UNIVERSIDADE DO VALE DO RIO DOS SINOS (UNISINOS)
UNIDADE ACADÊMICA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
NÍVEL MESTRADO

LUCIANA ALMEIDA NOBRE SAMPAIO

A PROTEÇÃO DOS DADOS PESSOAIS SOB UMA PERSPECTIVA PENAL:
Responsabilidade dos agentes de tratamento pela omissão imprópria

São Leopoldo/RS
2024

LUCIANA ALMEIDA NOBRE SAMPAIO

A PROTEÇÃO DOS DADOS PESSOAIS SOB UMA PERSPECTIVA PENAL:

Responsabilidade dos agentes de tratamento pela omissão imprópria

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

Orientadora: Prof.ª Dra. Têmis Limberger

Coorientador: Prof. Dr. Miguel Tedesco Wedy

São Leopoldo/RS

2024

S192p Sampaio, Luciana Almeida Nobre
A proteção dos dados pessoais sob uma perspectiva penal: responsabilidade dos agentes de tratamento pela omissão imprópria. / Luciana Almeida Nobre Sampaio -- 2024.
124 f. ; 30cm.

Dissertação (Mestrado em Direito) -- Universidade do Vale do Rio dos Sinos, Programa de Pós-Graduação em Direito, 2024.

Orientadora: Prof.ª Dra. Têmis Limberger; Coorientador: Prof. Dr. Miguel Tedesco Wedy.

1. Direito penal. 2. Proteção de dados. 3. Direito à privacidade. 4. Responsabilidade. 5. Omissão. I. Título. II. Limberger, Têmis. II. Wedy, Miguel Tedesco.

CDU 343.2

Catalogação na Publicação: Bibliotecária Eliete Mari Doncato Brasil - CRB 10/1184

UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS
UNIDADE ACADÊMICA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO – PPGD
NÍVEL MESTRADO

A dissertação intitulada: "**A PROTEÇÃO DOS DADOS PESSOAIS SOB UMA PERSPECTIVA PENAL: RESPONSABILIDADE DOS AGENTES DE TRATAMENTO PELA OMISSÃO IMPRÓPRIA."**, elaborada pela mestranda **Luciana Almeida Nobre Sampaio,** foi julgada adequada e aprovada por todos os membros da Banca Examinadora para a obtenção do título de MESTRA EM DIREITO.

São Leopoldo, 29 de novembro de 2024.

Prof. Dr. **Anderson Vichinkeski Teixeira,**
Coordenador do Programa de Pós-Graduação em Direito.

Apresentada à Banca integrada pelos seguintes professores:

Participação por Webconferência
Presidente: Dra. Têmis Limberger_____ _____

Participação por Webconferência
Coorientador: Dr. Miguel Tedesco Wedy_____ _____

Participação por Webconferência
Membro externo: Dr. Felipe Augusto Forte de Negreiros Deodato_ _____

Participação por Webconferência
Membro: Dra. Luciane Klein Vieira_____

Primeiramente, dedico este trabalho à minha família, em especial meu esposo e filhas, que me apoiaram incondicionalmente neste período. Aos meus pais, que sempre me motivaram na busca pelo aperfeiçoamento acadêmico.

AGRADECIMENTOS

A caminhada na construção deste trabalho foi acompanhada por desafios de diversas naturezas, mas que foram superados graças ao suporte que tive ao longo desses anos.

Agradeço a Deus, por permitir realizar esse mestrado que foi almejado por tantos anos. Não poderia deixar de agradecer ao meu esposo, que sempre prestou o suporte indispensável, principalmente com as nossas filhas para que eu pudesse me dedicar à pesquisa. Às minhas filhas Maria Elisa, Cecília e Clarice, que representam a energia que me moveu nos momentos mais difíceis desse percurso.

Aos meus pais, que além de sempre me incentivarem sobre a importância da busca pelo conhecimento, fizeram e ainda fazem parte da rede de apoio que me permitiu alcançar esse objetivo.

Por fim, agradeço à minha orientadora, Dra. Têmis Limberguer e ao meu co-orientador Dr. Miguel Tedesco Wedy, pelos conselhos valiosos e pela compreensão quanto aos obstáculos superados.

RESUMO

A sociedade moderna encontra-se imersa em recursos tecnológicos que pareciam antes inimagináveis. As facilidades trazidas pelas tecnologias da informação e comunicação otimizam tempo, bem como propiciam qualidade de vida à sociedade. Contudo, esta nova realidade não está isenta de riscos e vulnerabilidades decorrentes da alta exposição pelo uso de ferramentas cibernéticas, principalmente em razão da disponibilização de dados pessoais dos seus usuários. Por isso, a proteção dessas informações tem recebido cada vez mais atenção por parte das organizações públicas e privadas a fim de promoverem a sua adequada gestão. A legislação também acompanhou esse movimento com a criação de dispositivos de proteção desses dados. Nesse contexto, o direito à proteção de dados pessoais foi elevado a direito fundamental na Constituição Federal diante da sua crescente relevância para o exercício da personalidade e dignidade humana. No entanto, em que pese a Lei Geral de Proteção de Dados – LGPD estabelecer uma sistemática de penalização administrativa, a Autoridade Nacional de Proteção de Dados – ANPD, órgão responsável pela aplicação das sanções previstas, ainda não conseguiu alcançar uma atuação repressiva eficiente em razão de diversos fatores internos e externos. Diante deste cenário, o presente trabalho objetivou analisar a possibilidade de interação entre o sistema de proteção de dados pessoais e o Direito Penal na tutela dos dados pessoais, primeiramente, para verificar se os dados pessoais podem ser considerados como bem jurídico-penal merecedor de tutela repressiva extrema. Em outra perspectiva, a partir da reflexão da teoria geral do crime quanto ao instituto de responsabilidade penal por omissão, buscou-se responder se o controlador de dados pessoais pode assumir a posição de garante, figura necessária para a configuração dos crimes omissivos impróprios. Nas reflexões alcançadas por meio de uma investigação sustentada no estudo bibliográfico e jurisprudencial, constatou-se que as indagações levantadas podem ser respondidas afirmativamente, o que não se exclui a necessidade de elaboração de tipos penais especiais para proteção desse bem jurídico, a exemplo de países integrantes da União Europeia, como a Espanha.

Palavras-chave: PROTEÇÃO DE DADOS; RESPONSABILIDADE; DIREITO PENAL; OMISSÃO.

ABSTRACT

Modern society is immersed in technological resources that once seemed unimaginable. The conveniences brought by information and communication technologies optimize time and also provide quality of life to society. However, this new reality is not without risks and vulnerabilities arising from the high exposure due to the use of cyber tools, primarily due to the availability of personal data of its users. Therefore, the protection of this information has received increasing attention from public and private organizations to promote its proper management. Legislation has also kept pace with this movement by creating protective measures for such data. In this context, the right to personal data protection has been elevated to a fundamental right in the Federal Constitution due to its growing importance for the exercise of personality and human dignity. However, despite the General Data Protection Law (LGPD) establishing a system of administrative penalties, the National Data Protection Authority (ANPD), the body responsible for enforcing the prescribed sanctions, has still not managed to achieve an effective repressive performance due to various internal and external factors. Against this backdrop, this work aimed to analyze the possibility of interaction between the personal data protection system and Criminal Law in safeguarding personal data, primarily to verify whether personal data can be considered a legal interest deserving of extreme repressive protection. From another perspective, reflecting on the general theory of crime regarding the institute of criminal liability for omission, it sought to answer whether the personal data controller can assume the position of guarantor, a necessary figure for the configuration of improper omissive crimes. The reflections reached through an investigation based on bibliographic and jurisprudential study concluded that the raised inquiries can be answered affirmatively, which does not exclude the need for the elaboration of special penal types for the protection of this legal asset, akin to countries of the European Union, such as Spain.

Key-words: DATA PROTECTION; RESPONSABILITY; CRIMINAL LAW; OMISSION.

LISTA DE SIGLAS

ABRANET	Associação Brasileira de Internet.
ADI	Ação Direta de Constitucionalidade
AEPD	Agência Espanhola de Proteção de Dados
ANPD	Autoridade Nacional de Proteção de Dados
CDC	Código de Defesa do Consumidor
CPF	Cadastro de Pessoa Física
EaD	Educação à Distância
EDPB	Comitê Europeu de Proteção de Dados.
RGPD	Regulamento Geral de Proteção de Dados da União Europeia
IBGE	Instituto Brasileiro de Geografia e Estatística
IE-DPA	Autoridade Irlandesa de Proteção de Dados
INSS	Instituto Nacional de Seguro Social
LGPD	Lei Geral de Proteção de Dados
LOPDGDD	Lei Orgânica de Proteção de Dados e Garantia dos Direitos Digitais
LOTARD	Lei Orgânica de Proteção de Dados
MCI	Marco Civil da Internet
NSA	Agência de Segurança Nacional dos Estados Unidos
ONU	Organização das Nações Unidas
MP	Medida Provisória
ONU	Organização das Nações Unidas
PL	Projeto de Lei
SISBEN	Sistema Corporativo de Benefícios do INSS
STJ	Superior Tribunal de Justiça
TIC	Tecnologia da informação e comunicação

SUMÁRIO

1 INTRODUÇÃO

Na sociedade contemporânea, as tecnologias da informação tornaram-se onipresentes, influenciando profundamente as atividades cotidianas das pessoas. Desde a comunicação instantânea até o acesso a diversos conteúdos que podem ser acessados em qualquer lugar, a tecnologia tem transformado o modo de viver e interagir. A conveniência proporcionada por *smartphones*, aplicativos de entrega e plataformas de *streaming* exemplifica como a tecnologia molda rotinas diárias.

O fenômeno do Big Data está no cerne dessa revolução tecnológica. Refere-se ao imenso volume de dados coletados diariamente, derivados das interações digitais. Cada clique, pesquisa ou compra on-line contribui para um rastro digital que pode ser analisado e utilizado para diversas finalidades. A título de exemplo, as empresas podem utilizar esses dados para personalizar serviços e produtos, beneficiando os consumidores com experiências sob medida. Contudo, a gestão inadequada desses dados pode levar a violações à privacidade, com informações pessoais potencialmente expostas a usos indevidos.

A compra de produtos e serviços foi radicalmente modificada por tecnologias digitais, que simplificam o processo de aquisição e promovem uma experiência mais cômoda e barata ao consumidor. Plataformas de comércio eletrônico capturam dados dos usuários para direcionar produtos de potencial interesse, conforme a navegação realizada. Enquanto isso, sistemas de pagamento digital facilitam transações rápidas e seguras. Até mesmo consultas médicas *on-line* estão à disposição, propiciando conforto e segurança aos que não desejam comparecer a um hospital.

No entanto, essa dependência crescente quanto ao uso de tecnologias suscita preocupações com a privacidade e a segurança dos dados pessoais, que são frequentemente coletados e armazenados por diversas instituições públicas e privadas. As facilidades e conveniências vêm acompanhadas do risco de exposição a fraudes e roubos de identidade, caso os dados não sejam adequadamente protegidos.

