevantes.* São Paulo: Quartier Latin, 2012. p. 457-470.

BARRETO JUNIOR, I. F.; SAMPAIO, V. G. R.; GALLINARO, F. Marco Civil da Internet e o direito à privacidade na sociedade da informação. **Direito, Estado e Sociedade**, [Rio de Janeiro], n. 52, p. 114-133, jan./jun. 2018. DOI: <https://doi.org/10.17808/des.52.835>. Disponível em: <https://revistades.jur.puc-rio.br/index.php/revistades/article/view/835>. Acesso em: 26 jan. 2024.

BIONI, B. R. **Proteção de dados pessoais:** a função e os limites do consentimento. São Paulo: Forense, 2021.

BRASIL. [Constituição(1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2023]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm. Acesso em: 26 jan. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2022]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 26 jan. 2024.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: Presidência da República, [2022]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/113853.htm. Acesso em: 26 jan. 2024.

CANCELIER, M. V. L. O direito à privacidade hoje: perspectiva histórica e o cenário brasileiro. **Seqüência**, Florianópolis, v. 38, n. 76, p. 213-240, ago. 2017. DOI: <https://doi.org/10.5007/2177-7055.2017v38n76p213>. Disponível em: <https://periodicos.ufsc.br/index.php/sequencia/article/view/2177-7055.2017v38n76p213>. Acesso em: 26 jan. 2024.

CARVALHO, T. A. **Aplicabilidade da lei geral de proteção de dados e da metodologia “privacy by design” nos termos de uso e de política de privacidade**. 2019. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Faculdade de Direito de Vitória, Vitória, ES. 2019. Disponível em: <http://repositorio.fdv.br:8080/handle/fdv/781>. Acesso em: 26 jan. 2024.

DONEDA, D. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 3. ed. São Paulo: Revista dos Tribunais, 2021.

DONEDA, D. O direito fundamental à proteção de dados pessoais. In: MARTINS, G. G. (coord.). **Direito privado e internet**: atualizado pela Lei nº 12.965/2014: Marco Civil da Internet no Brasil. São Paulo: Atlas, 2014. p. 61-78.

ELER, K. C. G. A new understanding of privacy: from the right to be alone to the informative self-determination. **Techno Review. International Technology, Science and Society Review**, [Kwun Tong, Kowloon], v. 5, n. 2, p. 185-196, 26 Oct. 2016. DOI: <https://doi.org/10.37467/gka-revtechno.v5.1351>. Disponível em: <https://journals.eagora.org/revTECHNO/article/view/1351>. Acesso em: 26 jan. 2024.

FERRAZJÚNIOR, T. S. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito [da] Universidade de São Paulo**, São Paulo, v. 88, p. 439-459, 1º jan. 1993. Disponível em: <https://www.revistas.usp.br/rfdusp/article/view/67231>. Acesso em: 26 jan. 2024.

FREITAS, C. O. A.; SAIKALI, L. B.; REIS, R. A. O. Adoção do modelo de regu-

lação pela arquitetura de código e práticas de *privacy by design* e *by default* para o ambiente regulatório de proteção de dados pessoais no Brasil. **Direitos Fundamentais & Justiça**, Belo Horizonte, ano 16, n. 46, p. 363-385, jan./jun. 2022. DOI: <https://doi.org/10.30899/dfj.v16i46.1118>. Disponível em: <https://dfj.emnuvens.com.br/dfj/article/view/1118/1080>. Acesso em: 26 jan. 2024.

GENSO, M. G.; PICOLI, G. R. N.; LUZ, P. H. M. *Privacy by design* como possível medida de efetivação da proteção dos dados pessoais no século XXI. **Revista Contemporânea**, São José dos Pinhais, v. 3, n. 8, p. 11506-11533, 11 ago. 2023. DOI: <https://doi.org/10.56083/RCV3N8-086>. Disponível em: <https://ojs.revistacontemporanea.com/ojs/index.php/home/article/view/1415>. Acesso em: 26 jan. 2024.

LEMONS, R.; BRANCO, S. *Privacy by design*: conceito, fundamentos e aplicabilidade na LGPD. In: MENDES, L. S. *et al.* (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 449-460.

MACHADO, J. M. S. A expansão do conceito de privacidade e a evolução na tecnologia de informação com o surgimento dos bancos de dados. **Revista da AJURIS**, [Porto Alegre], v. 41, n. 134, p. 337-363, jun. 2014. Disponível em: <https://revistadaajuris.ajuris.org.br/index.php/REVAJURIS/article/view/206>. Acesso em: 26 jan. 2024.

MARRAFON, M. A.; COUTINHO, L. L. C. L. Princípio da privacidade por design: fundamentos e efetividade regulatória na garantia do direito à proteção de dados. **Revista Eletrônica Direito e Política**, Itajaí, v. 15, n. 3, p. 955-984, set./dez. 2020. DOI: <https://doi.org/10.14210/rdp.v15n3.p955-984>. Disponível em: <https://periodicos.univali.br/index.php/rdp/article/view/17119>. Acesso em: 26 jan. 2024.

MENDES, G. F.; BRANCO, P. G. G. **Curso de direito constitucional**. 9. ed. São Paulo: Saraiva, 2014.

MORAES, A. **Direito constitucional**. 6. ed. São Paulo: Atlas, 1999.

NOAIN-SÁNCHEZ, A. “Privacy by default” and active “informed consent” by layers: Essential measures to protect ICT users’ privacy. **Journal of Information, Communication and Ethics in Society**, [Bradford, UK], v. 14, n. 2, p. 124-138, 2016. DOI: <https://doi.org/10.1108/JICES-10-2014-0040>. Disponível em: <https://www.emerald.com/insight/content/doi/10.1108/JICES-10-2014-0040/>. Acesso em: 26 jan. 2024.

OLIVEIRA, R. **LGPD**: como evitar as sanções administrativas. São Paulo: Expressa, 2021.

SILVA, J. A. **Curso de direito constitucional positivo**. 34. ed. São Paulo: Malheiros, 2011.

SIMONETTE, M. *Privacy by design* e *privacy by default*. **Boletim do CEST**, São Paulo, v. 6, n. 6, p. 1-2, ago. 2021. Disponível em: http://www.cest.poli.usp.br/wp-content/uploads/2021/08/Privacy-By-Design-e-Default_pt_final.pdf. Acesso em: 26 jan. 2024.

VENOSA, S. S. **Código Civil interpretado**. 3. ed. São Paulo: Atlas, 2013.

WILLIS, L. E. Why not privacy by default? **Berkeley Technology Law Journal**, [Berkeley, CA], v. 29, p. 61-134, May 2014. DOI: <https://doi.org/10.15779/Z38X40V>. Disponível em: <https://lawcat.berkeley.edu/record/1126202>. Acesso em: 26 jan. 2024.