Por esse motivo, na era tecnológica na qual a sociedade se encontra atualmente, o sistema de proteção dos dados pessoais merece galgar um espaço cada vez maior sob a tutela do Estado, diante da sua importância em praticamente todas as relações jurídicas estabelecidas pelos indivíduos, sejam elas públicas ou privadas.

Com efeito, a proteção de dados se tornou tema de alta relevância nos últimos anos após a implementação de diversas inovações tecnológicas. Esse movimento foi acelerado pela Pandemia do Covid-19 em razão da imposição de isolamento social estabelecido de forma rigorosa. Os serviços de consumo pela internet foram intensificados e desenvolvidos ao longo desse período para que pudesse sustentar os mercados. Os consumidores foram conquistados pela facilidade e comodidade, trazendo uma consolidação do *e-commerc*e após a normalização. Serviços educacionais do modelo à distância (EaD) tiveram um aumento exponencial, o uso demasiado de redes sociais para publicações de informações da vida pessoal, interações por mensagens instantâneas, bem como a utilização de serviços públicos *on-line* também são exemplos das mudanças nas rotinas das pessoas. Uma compra de livro, um cadastro em sítio governamental, publicações em redes sociais, todos esses serviços possuem em comum a necessidade de tratamento de dados por parte das organizações públicas e privadas.

Em que pese as facilidades trazidas pela informatização de atividades acima e outras não mencionadas, há a necessidade de fornecimento de informações pessoais, bancárias, entre outras, para a obtenção de acesso a produtos e serviços. Informações estas que, ao serem lançadas na rede mundial de computadores podem estar ameaçadas em caso de vulnerabilidades dos sistemas adotados pelas organizações. Por esse motivo, atualmente as legislações de diversos países preveem a necessidade de adoção de programas de boas-práticas e de conformidade no tratamento de dados, de modo a evitar ou ao menos minimizar os riscos decorrentes de suas atividades.

No âmbito nacional, a Lei Geral de Proteção de Dados (LGPD) - Lei n.º 13.709 de 14 de agosto de 2019, representa um marco na regulamentação da proteção de dados pessoais no ordenamento jurídico brasileiro. A origem desta lei recebeu grande influência do Regulamento Geral de Proteção de Dados da União Europeia – RGPD.

Além de estabelecer definições e princípios basilares, a LGPD prevê os direitos dos titulares, bem como a responsabilidade dos agentes de tratamento e as sanções aplicáveis em caso de descumprimento das normas de proteção de dados pessoais. O diploma estabelece em seus artigos 52 a 55 penalidades no âmbito administrativo, como advertência, multa, publicização da infração, bloqueio e eliminação de dados pessoais, suspensão parcial de funcionamento e proibição de funcionamento.

O tratamento de dados deve ser regido por diversos princípios elencados na LGPD, entre eles, o da segurança, segundo o qual os agentes de tratamento devem utilizar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos maliciosos ou de situações ilícitas ou acidentais de destruição, perda, alteração, comunicação ou difusão dos dados dos titulares.

Ressalte-se que no contexto empresarial, apesar da normatização e obrigatoriedade da adequação das ações para garantir a proteção de dados pessoais, é sabido que as organizações determinam sua atuação com base na rentabilidade de suas atividades. Ou seja, em algumas situações, a vantagem econômica pode ser maior do que a as sanções administrativas previstas na LGPD, o que pode levar as organizações a atuarem em não-conformidade de forma consciente e voluntária.

Em outra perspectiva, os dados pessoais se tornaram moeda de grande valor econômico para as empresas. Diante desde cenário, o ponto inicial da discussão consiste em analisar, diante da importância cada vez mais crescente do direito fundamental à proteção de dados e, consequentemente da constatação de sua vulnerabilidade, se é possível e necessária uma intersecção do sistema de proteção de dados com o Direito Penal. Assim, serão analisados os fundamentos para responder em que medida o direito à proteção de dados pessoais pode ser considerado como um bem-jurídico penal.

De igual forma, caso se conclua que a proteção de dados constitui um bem jurídico-penal, o estudo abordará a possibilidade de responsabilização penal do controlador de dados pessoais e, eventualmente do operador em razão da omissão imprópria, considerando que a LGPD prevê que estas figuras possuem o dever de promover a segurança dos dados pessoais e a responsabilidade administrativa pelos danos causados pela gestão de dados.

A discussão do tema exige um estudo aprofundado sobre o microssistema de proteção de dados e o institutos basilares do Direito Penal brasileiro, principalmente quanto aos princípios norteadores desse ramo e definições essenciais, como o crime comissivo por omissão.

A pesquisa científica propõe realizar um estudo sobre a interação dos sistemas jurídicos de proteção de dados pessoais e direito penal sob o enfoque de teorias de hermenêutica que permitam a intersecção e coordenação entre esses ramos do direito, à luz de uma interpretação sistemática da Constituição Federal.

Portanto, o objetivo geral proposto consiste em analisar a possibilidade do direito fundamental à proteção de dados pessoais ser considerado um bem jurídico tutelado pelo direito penal. De forma a direcionar os estudos para o alcance proposto, foram delimitados os seguintes objetivos específicos: a) compreender o microssistema de proteção de dados, com análise dos conceitos, princípios e institutos mais importantes, bem como a sua interação com outros ramos do direito, notadamente o direito penal; b) realizar uma análise do cenário nacional quanto às sanções administrativas já aplicadas pela ANPD e avaliar se elas podem ser consideradas suficientes para as funções preventiva e repressiva contra o tratamento irregular de dados pessoais; c) refletir sobre o instituto da omissão imprópria no direito penal e as teorias que fundamentam a existência da posição do garante d) estudar sobre os agentes de tratamento e suas atribuições de modo a identificar se podem ser considerados como garantidores em razão de suas atribuições legais no tratamento de dados pessoais.

A partir do estudo sistemático do microssistema de proteção de dados à luz da Constituição Federal, principalmente após a Emenda Constitucional n.º 115 de 2022, que incluiu a proteção de dados no rol dos direitos e garantias fundamentais, constatou-se que os mecanismos atuais de fiscalização e aplicação de sanções administrativas ainda são executados de maneira tímida, não demonstrando (ao menos por enquanto) serem suficientes para atingir as finalidades de prevenção e punição pelas irregularidades no tratamento de dados pessoais.

Nesse sentido, a partir da adoção de teorias hermenêuticas, o microssistema da proteção de dados não exclui a aplicabilidade de normas de outros ramos do direito, notadamente o Direito Penal. A teoria do diálogo das fontes permite a realização de uma intersecção harmônica entre sistemas jurídicos sem a necessidade de exclusão de um ou de outro e sem violação às normas de interpretação e integração das leis.

Em um estudo do Direito Penal a partir de sua finalidade instrumental de proteção aos bens jurídicos-penais, conclui-se que a proteção de dados é passível de ser considerada como tal. Como é sabido, esse ramo do direito deve adentrar somente nas hipóteses em que o remédio sancionador extremo seja necessário, quando outras formas de intervenção se mostrarem insuficientes. Assim, medidas de responsabilização penal devem ser a *ultima ratio*, dentro da observância dos princípios da intervenção mínima, legalidade e fragmentariedade.

Conforme demonstrado, o direito à proteção de dados pessoais alcançou relevância como direito fundamental autônomo e sua garantia se tornou extremamente necessária ao desenvolvimento da personalidade e dignidade humana. Diante da vulnerabilidade que este direito está submetido em razão das tecnologias da informação e comunicação, a sua violação pode acarretar graves danos de diversas ordens aos indivíduos, sejam de natureza material, moral, de imagem, entre outras.

Infelizmente, a realidade atual sobre os mecanismos de fiscalização e responsabilização administrativa ainda têm apresentado deficiências que dificultam ou até mesmo impossibilitam o alcance necessário para a repressão da violação do direito à proteção de dados.

Dessa forma, a partir da conclusão de que a proteção de dados consiste em um bem jurídico tutelado penalmente, verifica-se que o Direito Penal pode intervir na proteção desse direito fundamental por meio da previsão de responsabilidade criminal em razão da relação jurídica especial entre os agentes de tratamento e os titulares dos dados pessoais.

A teoria geral do crime adotada pelo ordenamento jurídico brasileiro prevê a possibilidade de configuração da tipicidade por meio de um comportamento comissivo ou omissivo. O enfoque do trabalho consistiu em estudar o instituto do crime omissivo impróprio, em especial o requisito da posição do garantidor para a configuração deste tipo.

Nesse contexto, a LGPD prevê a existência de duas figuras principais responsáveis pela gestão dos dados pessoais, o controlador e o operador, denominados agentes de tratamento. O referido diploma legal estabelece as responsabilidades do controlador como agente detentor do poder de decisão dentro da organização a respeito da adoção de medidas preventivas e cumprimento de todas as normas de proteção de dados. A partir da análise dessas responsabilidades previstas legalmente, chegou-se à conclusão que o controlador pode ser responsabilizado criminalmente pela omissão dolosa no tratamento irregular de dados, a partir do descumprimento de suas obrigações. O operador, em que pese possuir, em tese, a atribuição restrita ao cumprimento das determinações do controlador, não é possível ainda excluir a possibilidade de sua responsabilização, a depender da situação concreta.

Portanto, esses agentes previstos na LGPD atuam como figuras típicas de “garantes” na definição adotada pelo artigo 13, § 2º do Código Penal, uma vez que assumem responsabilidades contratuais e legais.

A fim de alcançar os objetivos geral e específicos estabelecidos, a presente pesquisa adotará o método hermenêutico fenomenológico. Para o aprofundamento necessário à discussão do tema, será adotado como metodologia de procedimento o método bibliográfico, a partir de revisão bibliográfica de doutrina e artigos jurídicos de periódicos com classificações elevadas no Qualis da CAPES, bem como de referências jurisprudenciais relacionadas ao tema.

O trabalho possui suporte na Linha de Pesquisa Hermenêutica, Constituição e Concretização de Direitos do Programa de Pós-Graduação em Direito da Universidade do Vale do Rio dos Sinos. O tema proposto vincula-se com a área de pesquisa Cibertransparência da professora orientadora Dra. Têmis Limberger.

O presente estudo está estruturado em três capítulos. O primeiro busca abordar os conceitos principais que norteiam o sistema de proteção de dados pessoais, bem como os princípios que regem a matéria, sob o enfoque da relação deste novo direito com outros direitos fundamentais. Ainda serão apresentadas considerações sobre a Autoridade Nacional de Proteção de Dados – ANPD e suas atribuições enquanto órgão fiscalizatório e sancionador em face do tratamento ilícito ou indevido de dados pessoais. A partir deste aparato conceitual, ainda serão analisados os números relacionados aos processos administrativos sancionadores instaurados pela ANPD.

No segundo capítulo serão levantadas reflexões sobre a intersecção do sistema de proteção de dados pessoais e outros ramos do direito, em especial o direito penal, como objetivo específico da pesquisa. A partir dessa análise, propõe-se estudar sobre a função do direito penal de proteção de bens jurídicos, enquadrando a proteção de dados nesse conceito.

Por sua vez, no terceiro capítulo, a pesquisa será direcionada ao estudo do tipo penal comissivo por omissão, ou denominado também de omissivo impróprio, com destaque para a análise da figura do garante e das teorias que justificam a sua responsabilidade. Em seguida, os deveres dos agentes de tratamento previstos na LGPD serão estudados e fim de verificar se o controlador e, eventualmente o operador, podem ser enquadrados na posição de garantes no exercício de suas atribuições.

No último capítulo ainda serão tecidos breves comentários sobre a adoção de boas práticas e de governança como mecanismos de prevenção à violação de dados pessoais pelas instituições. Por fim, ainda serão apresentados exemplos de legislações no âmbito internacional sobre a proteção de dados pessoais nos campos penal e administrativo.

Portanto, a estruturação de cada seção pretende conduzir o leitor à compreensão lógica do contexto atual do sistema de proteção de dados para, após, possibilitar o entendimento quanto aos elementos essenciais do diálogo entre este novo direito fundamental e o Direito Penal.

2 SISTEMA DE PROTEÇÃO DE DADOS PESSOAIS: INTRODUÇÃO AOS CONCEITOS E PRINCÍPIOS FUNDAMENTAIS.

O sistema de proteção de dados pessoais pode ser considerado, em certa medida, como uma nova estrutura no ordenamento jurídico nacional. Ao passo que foi verificado o aumento exponencial de fluxo de informações na internet e, consequentemente o aumento da ocorrência de violações de dados pessoais, o Direito precisou acompanhar esse movimento em direção à implementação de normas próprias sobre o tratamento de dados pessoais. Este primeiro capítulo destina-se a abordar os principais conceitos e institutos que envolvem o tema, de modo a facilitar o entendimento das questões que serão levantadas em seguida.

No entanto, antes de adentrar ao objeto deste capítulo, entende-se pela necessidade de apresentar uma contextualização do cenário atual sobre a realidade da sociedade quanto ao uso de tecnologias para a execução de diversas atividades no quotidiano da maioria das pessoas. É o que será brevemente apresentado nas próximas linhas.

2.1 Contexto atual sobre o uso das tecnologias na sociedade.

A afirmação de que grande parte da população alcançou um alto nível de uso de tecnologias em suas atividades rotineiras não surpreende mais. No entanto, ao analisar os dados atualizados de 2024 é possível chegar a uma noção mais concreta desta realidade.

Segundo dados extraídos do relatório global de visão geral digital 2024, de uma população global de mais de 08 (oito) bilhões de pessoas no mundo, 69,4% (sessenta e nove vírgula quatro por cento) utiliza um dispositivo móvel, representando um aumento de mais de 2,5% (dois e meio por cento) em relação ao início de 2023. Outro dado de grande relevância consiste na quantidade de pessoas que usam a internet. Ao todo, mais de 66% (sessenta e seis por cento) de indivíduos em todo o mundo possuem acesso à rede mundial de computadores. Foram 97 (noventa e sete) milhões de novos usuários desde o ano anterior. Segundo dados divulgados no Relatório Global de visão geral digital 2024, há mais de 5 (cinco) bilhões de identidades de usuários ativos de mídia social, o que representa cerca de 62,3% (sessenta e dois vírgula três por cento) das pessoas no mundo. Em um ano, houve um aumento de

5,6% (cinco vírgula seis por cento), equivalente a 266 (duzentos e sessenta e seis) milhões de novas identidades.[1]

Por sua vez, o Brasil alcançou a marca de segundo colocado em relação ao tempo diário conectado à internet, com a média de 9 (nove) horas e 13 (treze) minutos por dia, ficando atrás apenas da África do Sul.[2] Deste tempo conectado, boa parte reflete em horas de trabalho, entreterimento, educação, consumo e realização de diversas atividades que antes eram executadas de forma presencial.

A percepção da magnitude dos números apresentados contribui para a compreensão da importância do tema proposto neste trabalho. Em que pese a proteção de dados não ser restrita somente aos dados informatizados, atualmente os riscos mais significativos de violação das informações acontecem por meio das tecnologias da informação, principalmente em razão da quantidade de dados pessoais tratados, o que pode acarretar vulnerabilidades para o tratamento ilícito ou indevido de dados pessoais.

Em termos de violação de dados pessoais, não há dificuldade em localizar notícias sobre casos de maior repercussão, considerando os números de pessoas atingidas, as quais tiveram informações importantes vazadas na internet em razão de falhas de segurança e/ou de invasões por agentes maliciosos. Nas próximas linhas serão citados alguns exemplos a fim de deixar mais clara a gravidade desses fatos e a imprescindibilidade da efetivação do sistema de proteção de dados no mundo e no Brasil.

Em uma pesquisa rápida na internet diversas notícias sobre vazamento de dados podem ser encontradas com facilidade. Contudo, a fim de não tornar a leitura morosa, serão destacadas algumas que mais repercutiram no campo da tecnologia.

No que se refere ao vazamento de dados, um caso que atingiu grandes proporções na mídia mundial foi chamado de “Escândalo de Cambridge Analytica”, por meio do qual foi noticiado que mais de 50 (cinquenta) milhões de perfis do Facebook foram utilizados pela empresa inglesa Cambridge Analytica para análise de informações pessoais, com o objetivo de traçar perfis psicográficos de eleitores a serem utilizados na campanha para eleição de presidente dos Estados Unidos da

---

1 EUA. Digital 2024: 5 bilhões de usuários de mídia social. Análise do relatório global de visão geral digital 2024. Londres, 2024 Disponível em: https://wearesocial-com.translate.goog/uk/blog/2024/01/digital-2024-5-billion-social-media-users/?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-br&_x_tr_pto=sc. Acesso em 18.jul.2024.

2 Ibid.

América em 2016. Posteriormente, verificou-se que o número de perfis invadidos ultrapassou 500 (quinhentos) milhões de usuários da rede social.[3] Após a descoberta, a empresa Meta foi multada em diversos países em razão constatação da violação dos dados pessoais de seus usuários.

No Brasil estima-se que dados de aproximadamente 8 (oito) milhões de brasileiros foram violados em razão do ocorrido. Com efeito, o Tribunal de Justiça de Minas Gerais condenou o Facebook ao pagamento de R$5.000,00 (cinco mil reais) para cada usuário que comprovasse a utilização da ferramenta no período da coleta dos dados, além da fixação de indenização coletiva no valor de R$72.000.000,00 (setenta e dois milhões de reais) revertido ao Fundo Estadual de Interesses Difusos.[4]

Outra notícia amplamente divulgada refere-se ao vazamento de dados de mais de 223 (duzentos e vinte e três) milhões de brasileiros ocorrido em 2021. As informações estavam à venda na internet e incluíam dados de CPF, endereços, fotos de rostos, *score* de crédito, imposto de renda de pessoa física, dados cadastrais de empresas de telefonia, benefícios do Instituto Nacional de Seguro Social – INSS, informações da rede social Linkedin, dentre outros. O número de indivíduos atingidos com a invasão superou o número de brasileiros, pois incluiu dados de pessoas já falecidas à época.[5]

No ano de 2022, o Instituto Nacional de Seguro Social (INSS) comunicou à ANPD a ocorrência de um volume anormal de consultas de dados de seus beneficiários. Nos meses de agosto e setembro daquele ano, mais de 90 (noventa) milhões de consultas foram realizadas no Sistema Corporativo de Benefícios do INSS (SISBEN) e 09 (nove) milhões de consultas ao BHL00. Os dados coletados incluíram nome, CPF, o número de inscrição do trabalhador (NIT), identidade, data de nascimento, sexo, ramo de atividade profissional, dados bancários e quantidade de dependentes. Os dados foram extraídos por meio de acesso realizado por credenciais de ex-funcionários e ex-estagiários que ainda se encontravam válidas.

---

3 BBC News Brasil. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira das autoridades. São Paulo, 2018 Disponível em: < https://www.bbc.com/portuguese/internacional-43461751>. Acesso em 23 set de 2024.

4 CNN, Brasil. Facebook é condenado a pagar R$ 20 milhões por vazamento de dados de usuários. São Paulo, 2024 Disponível em: https://amti.com.br/blog/dados-vazados-pelo-facebook/ https://www.cnnbrasil.com.br/nacio.nal/facebook-e-condenado-a-pagar-r-20-milhoes-por-vazamento-de-dados-de-usuarios/. Acesso em 23 set. 2024.

5 GLOBO. Megavazamento de dados expõem informações de 223 milhões de números de CPF. São Paulo, 2021.Disponível em: https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2021/01/25/vazamentos-de-dados-expoem-informacoes-de-223-milhoes-de-numeros-de-cpf.ghtml. Acesso em 23 set. 2024.

Tais fatos foram apurados em processo administrativo instaurado pela ANPD. Em resposta, o responsável pelo gerenciamento das credenciais na Advocacia Geral da União afirmou que:

> 44 dos 66 usuários cadastrados poderiam ser excluídos. Desses, 39 seriam pessoas desconhecidas e 5 seriam ex-estagiários, sem vínculo atual com a instituição, indicando que 2/3 dos usuários do grupo de acesso estavam cadastrados indevidamente[6].

O INSS reconheceu que o incidente afetou dados sensíveis referentes à saúde e registros financeiros dos beneficiários.[7] Os danos decorrentes desse vazamento podem ser incalculáveis em decorrência das dificuldades de apuração sobre eventuais usos desses dados.

Diversos outros casos de vazamento de dados ocorreram no Brasil e no mundo. Em muitos deles, a violação das informações atingiu centenas de milhares de usuários de sistemas de banco de dados de instituições públicas e privadas. Considerando a magnitude dos vazamentos e a constatação de vulnerabilidades que as informações pessoais estão submetidas, o aprofundamento do estudo sobre a responsabilidade dos agentes de tratamento nas diversas esferas do direito possui urgência e alta relevância.

Realizada essa contextualização, torna-se imprescindível compreender como o ordenamento jurídico atual vem tratando a matéria. Para tanto, os aspectos principais do sistema nacional de proteção de dados serão apresentados, assim como os conceitos, princípios e institutos que norteiam este novo direito.

2.2 A normatização do direito à proteção de dados pessoais.

Com a imersão progressiva das pessoas no mundo virtual, como visto anteriormente, houve um aumento assustador na velocidade na produção e armazenamento de dados pessoais nos últimos anos. Ocorre que o processamento de dados não se tornou uma preocupação atual. Na década de 90, com a utilização de computadores para a realização de tratamento da dados, constatou-se um

6 ANDP. Relatório de instrução n.º 01/2024/CGF/ANDP. 25 de janeiro de 2024. Brasília, 2024. Disponível em: https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao/PAS_INSS_principal_publica.pdf. Acesso em 24 set 2024

7 ANDP. Processo administrativo 00261.001888/2023-21 p. 12. Brasília, 2023. Disponível em https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao/PAS_INSS_principal_publica.pdf. Acesso em 24 set 2024.

crescimento ainda maior na produção de informações de forma mais estruturada, o que levou ao início do surgimento de legislações que objetivaram a sua proteção.[8]

Manuel Castells levantou reflexões de grande importância no seu estudo sobre a revolução da tecnologia da informação e comunicação (TIC) e seus efeitos sociais. Para ele, o impacto que as TIC's exerceram na sociedade provocou uma penetrabilidade da informação por toda a sua estrutura. Esta revolução trouxe a transformação de uma "cultura material" por meio de um novo paradigma tecnológico, que inclui a microeletrônica, computação, telecomunicações e radiodifusão, optoeletrônica e ainda a engenharia genética.[9]

A sociedade atual é, pois, digital. Segundo Castells,

> [...] o processo atual de transformação tecnológica expande-se exponencialmente em razão de sua capacidade de criar uma interface entre campos tecnológicos mediante uma linguagem digital na qual a informação é gerada, armazenada, recuperada, processada e transmitida.[10]

A utilização crescente das tecnologias nas mais diversas atividades dos indivíduos contribuiu para um fenômeno denominado de digitalização dos direitos fundamentais. Em outras palavras, surgiu a necessidade de realização de uma análise dos direitos fundamentais sob uma nova perspectiva, a partir da alteração substancial nas relações sociais, comerciais, culturais, políticas entre outras.[11]

Segundo Marcos César Botelho, a alta exposição dos dados pessoais da sociedade digital causa uma fragilidade à personalidade, intimidade e privacidade da pessoa, pois as ações realizadas com o manuseio da internet deixam rastros de informações que se tornam preciosas para as organizações em seus negócios, sendo, muitas vezes, utilizadas sem o conhecimento do titular.[12]

O avanço rápido da tecnologia da informação e a expansão da sua utilização pela sociedade pós-moderna modificou sua organização e as próprias relações entre os indivíduos. Novas formas de serviços e de consumo *on-line* passaram a ser rotina

---

8 DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico Journal of Law [EJJL], v. 12, n. 2, p. 91-108, 2011. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315/658. Acesso em 18 jul. 2022.

9 CASTELLS, Manuel. A sociedade em rede. V. 1. 8.ed. São Paulo: Paz e Terra, 2005. p. 67 e 114.

10 Ibid. p. 68.

11 SARLET, Ingo. Proteção de dados como direito fundamental na Constituição Federal Brasileira de 1988: contributo para a construção de uma dogmática constitucional adequada. Direitos Fundamentais & Justiça | Belo Horizonte, ano 14, n. 42, p. 179-218, jan./jun. 2020. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/875. Acesso em 30.08.2023.

12 BOTELHO. Marcos César. A LGPD e a Proteção ao Tratamento de Dados Pessoais de crianças e Adolescentes. Revista de Direitos Sociais e Políticas Públicas (UNIFAFIBE). São Paulo, 2020. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_informativo/bibli_inf_2006/Rev-Dir-Soc-Pol-Publicas_v.8_n.2.08.pdf.Acesso em 01 fev. 2021.p.10.

para parte considerável da população. A política, a cultura e as relações sociais também sofreram grande impacto com o uso quotidiano de recursos informáticos, produzindo um alto volume de troca de informações em uma velocidade nunca antes pensada.

As relações sociais sofreram grande impacto com a invasão da tecnologia graças ao maior alcance da população à aquisição de *smartphones* e computadores em geral, o que facilitou o acesso a redes sociais e diversos aplicativos para acesso a produtos e serviços. As relações entre os indivíduos passaram a ser instantâneas, possibilitando uma expansão no alcance de outras pessoas que antes enfrentavam uma limitação na comunicação em razão da distância geográfica. Por outro lado, conforme o sociólogo polonês Zygmunt Bauman esclareceu, essas relações se tornaram superficiais e temporárias:

> O tempo instantâneo e sem substância no mundo do software é também um tempo sem consequências. “Instantaneidade” significa realização imediata, “no ato”, - mas também exaustão e desaparecimento do interesse”[13]

Nessa modernidade líquida, na qual a velocidade das informações tornou-se uma das principais exigências da sociedade, as tecnologias e recursos da informática passaram a fazer parte de quase todos os campos da vida das pessoas.

O livro de Zygmunt Bauman apresenta o conceito de uma modernidade fluida, caracterizada pela flexibilidade, efemeridade e incerteza. A sociedade, segundo o autor, se tornou líquida como os fluidos, constantemente em transformação, sem estruturas sólidas e duradouras. Essa característica se manifesta em diversos aspectos da vida, impactando as relações sociais, as identidades individuais e a forma como as pessoas experimentam o tempo e o espaço.

Essa reflexão de Bauman possui um paralelo direto com a realidade tecnológica contemporânea, principalmente no que diz respeito à velocidade e à fluidez da informação. A internet, com sua capacidade de disseminar conteúdo instantânea e globalmente cria um ambiente que espelha a "liquidez" descrita pelo sociólogo. A constante atualização de softwares, a obsolescência programada de produtos tecnológicos, a volatilidade do mercado e as mudanças rápidas nas tendências da tecnologia ilustram perfeitamente essa dinâmica de mudança.

13 BAUMAN, Zygmunt. Modernidade líquida. Tradução de Plinio Dentzien. Rio de Janeiro: Zahar, 2021

Além das relações sociais, a expansão do uso de ferramentas tecnológicas em diversas atividades, não somente comerciais, mas de serviços públicos, representou também uma mudança na lógica do consumo. O efeito comum decorrente da utilização das tecnologias em todas as esferas da sociedade citadas consiste na produção de um alto volume de dados pessoais, que são disponibilizados na internet pelos usuários de produtos e serviços.

É possível citar diversos exemplos de rotinas comuns de quantidade significativa da população, como transações bancárias por meio do navegador de internet ou em aplicativos de *smartphones*, a exposição da imagem por meio de monitoramento com videocâmeras de segurança, programas interativos e rastreadores na internet e tantos outros. Não se pode esquecer dos riscos decorrentes das compras *on-line* e das informações inseridas despretensiosamente em diversas redes sociais que aparentam ser inofensivas.

Nesse contexto, impedir a exposição indevida de informações pessoais na rede mundial de computadores tornou-se uma árdua tarefa para instituições públicas e privadas. Constata-se rotineiramente a vulnerabilidade sofrida pela possibilidade de vazamento ou tratamento irregular dos dados pessoais capazes de provocar interferências nos direitos fundamentais dos indivíduos, como a privacidade, a intimidade, autodeterminação informativa, personalidade e da própria proteção de dados, inserida recentemente no rol dos direitos fundamentais estabelecido no art. 5º da Constituição Federal do Brasil.[14]

Por essa razão, tornou-se urgente a necessidade de uma regulamentação voltada à proteção da pessoa natural quanto ao tratamento de dados pessoais disponíveis na rede mundial de computadores, de modo que aqueles não sejam utilizados para finalidades diversas das autorizadas pelos seus titulares ou até mesmo para a prática de atos ilícitos.

Nesse contexto, é fundamental que as organizações adotem medidas adequadas de prevenção e de respostas a fim de mitigar os danos e proteger os direitos dos titulares dos dados. O ordenamento jurídico tem tentado acompanhar

14 Segundo a Abranet, em 2022, o Brasil ficou em 4º lugar no ranking de países que mais sofreram violações de segurança cibernética. No segundo trimestre daquele ano, foram cerca de 3,2 milhões de usuários atingidos com violação de dados. – ASSOCIAÇÃO BRASILEIRA DE INTERNET (ABRANET). Vinte e cinco contas sofrem violação de dados por minuto no Brasil. São Paulo, 2022. https://www.abranet.org.br/Noticias/Vinte-e-cinco-contas-sofrem-violacao-de-dados-por-minuto-no-Brasil-3966.html?UserActiveTemplate=mobile%2Csite. Acesso em 03 mai.2024

essas mudanças, a exemplo de legislações que foram publicadas a fim de regular o uso da internet e das informações.

A partir da constatação de que o grande volume de informações disponibilizadas pelos usuários se tornou alvo de interesse das instituições para a prática de atividades comerciais (principalmente captação de perfis para direcionamento de publicidade), além de ter se tornado um atrativo para a prática de ilícitos, verificou-se o movimento em diversos países em direção à regulamentação da proteção de dados pessoais, principalmente quando informatizados.

Governos e organizações ao redor do mundo têm buscado implementar legislações cada vez mais rigorosas para proteger os dados pessoais dos seus cidadãos. O Regulamento Geral de Proteção de Dados (RGPD) na União Europeia e a Lei Geral de Proteção de Dados (LGPD) no Brasil são exemplos de esforços para definir diretrizes claras sobre como as organizações devem tratar as informações pessoais. Essas regulamentações visam garantir que as empresas sejam transparentes no tratamento de dados, de modo a assegurar que os consumidores tenham controle sobre suas próprias informações.

Para compreender o estudo da proteção de dados pessoais, sua definição e como ela surgiu no ordenamento jurídico, torna-se indispensável mencionar a origem desse direito no campo internacional, notadamente na Europa. Não se pretende ignorar a importância de relevantes legislações de outros países, como Estados Unidos, mas o recorte de pesquisa se deu em razão, principalmente, da forte influência que o RGPD exerceu para a construção normativa brasileira.

Os primeiros debates e estudos a respeito da proteção de dados tiveram início a partir da inserção de tecnologias de tratamento de dados pessoais na sociedade por volta do final de década de 60 e início da década de 70 com a expansão do capitalismo. Após as primeiras reflexões e, com o avanço rápido do acesso aos recursos tecnológicos por parte dos indivíduos e das organizações, grande parte dos países passou a criar legislações de proteção de dados.[15]

O movimento de elaboração de um novo sistema jurídico de proteção de dados foi, então, decorrente da dimensão alcançada pela chamada sociedade tecnológica, na qual afetou as relações econômicas, sociais e políticas e culturais. Essa nova

15 A Lei de Proteção de Dados do Land alemã do Estado de Hesse promulgada em 30 de setembro de 1970 foi considerada a primeira legislação que trata especificamente da disciplina de proteção de dados. DONEDA, Danilo. Panorama histórico da proteção de dados pessoais In: DONEDA. Danilo et al (coord). Tratado de Proteção de dados Pessoais. Rio de Janeiro: Forense, 2021. p. 3.

realidade chamada de *Ubiquituous Computing* representa as características desse fenômeno de digitalização dinâmico e complexo: a computação onipresente.[16]

Em 1967, o Conselho da Europa criou uma Comissão Consultiva para estudar as tecnologias da informação e sua influência em relação ao direito do indivíduo não sofrer ingerências em sua vida privada. Como resultado, foi elaborada a Resolução 509 da Assembleia do Conselho da Europa sobre os direitos humanos e as novas conquistas científicas e tecnológicas. Pinãr Mañas afirma que tal resolução foi a verdadeira origem do movimento legislativo em busca do reconhecimento do direito à proteção de dados.[17]

É possível destacar na Europa três fases no desenvolvimento das legislações sobre o tema: a primeira em 1970 na Alemanha, com as leis denominadas “Land Hass”; em segundo, na França em 1978, quando previu a criação de Comissão Nacional para Proteção de Dados; e em um terceiro período, com a criação do tratamento jurídico uniforme, que autorizou a livre circulação de dados entre os países que compõem a União Europeia.[18]

Com a promulgação de algumas constituições mais recentes na Europa, a exemplo de Portugal (1976) e Espanha (1978), houve a previsão de dispositivos relacionados à utilização da internet, de modo a estabelecer a proteção da intimidade e da honra. Nesse contexto e, com o objetivo de garantir ao cidadão a proteção do direito à informação e controle dos próprios dados, foi desenvolvido o chamado direito à autodeterminação informativa, que “equivale à liberdade informática como valor na sociedade da informação”.[19]

Até então, as legislações vinculavam a proteção de dados pessoais ao direito à privacidade. Em 2000 abriu-se uma nova etapa legislativa com a Carta dos Direitos Fundamentais da União Europeia[20] proclamada em Nice, com a previsão expressa da proteção de dados pessoais como um direito fundamental autônomo e independente do direito à intimidade.[21]

---

16 DONEDA, Danilo. Panorama histórico da proteção de dados pessoais In: DONEDA. Danilo et al (coord). Tratado de Proteção de dados Pessoais. Rio de Janeiro: Forense, 2021. p. 21.

17 MAÑAS, José Luis Piñar. El derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro. Asamblea. Revista parlamentaria de la Asamblea de Madrid, n. 13, 2005.p. 23.

18 LIMBERGER, Têmis. Informação e Internet: Apontamentos para um estudo comparado entre o regulamento geral de proteção de dados europeu e lei de proteção de dados brasileira. Novos Estudos Jurídicos, v. 25, n. 2, p. 481, 2020.

19 Ibid, p. 481

20 UNIÃO EUROPEIA. Carta dos direitos fundamentais da União Europeia. 2000/C 364/01. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em 24 de jul. 2024.

21 MAÑAS, José Luis Piñar. El derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro. Asamblea. Revista parlamentaria de la Asamblea de Madrid, n. 13, 2005.p. 25.

Em 2016, foi publicado o Regulamento Federal de Proteção de Dados Europeu - RGPD (2016/679), o qual serviu de maior inspiração para a LGPD no Brasil. Após a entrada em vigor do RGPD, os países membros passaram a regulamentá-lo por meio de legislações internas, a exemplo da França, Portugal e Reino Unido.

No Brasil, a proteção de dados pessoais tal como é considerada atualmente foi resultado de um processo recente. De igual forma como em alguns países europeus, esse direito foi inicialmente associado à privacidade, sendo, inclusive, ambos utilizados equivocadamente como sinônimos. A nível nacional, em que pese terem ocorrido tentativas anteriores de previsão legal sobre a proteção de dados pessoais, somente com o Projeto da Constituição Federal de 1988 houve a inclusão de direito ao acesso e retificação de informações em bancos de dados de entidades públicas, por meio da previsão do *habeas data*. Ainda que não se refira com exatidão sobre a proteção de dados, o projeto levou em consideração a existência de uma liberdade informática.[22]

Por sua vez, o Código de Defesa do Consumidor (CDC), Lei n.º 8.078, de 1990, estabeleceu diversos institutos de proteção das informações dos consumidores, fixando princípios que atualmente são relacionados ao sistema de proteção de dados implementado pela LGPD. Conforme prevê o CDC, o consumidor terá direito de ser notificado em caso de inserção das suas informações em banco de dados. Segundo o art. 43 do Código, o fornecedor de bens e serviços terá o dever de garantir o acesso do consumidor aos dados armazenados. Ainda há a obrigatoriedade de que tais informações sejam exatas e inseridas no banco de dados apenas para alcançar as finalidades para as quais se destinaram. Além disso, o consumidor poderá requerer a retificação ou cancelamento do armazenamento e os referidos dados permanecerão armazenados pelo prazo de até cinco anos.[23]

Ainda merece destaque a menção à Lei n.º 12.414/2011, chamada de Lei do Cadastro Positivo, por meio da qual houve o estabelecimento de diversos conceitos e princípios referentes ao tema. A lei estabeleceu a criação de um cadastro destinado a aferir a capacidade financeira a adimplemento do consumidor para fins de concessão

22 DONEDA, Danilo. Panorama histórico da proteção de dados pessoais In: DONEDA. Danilo et al (coord). Tratado de Proteção de dados Pessoais. Rio de Janeiro: Forense, 2021. p. 12

23 BRASIL. Lei federal n. 8.078, de 11 de setembro de 1990. Disponível em https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 21 de maio. 2024

de crédito.[24] A Lei complementar n.º 166 de 08 de abril de 2019[25] alterou a Lei do Cadastro Positivo e o Decreto n.º 9.936 de 24 de julho de 2019 a regulamentou, fixando, entre outras, a obrigatoriedade de autorização da pessoa natural ou jurídica para a disponibilização do seu histórico de crédito.[26]

Importante citar a Lei 12.965/2011, o Marco Civil da Internet (MCI), que implementou um sistema de direitos dos indivíduos no tocante ao uso da internet. Uma informação interessante a respeito do processo de elaboração do projeto que originou esta lei se refere ao movimento de impedir que outro projeto de lei fosse aprovado antes, o PL 84/99 e seus apensos, nos quais previa uma regulamentação do uso da internet por meio de dispositivos penais repressivos rígidos, os quais foram considerados obstáculos ao progresso da internet no país, pois tipificariam como crimes diversas condutas rotineiras dos seus usuários.

O MCI também foi influenciado durante a sua elaboração pelo “Efeito Snowden”, caracterizado pela repercussão provocada pelo vazamento de documentos da Agência de Segurança Nacional dos Estados Unidos (NSA) em 2013 pelo ex-contratado Edward Snowden. Os referidos documentos revelaram que a NSA monitorava as comunicações de pessoas em todo o mundo, inclusive chefes de Estado.[27]

Assim, com tais descobertas, houve um grande impacto no processo de conscientização pública sobre privacidade, vigilância e direitos digitais, o que provocou uma necessidade de reformulação de legislações com vistas a aumentar o rigor na promoção da privacidade, além de outras consequências para a implantação de ferramentas para proteção das comunicações na internet.

O “Efeito Snowden” acelerou o processo de aprovação do MCI, além de ter provocado a inclusão de diversos dispositivos para aumentar a proteção da privacidade e dos dados pessoais, bem como a previsão de responsabilidade dos provedores de internet pelos conteúdos gerados por terceiros.

---

24 BRASIL. **Lei federal 12.414**, **de 09 de junho de 2011**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm#:~:text=LEI%20N%C2%BA%2012.414%2C%20DE%209%20DE%20JUNHO%20DE%202011.&text=Convers%C3%A3o%20da%20Medida%20Provis%C3%B3ria%20n%C2%BA%20518%2C%20de%202010.&text=Disciplina%20a%20forma%C3%A7%C3%A3o%20e%20consulta,forma%C3%A7%C3%A3o%20de%20hist%C3%B3rico%20de%20cr%C3%A9dito.Acesso em 21.05.2024.

25 BRASIL. **Lei complementar 166 de 08 de abril de 2019**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp166.htm. Acesso em 21. maio 2024.

26 BRASIL. **Decreto 9.936 de 24 de abril de 2019**. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d9936.htm#:~:text=DECRETO%20N%C2%BA%209.936%2C%20DE%2024,forma%C3%A7%C3%A3o%20de%20hist%C3%B3rico%20de%20cr%C3%A9dito. Acesso em 21. maio 2024.

27 GLOBO. **Documentos da NSA apontam Dilma Rousseff como alvo de espionagem. São Paulo, 2024..** Disponível em: https://g1.globo.com/politica/noticia/2013/09/documentos-da-nsa-apontam-dilma-rousseff-como-alvo-de-espionagem.html. Acesso em 22.05.2024.

Finalmente, em 13 de junho de 2012 foi apresentado o Projeto de Lei - PL n.º 4060 na Câmara dos Deputados para dispor sobre o tratamento de dados pessoais. O PL visava atender a uma regulação de caráter geral do tema, conforme se extrai da justificativa do projeto.[28] Após um longo período de tramitação, houve uma expansão significativa das discussões para tornar o seu alcance mais completo. O texto final foi aprovado pelo Plenário em 29 de maio de 2018 e, por sua vez, o Senado Federal aprovou o documento no dia 10 de julho, que recebeu sanção presidencial com veto parcial.

Assim, a Lei 13.709, apelidada de Lei Geral de Proteção de Dados (LGPD) foi publicada em 14 de agosto de 2018 e entrou em vigor parcialmente em 28 de dezembro do mesmo ano. Por sua vez, os artigos 52,53 e 54, relacionados às sanções administrativas entraram em vigor somente no dia 1º de agosto de 2021. Contudo, antes de sua completa entrada em vigor, a LGPD teve seu conteúdo alterado pela Medida Provisória n.º 869 de 27 de dezembro de 2018, posteriormente convertida na Lei n.º 13.853, de 08 de julho de 2019.[29]

Enfim, a LGPD se tornou um marco legal no Brasil, uma vez que “dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou pessoa jurídica de direito público ou privado”.[30]

O referido diploma legal representa uma estrutura essencial para a implementação de um sistema próprio de proteção de dados, a começar com o estabelecimento dos fundamentos que devem sustentar o tratamento de dados, como respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, de informação, de comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem, além da livre iniciativa, a livre concorrência, a defesa do consumidor, aos direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.[31]

---

28 CÂMARA DOS DEPUTADOS. Projeto de Lei n.º 4060 de 13 de junho de 2012. Disponível em https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1001750&filename=Tramitacao-PL%204060/2012. Acesso em 25 de out. 2024.

29 A Medida Provisória 869/2018 teve o propósito de: (i) excepcionar, condicionar ou adequar sua aplicação em situações específicas, como a pesquisa acadêmica, a formulação de políticas públicas ou a prestação de serviços por órgãos estatais ou por seus prepostos; e (ii) instituir a Autoridade Nacional de Proteção de Dados (ANPD), órgão competente para regulamentar, interpretar e fiscalizar o cumprimento da referida lei, bem como, eventualmente, sancionar agentes responsáveis por seu descumprimento. BRASIL. Medida Provisória n.º 869, de 27 de dezembro de 2018. Disponível em: https://www12.senado.leg.br/publicacoes/estudos-legislativos/tipos-de-estudos/sumarios-de-proposicoes/mpv869. Acesso em 25 de out. 2024.

30 BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Art. 21. Disponível em: www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 15 de out 2024.

31 Ibid.

A LGPD estabelece os princípios da proteção de dados pessoais, apresenta os conceitos legais dos principais institutos atrelados ao tema, além de definir as hipóteses de tratamento de dados pessoais, os direitos dos seus titulares, os deveres dos agentes de tratamento, além da previsão de sanções administrativas. Ainda houve a previsão da criação da Autoridade Nacional de Proteção de Dados – a ANPD, que possui entre as suas funções, a fiscalização e instauração de processos sancionadores previstos na lei.

A propósito, ainda que não esteja no bojo do presente estudo, importante acrescentar que o direito à proteção de dados encontra-se intrinsecamente ligado a diversos direitos correlatos, como direito à informação. Nesse contexto, a própria LGPD remete a obrigatoriedade de cumprimento das normas de proteção de dados pessoais por parte do Poder Público em face do fornecimento de informações para exercício da publicidade e transparência de seus atos. [32]

Contudo, ainda que não sejam de aplicação idêntica do que a exigida nas relações de direito privado, certo é que as regras sobre tratamento de dados pessoais devem ser aplicadas nas situações em que as informações pessoais são tratadas pelo Estado em razão do exercício de suas atividades.[33]

Esta compreensão sobre a amplitude da proteção de dados pessoais no sistema jurídico atual demonstra a sua importância para o Estado Democrático de Direito, que perpassa pelas relações privadas e públicas e pelo objetivo de alcançar uma sociedade mais justa e consciente de seus direitos e deveres:

> Assim, a revolução tecnológica permite e exige uma administração mais eficaz e eficiente, mais próxima ao cidadão, mais moderna, mais rápida, que permita oferecer aos cidadãos um serviço muito melhor. Porém, ao mesmo tempo, exige uma administração pública mais transparente, mais democrática, mais controlada, mais acessível e mais respeitosa com a privacidade, a que se adiciona a proteção dos dados pessoais.[34]

Nesse sentido, não somente as instituições privadas possuem a obrigatoriedade de fornecer às pessoas a informação sobre o tratamento de seus

---

32 LIMBERGER. TÊMIS. **Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso a Informação Pública (LAI):** um diálogo (im)possível? As influências do direito europeu. Revista de Direito Administrativo. Rio de Janeiro: FGV. Vol. 281, n. 1, p. 113-144, jan/abr. 2022. Disponível em: https://periodicos.fgv.br/rda/issue/view/4786. Acesso em 25 de out. 2024.

33 Nesse sentido, a Professora ressalta: O tratamento de dados das pessoas jurídicas de direito público ou privado não é idêntico, mas uma proteção básica está assegurada pelo art. 3º, da LGPD. A toda evidência, alguns institutos, por exemplo, consentimento para coleta dos dados ou pedido de cancelamento, deverão ser mitigados quando se está diante de uma pessoa de direito público. Ibid. p. 129.

34 Ibid. p. 124.

dados, mas a Administração Pública também deve estar apta a disponibilizar o fluxo de dados produzidos no âmbito de suas competências.

A discussão a respeito da relação e eventual conflito entre a proteção de dados pessoais e o direito à informação como cumprimento do princípio da transparência merece enfoque específico, o qual não foi incorporado como objeto de pesquisa. Em resumo, cabe destacar que, ainda que se trate de um direito fundamental, a proteção de dados pessoais não consiste em um direito absoluto e sobre ele devem ser aplicadas as regras de ponderação de princípios em virtude de conflito aparente de normas.[35]

Apresentado um panorama sobre o sistema legal vigente de proteção de dados, cabe adentrar à compreensão sobre a definição de dado pessoal e sua conexão com outros direitos fundamentais de alta relevância.

2.3 Conceito de dado pessoal e sua relação com o direito à intimidade.

Após uma breve contextualização histórica sobre a origem da regulamentação do direito à proteção de dados pessoais, passa-se a estabelecer reflexões sobre o conceito legal de dado pessoal e a natureza jurídica do direito à sua proteção. Conforme artigo 5º, inciso I da LGPD, dado pessoal consiste na "informação relacionada a pessoa natural identificada ou identificável".[36] Ou seja, estão englobados nessa definição o nome completo, o número do cadastro de pessoa física – CPF -, endereço residencial, endereço eletrônico, número de telefone e outras informações.

Além desses elementos capazes de identificar a pessoa, alguns tipos de informações são considerados mais delicados e merecem uma proteção especial. São os chamados dados pessoais sensíveis, que se referem à informações sobre raça, etnia, opiniões políticas, convicção religiosa, filosófica, dados relacionados à saúde e à sexualidade do titular e filiação sindical. A diferenciação de tratamento para essa

35 LIMBERGER. TÊMIS. Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso a Informação Pública (LAI): um diálogo (im)possível? As influências do direito europeu. Revista de Direito Administrativo. Rio de Janeiro: FGV. Vol. 281, n. 1, p. 113-144, jan/abr. 2022. Disponível em: https://periodicos.fgv.br/rda/issue/view/4786. Acesso em 25 de out. 2024.

36 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Art. 21. Disponível em: www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 15 de out 2024.

categoria de dados revela a preocupação com a ocorrência a violação da igualdade de tratamento, além da própria privacidade[37]

Sob uma perspectiva de sua gênese, os dados pessoais podem ser considerados como projeção da personalidade do cidadão. Como explica Bruno Ricardo Bioni, a personalidade é formada pelos atributos tangíveis e intangíveis que distinguem uma pessoa da outra.[38]

O Código Civil apresenta um rol exemplificativo de direitos de personalidade como a vida, nome, honra, imagem, privacidade, integridade física e moral. O direito de personalidade representa, pois, um conjunto de direitos fundamentais que busca garantir a identidade, integridade e dignidade dos cidadãos.[39]

Um dos direitos mais importantes contidos no direito de personalidade se refere à intimidade. Por meio dele, são tutelados dois interesses: o primeiro que consiste em não sofrer agressões na intimidade e o segundo de que ela não seja divulgada. Ambos fazem parte do mesmo direito à intimidade, mas que contém esses dois aspectos.[40] O Professor Costa Júnior elucida:

> Para concluir: se o direito é o único e seu bem tutelado é o mesmo, conquanto com ligeiras tonalidades diversificativas, consiste a diferença na modalidade de agressão. Trata-se, pois, de dois momentos do mesmo direito subjetivo. De um momento antecedente, de reação à interferência ilícita da intimidade. E de um momento subsequente, de repulsa à divulgação indevida da intimidade legitimamente alcançada.[41]

A partir dessa diferenciação, é possível reconhecer a presença desses dois aspectos quando é realizada a análise no contexto da proteção de dados pessoais. Primeiramente, a devassa das informações pode ocorrer por meio de uma conduta de usurpação de dados pessoais, como é o caso do crime previsto no art. 154-A do Código Penal[42], que prevê a invasão de dispositivo informático.

---

37 LIMBERGER, Têmis. O direito à Intimidade na Era da Informática: A necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.p. 203.

38 BIONI, Bruno R. Proteção de Dados Pessoais - A Função e os Limites do Consentimento. Rio de Janeiro: Grupo GEN, 2021. E-book. ISBN 9788530994105. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994105/. Acesso em: 21 mai. 2024, p. 55.

39 BRASIL. Lei 10.406, de 10 de janeiro de 2002. Disponível em https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em 22.05.2024

40 COSTA JÚNIOR, Paulo José. O direito de estar só. Tutela penal da intimidade. 2.ed. rev. e atual.. São Paulo: Revista dos Tribunais, 1995. p. 34.

41 Ibid.

42 Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Redação dada pela Lei nº 14.155, de 2021). BRASIL. **Decreto 2.848, de 07 de dezembro de 1940**. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 25 de jul. 2024.

Com efeito, os dados pessoais podem ser divulgados ilicitamente a partir de vulnerabilidades na segurança de instituições públicas e privadas que detêm legitimamente os dados pessoais dos indivíduos em razão da execução das mais variadas atividades, sejam de natureza pública ou privada, com destaque para a venda de produtos ou prestação de serviços.

A doutrina adota a teoria dos círculos concêntricos ou das esferas para explicar as dimensões existentes na vida privada do indivíduo, conforme o grau de intimidade definida por seu titular. Desse modo, o círculo maior consiste na esfera privada *estrito sensu*, onde estão dispostos os comportamentos ou acontecimentos os quais não há interesse de que sejam de domínio público. Por sua vez, dentro da esfera privada, se encontra a esfera da intimidade ou confidencial. Neste círculo, o indivíduo permite o acesso de certas pessoas de sua confiança para compartilhar acontecimentos íntimos. Por último, o âmbito mais íntimo da vida privada consiste na esfera do segredo, o qual exige uma maior necessidade de proteção contra violações. As pessoas da esfera da intimidade não possuem acesso à esfera do segredo, sendo este o círculo mais restrito do indivíduo.[43]

Portanto, a teoria dos círculos concêntricos auxilia na compreensão sobre o poder que o indivíduo possui para decidir sobre quais os aspectos de sua vida ele deseja manter em sigilo e quais ele permitirá o conhecimento por outras pessoas e/ou instituições.

Informações sobre doenças, opiniões políticas ou outras podem afetar decisões nas mais diversas esferas da vida, desde a escolha pela contratação de um empregado, por exemplo, violando o princípio da isonomia entre as pessoas, até decisões estratégicas para o mercado ou para a política, que podem afetar o resultado de uma eleição ou do mercado, por exemplo.

Inicialmente o direito à intimidade possuía um aspecto negativo, consistente no direito de ser deixado só. Nesta fase, um trabalho de grande repercussão quanto ao início do estudo desse direito se refere ao artigo *The rigth to privacy*, dos autores Samuel D. Warren e Louis D. Brandeis publicado na *Harvard Law Review* em 1890.[44]

Por meio deste trabalho, Warren e Brandeis defendiam que o direito à privacidade deveria ser considerado um direito fundamental, tendo em vista a rápida

43 COSTA JÚNIOR, Paulo José. O direito de estar só. Tutela penal da intimidade. 2.ed. rev. e atual.. São Paulo: Revista dos Tribunais, 1995. p. 36 e 37.

44 SAMUEL D. Warren; LOUIS D. Brandeis. The Right to Privacy. Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890). Havard, EUA, 1980, p. 193-220. Disponível em: https://www.jstor.org/stable/i256795. Acesso em 23 de jul. 2024.

mudança do mundo, no qual tornaram-se comuns as invasões a esse direito em razão do advento de novas tecnologias à época, como a fotografia, utilizada principalmente pela mídia que especulava a vida privada de figuras públicas.

Nesse sentido, o direito à privacidade deveria ser reconhecido como um direito jurídico autônomo. O texto ainda abordou sobre a evolução do direito para garantir não somente os direitos em questões tangíveis, como a integridade física, mas com o tempo foi necessário oferecer instrumentos de proteção dos bens imateriais, como a privacidade. Os autores criaram o conceito de “o direito de ser deixado só” (*the right to be let alone*), que foi considerado um marco na doutrina como fundamento de proteção da vida privada contra invasões e explorações.

Posteriormente, somente a abstenção do Estado não era mais suficiente para alcançar a efetividade do direito à intimidade, o que desencadeou uma evolução para a adoção de um aspecto positivo, demandando prestações concretas com vistas à proteção desse direito fundamental. Cite-se o direito ao esquecimento, a exigência de objetividade, de estabelecimento de prazo para o armazenamento de informações, direito à retificação de informações, necessidade de consentimento expresso para tratamento de dados e outros previstos nas legislações esparsas.[45]

Com o avanço da tecnologia e ampliação de acesso a diversos recursos que facilitaram a comunicação entre os indivíduos, constatou-se cada vez mais intenso esse movimento de prestação positiva por parte do Poder Público no tocante à proteção da intimidade, tendo em vista que as informações pessoais se tornaram cada vez mais valiosas para as instituições. Para estas, o conhecimento é poder.

Com efeito, a personalidade possui uma característica de elasticidade, segundo a qual a construção desse direito fundamental deve ser centrado na promoção da pessoa humana, de modo que a cláusula geral do direito à personalidade pode abranger novas figuras, como é o caso dos dados pessoais.[46]

A conclusão de que os dados pessoais são considerados como extensão do direito de personalidade pode ser extraída do seu conceito legal, pois será considerado como dado pessoal a informação capaz de identificá-la ou de torná-la identificável, ou seja, elementos por meios dos quais a pessoa possa ser

45 LIMBERGER, Têmis. O direito à Intimidade na Era da Informática: A necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.p. 40.

46 BIONI, Bruno R. Proteção de Dados Pessoais. A Função e os Limites do Consentimento. Rio de Janeiro: Grupo GEN, 2021. E-book. ISBN 9788530994105. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994105/. Acesso em: 21 mai. 2024, p. 50.

individualizada. Além do conceito de dado pessoal já mencionado inicialmente, o Decreto 8.771 de 2016, que regulamenta o Marco Civil da Internet trouxe uma definição no seu art. 14, inciso I:

> Art. 14, Para os fins do disposto neste Decreto, considera-se:
> I - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa"[47]

Verifica-se que o conceito trazido pelas legislações citadas traduz uma definição expansionista do dado pessoal, pois será considerado como tal toda a informação que possa identificar a pessoa de forma direta ou indireta, ou seja, será considerada qualquer informação que tenha o potencial de identificar o indivíduo de algum modo. Bioni explica que essa definição alargada decorre da falibilidade do processo de anonimização[48] dos dados.[49]

Ao observar a evolução do ordenamento jurídico, desde o reconhecimento do direito à intimidade de forma mais genérica e, após, a aclamação do reconhecimento à proteção dos dados pessoais como direito autônomo, é possível perceber que tal movimento decorreu da necessidade de adequação do sistema normativo a partir de novos hábitos da sociedade.

Destaca-se que mesmo antes da chamada sociedade tecnológica, com a invasão da internet, já havia o direito à proteção da intimidade e dos dados manipulados e armazenados de forma física. Aliás, para fins de proteção, atualmente independe o tipo de formato do dados pessoais, podendo ser físico ou digital.[50]

É certo que com a inserção das tecnologias da informação, houve uma aceleração no processo de produção de dados pessoais, o que reclamou a necessidade de estabelecer a sua definição como direito independente da intimidade (ainda que não seja desconexo a ela), merecedor de um sistema próprio de regulação, fiscalização e sanção.

---

47 BRASIL. Decreto nº 8.771, de 11 de maio de 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm. Acesso em 24 mai 2024.

48 Segundo o art. 5º, inciso XI da LGPD, a anonimização consiste na utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

49 BIONI, Bruno R. Proteção de Dados Pessoais - A Função e os Limites do Consentimento. Rio de Janeiro: Grupo GEN, 2021. E-book. ISBN 9788530994105. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994105/. Acesso em: 21 mai. 2024, p. 64.

50 BRASIL. [Constituição (1988)]. Emenda Constitucional n° 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#art1. Acesso em: 25 out 2024.

A respeito especificamente aos dados pessoais em formato digital, além da preocupação com a exposição dessas informações na internet para uso em atividades ilícitas por agentes maliciosos (como fraudes, extorsões e golpes em geral), constatou-se que o alto volume de dados pessoais passou a ser objeto de interesse de instituições privadas como objeto de captação de nichos mercadológicos.

A respeito desse novo cenário, Bioni faz uma análise do mecanismo existente na economia da informação, pelo qual os dados pessoais informados pelos usuários de internet são comercializados com a finalidade de realização de publicidade direcionada. Assim, ao acessar aplicativos de GPS, redes sociais, utilização de serviços gratuitos que exigem o fornecimento de dados pessoais do consumidor, há um fomento desse comércio de informações, muitas das vezes, sem que o usuário tome consciência dessa prática.[51]

> Os dados traduzem aspectos da personalidade e revelam comportamentos e preferências, permitindo até traçar um perfil psicológico dos indivíduos. Dessa maneira, podem-se detectar hábitos de consumo, que têm grande importância para a propaganda e o comércio. É possível, por meio dessas informações, produzir uma imagem total e pormenorizada da pessoa, que se poderia denominar de traços de personalidade, inclusive na esfera da intimidade. O cidadão converte-se no denominado “homem de cristal”.[52]

Essas informações categorizadas são matéria-prima para a geração de riqueza na economia da informação, tendo, pois, valor ativo no mercado. Ocorre que a disponibilização de informações na rede pode acarretar uma variedade de consequências incertas para o indivíduo, principalmente prejuízos financeiros, morais e de imagem.

As legislações surgidas pelo mundo estabeleceram direitos e garantidas aos cidadãos, bem como limites à utilização dos dados pessoais, que passaram a ser considerados mais relevantes para as sociedades. Além de prever uma proteção, as legislações também buscaram estabelecer hipóteses legais para o tratamento de dados, bem como a responsabilização pelos prejuízos decorrentes do tratamento irregular.[53]

---

51 BIONI, Bruno R. Proteção de Dados Pessoais - A Função e os Limites do Consentimento. Rio de Janeiro: Grupo GEN, 2021. E-book. ISBN 9788530994105. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994105/. Acesso em: 21 mai. 2024, p. 22

52 LIMBERGER, Têmis. O direito à Intimidade na Era da Informática: A necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.p. 58.

53. DONEDA, Danilo. Panorama histórico da proteção de dados pessoais In: DONEDA. Danilo et al (Coord). Tratado de Proteção de dados Pessoais. Rio de Janeiro: Forense, 2021. p. 4.

Tal movimento de criação de novos direitos, como é o caso da proteção de dados pessoais, decorre da necessidade de evolução do sistema jurídico a partir das mudanças sofridas pela sociedade. O direito deve ser dinâmico e não estático, sob pena de se tornar obsoleto. Refletir sobre as inovações que a tecnologia promoveu nas mais diversas relações sociais, comerciais, políticas, culturais e outras se torna primordial para que seja alcançada maior efetividade do respeito aos direitos fundamentais.

Como visto, o direito à intimidade integra o direito fundamental de personalidade. Este, por sua vez, deve ser garantido a todos os cidadãos porque representa também o respeito à dignidade da pessoa humana, princípio basilar para o alcance do Estado Democrático de Direito. Ao lado desses direitos, encontra-se a proteção dos dados pessoais, compreendido hoje como um direito autônomo que, por sua vez, decorre do exercício do direito à intimidade.

Ao longo da evolução da sociedade digital a partir do avanço de novas tecnologias, o direito à proteção de dados passou a receber cada vez mais atenção, não somente nas legislações infraconstitucionais citadas, mas alcançou destaque na própria Constituição Federal. Como parte deste avanço, o direito à proteção de dados pessoais subiu mais um degrau no ordenamento e passou a integrar a categoria de direito fundamental, conforme será abordado adiante.

2.4 Proteção de dados como direito humano e fundamental.

A proteção de dados pessoais, inclusive nos meios digitais, foi incorporada ao rol dos direitos e garantias fundamentais previstos no art. 5º da Constituição Federal por meio da Emenda Constitucional n.º 115, de 10 de fevereiro de 2022. Ainda foi estabelecida a competência da União para fiscalizar e organizar a proteção e o tratamento de dados pessoais, nos termos da lei (art. 21, inciso XXVI), bem como a competência privativa para legislar sobre esses mesmos temas (art. 22, inciso XXX).[54]

54 BRASIL. [Constituição (1988)]. Emenda Constitucional n° 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#art1. Acesso em: 21 jul. 2023.

Contudo, antes mesmo desta previsão expressa na Carta Maior, já era possível encontrar estudos nos quais se defendia o status da proteção de dados como direito fundamental e humano implícito.[55]

Ingo Sarlet contribuiu com importantes ensinamentos a respeito dos fundamentos filosóficos para justificar a existência de um direito fundamental implícito (à época) à proteção de dados pessoais com base nas teorias do reconhecimento de Hegel, Honneth e Solove. Em suas considerações, o professor já defendia o reconhecimento do direito fundamental à proteção de dados pessoais como desdobramento do direito ao livre desenvolvimento e determinação da personalidade.[56]

Em 1983, o Tribunal Constitucional Alemão exerceu grande contribuição na atualização da interpretação das garantias fundamentais para adequação à nova realidade trazida pelas inovações tecnológicas. No julgamento de ação que questionava uma lei que regeu o censo do país no ano de 1982, o Tribunal reconheceu o direito à autodeterminação informativa como o direito de controlar a divulgação e utilização de informações relacionadas à personalidade. O novo cenário de processamento de dados exigia uma readequação da visão de alguns direitos fundamentais, entre eles a privacidade[57]

Pinãr Manãs relaciona a proteção de dados com outros direitos, de modo que aquele permite tornar outros direitos e liberdades mais efetivos, seja direta ou indiretamente:

> [...] Em efecto, siendo com es um derecho fundamental, es asimismo requisito para que otras libertates sean respetadas. Impide (debería impedir) que la información disponible sobre las personas pueda ser utilizada em contra de sus derechos y libertades. El mal uso de los datos pernosales puede traer como consecuencia la restricción ilegítima de derechos tales como el de libertad de circulación, libertad religiosa, libertad de sindicación, acceso a funciones públicas, el derecho al trabajo. Son muchos los supoestos reales que se han producido em este sentido, com el agravante, además, de que la violación del derecho a la protección de datos puede passar inicialmente (o constantemente) desapercibida para su titular, de modo que no puede

55 SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: DONEDA, Danilo et al (Coord). Tratado de Proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p. 24 e ss.

56 SARLET, Ingo Wolfgang; SAAVEDRA, Giovani Agostini. Fundamentos jusfilosóficos e âmbito de proteção do direito fundamental à proteção de dados pessoais. Revista Direito Público. Brasília, 2020 .Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://meriva.pucrs.br/dspace/bitstream/10923/18861/2/Fundamentos_Jusfilosficos_e_mbito_de_Proteo_do_Direito_Fundamental_Proteo_de_Dados_Pessoais.pdf

57 DONEDA, Danilo. Panorama histórico da proteção de dados pessoais In: DONEDA. Danilo et al (Coord). Tratado de Proteção de dados Pessoais. Rio de Janeiro: Forense, 2021.p. 9

> identificar el motivo por el que se producem consecuencias negativas em la esfera de sus derechos.[58]

Quanto ao caráter de direito humano, Ingo Sarlet ensina que essa espécie de direito se refere àqueles que estão previstos no âmbito de tratados internacionais, “tendo como titulares todas as pessoas em todos os lugares, ou seja, titularidade universal, com vigência, validade e eficácia sempre condicionadas à ratificação dos tratados por um número significativo de Estados”. Nesse sentido, há uma intenção de promover uma universalidade desses direitos.[59]

O Pacto Internacional de Direitos Civis e Políticos, recepcionado pelo Decreto n.º 592, de 06 de julho de 1992, estabelece em seu preâmbulo o reconhecimento da “dignidade inerente a todos os seres humanos e de seus direitos iguais e inalienáveis constituem o fundamento da liberdade, justiça e paz no mundo”. Por sua vez, o artigo 17 determina o direito à proteção do ser humano contra ingerências arbitrárias ou ilegais na vida privada, na família, no domicílio e correspondências. Do mesmo modo prevê a proteção contra ofensas ilegais contra a sua honra e reputação. [60]

Em uma análise do sistema internacional, a Comissão da Organização das Nações Unidas – ONU tem considerado o direito à proteção de dados pessoais como decorrente do direito à privacidade, em que pese não coincidirem, como pode ser constatado nos documentos da ONU e da União Europeia, a exemplo do Pacto Internacional de Direitos Civis e Políticos e a Convenção Europeia.

O *status* de direito fundamental da proteção de dados pessoais está atrelado ao caráter de direito humano pela análise do seu fundamento de natureza material, quanto à relevância do seu conteúdo para o sistema jurídico. Dito de outro modo, a natureza de direito humano pode ser constatada quando for possível relacionar a proteção de dados com diversos princípios e direitos, como dignidade da pessoa humana, da personalidade, da privacidade e da livre autodeterminação informativa. [61]

Pelo exposto, mostra-se necessário colocar o direito a proteção de dados pessoais como peça chave do Estado Democrático de Direito, uma vez que se tornou

---

58 PIÑAR MAÑAS, José Luis. Seguridad, transparencia y protección de datos: el futuro de um necessário e incierto equilíbrio. V. 147. Madrid: Documentos de trabaljo (Laboratorio de alternativas). Fundación Alternativas, 2009. Disponível em: https://fundacionalternativas.org/publicaciones/seguridad-transparencia-y-proteccion-de-datos-el-futuro-de-un-necesario-e-incierto-equilibrio/. Acesso em 11 jun. 2024. p. 12

59 SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: DONEDA, Danilo et al (Coord). Tratado de Proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p. 28.

60 BRASIL. Decreto n.º 592, de 06 de julho de 1992. Disponível em: https://legislacao.presidencia.gov.br/atos/?tipo=DEC&numero=592&ano=1992&ato=2dco3YE10MFpWTf3e. Acesso em 11 jun. 2024.

61 Ibid. p. 29 e 30.

essencial para o desenvolvimento efetivo de outros direitos, com destaque à dignidade humana.[62]

Segundo Jürgen Habermas, há uma conexão entre a noção moral de dignidade humana e a concepção jurídica dos direitos humanos. Para o filósofo e sociólogo alemão, a dignidade representa um portal pelo qual se importa para o direito um conteúdo universal e igualitário da moral. Em sua concepção, dignidade humana é a fonte da qual derivam todos os direitos básicos, sendo considerada a chave para sustentar a indivisibilidade de todas as gerações de direitos humanos[63]

A dignidade humana desempenha a função de um sismógrafo, que registra o que é constitutivo de uma ordem democrática legal, qual seja: aqueles direitos que os cidadãos de uma comunidade política devem conceder-se a si mesmos, se são capazes de se respeitarem como membros livres e iguais de uma sociedade. Ou seja, por meio da garantia dos direitos humanos, os cidadãos podem exigir o respeito à sua dignidade humana.[64]

Por tais razões, considerando a natureza de direito humano e fundamental da proteção de dados pessoais na sociedade atual e, principalmente pela sua importância para o exercício de outros direitos fundamentais, a discussão sobre a responsabilidade pelo tratamento indevido ou vazamento de dados pessoais torna-se cada vez mais pertinente. Analisar as legislações existentes e suas repercussões na prática pode fornecer importantes contribuições para o aprimoramento do sistema jurídico existente.

Antes de adentrar ao foco do tema proposto quanto à discussão sobre a responsabilidade pelas violações dos dados pessoais, propõe-se a seguir uma breve reflexão sobre os princípios previstos na LGPD no sistema de proteção de dados pessoais. Não se pretende esgotar ou aprofundar o estudo sobre esta base conceitual, mas promover uma melhor compreensão sistemática da matéria, de modo a viabilizar o alcance dos objetivos apresentados alhures.

62 PIÑAR MAÑAS, José Luis. Seguridad, transparencia y protección de datos: el futuro de um necessário e incierto equilíbrio. V. 147. Madrid: Documentos de trabaljo (Laboratorio de alternativas). Fundación Alternativas, 2009. Disponível em: https://fundacionalternativas.org/publicaciones/seguridad-transparencia-y-proteccion-de-datos-el-futuro-de-un-necesario-e-incierto-equilibrio/. Acesso em 11 jun. 2024. p. 58

63 HABERMAS, Jürgen. El concepto de dignidad humana y la utopia realista de los derechos humanos. Diánoia, v. LV, n. 64, p. 3–25, maio 2010. p.03.

64 Ibid. p.10.

2.5 Princípios aplicados à proteção de dados segundo a LGPD.

A Lei Geral de Proteção de Dados foi inspirada em legislações internacionais, especialmente no Regulamento Geral de Proteção de Dados da União Europeia. A referida lei estabelece diversos princípios fundamentais que devem conduzir o tratamento de dados pessoais no Brasil.[65]

A exemplo de outras legislações, a LGPD apresentou uma estrutura principiológica como parte fundamental da política nacional de proteção de dados pessoais. Por meio dessas premissas, houve uma preocupação em promover uma postura preventiva e educativa por parte dos entes públicos e privados. Nesse sentido, em seu artigo 6º, a LGPD estabelece que o tratamento de dados deve observar a boa-fé e os princípios da finalidade, adequação, necessidade, livre acesso, transparência, segurança, prevenção, não discriminação, responsabilidade e prestação de contas. A seguir serão apresentadas brevemente as características principais de cada princípio[66]

O princípio da finalidade determina que os dados pessoais devem ser coletados para propósitos legítimos e específicos e não podem ser utilizados de forma incompatível com esses objetivos. Este princípio possui papel primordial no sistema de proteção dos dados pessoais, tendo em vista que tem como preocupação evitar o desvio de finalidade no uso dos dados pessoais.

Por sua vez, o princípio da adequação estabelece que os dados devem ser relevantes, proporcionais e limitados para alcançar as finalidades pretendidas. Pelo princípio da necessidade, o tratamento de dados deve ser limitado ao mínimo necessário para o alcance de sua finalidade. Assim, por esse princípio, deve ser observada a proporcionalidade em relação ao tratamento para não exceder ao objetivo que o fundamentou.[67]

O princípio da transparência determina o dever das organizações de informar de forma clara e acessível aos titulares sobre o tratamento de seus dados e os seus agentes. Em relação ao princípio da segurança, o art. 6º, inciso VII estabelece a obrigatoriedade de adoção das medidas técnicas e administrativas necessárias para garantir a proteção dos dados pessoais de acessos não autorizados, de atos ilícitos

65 BRASIL. Lei Federal n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Disponível em http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 21 de jul. 2023.

66 Ibid.

67 Ibid.

ou acidentes que acarretem a destruição, perda, alteração ou difusão das informações. Relacionado à segurança, o princípio da prevenção consiste na implementação por parte dos agentes de tratamento de medidas aptas a prevenir danos decorrentes do tratamento de dados pessoais.[68]

O princípio da não discriminação estabelece que o tratamento de dados pessoais não pode ser utilizado para fins discriminatórios ilícitos ou abusivos. O último princípio previsto no art. 6º da mesma lei consiste na comprovação pelo agente de tratamento da adoção de medidas eficazes que demonstrem o cumprimento de todas as normas vigentes sobre proteção de dados pessoais.

Em que pese a alta relevância de todos os princípios elencados na LGPD, como recorte para o estudo proposto, o princípio da segurança se mostra em destaque, em razão da maneira como ele deverá observado e alcançado. Para isso, a LGPD estabelece no Capítulo VI as atribuições dos agentes de tratamento e disciplina a responsabilidade dessas figuras em face do tratamento irregular de dados pessoais, bem como prevê a reparação de danos decorrentes de sua violação.[69]

Quanto à definição a respeito da violação dos dados pessoais, a própria lei em referência apresenta o conceito de tratamento irregular no seu art. 44, que consiste nas hipóteses em que os agentes de tratamento deixarem de observar a legislação ou quando não oferecerem a segurança esperada.[70]

Ressalte-se que o dever de segurança foi previsto antes da LGPD pelo Código de Defesa do Consumidor, em seu art. 4º, consistindo em um dos objetivos da Política Nacional das Relações de Consumo. O complexo conjunto de direitos previstos aos consumidores reflete a sua hipervulnerabilidade em relação aos fornecedores de produtos e serviços no tocante ao dever de informação e na responsabilidade pela coleta de dados pessoais em suas diversas atividades.[71]

Nesse aspecto, destaca-se o dever de fornecimento das informações de maneira ampla e especializada, principalmente no tocante aos riscos envolvidos no

---

68 BRASIL. Lei Federal n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Disponível em http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 21 de jul. 2023.

69 Ibid.

70 Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado. Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano. BRASIL. Lei Federal n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Disponível em http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 21 de jul. 2023.

71 MENKE, Fabiano; GOULART, Guilherne Damasio. Segurança da Informação e vazamento de dados. In: DONEDA, Danilo et al (coord). Tratado de Proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p. 342.

tratamento de dados pessoais. Diretamente atrelada a essas disposições localizadas na LGPD e no CDC, encontra-se a boa-fé objetiva como um princípio da proteção de dados.

A função da boa-fé está refletida na constituição dos deveres anexos e de proteção dos contratos. Sua importância reside principalmente no fato de que, na maioria das vezes, o tratamento de dados pessoais não consiste no objeto principal da prestação de um serviço ou no fornecimento de um produto. Assim, a observância desse princípio constitui um fundamento ético para o exercício das atividades por parte das instituições e na promoção da confiança do consumidor/usuário em suas relações.[72]

Merece destaque, ainda, o dever de informação como parte do dever de proteção dos dados pessoais. Aquele pode ser considerado como decorrente do princípio da boa-fé objetiva.

Desse modo, o dever de informação, a boa-fé objetiva, a segurança, além de todos os demais princípios já mencionados, precisam ser observados antes, durante e após o término do contrato, ainda que não estejam previstos expressamente na contratação do produto ou serviço. Assim, mesmo após o término da obrigação principal contratada, os agentes de tratamentos ainda serão responsáveis pelo armazenamento e eliminação dos dados coletados.[73]

Conforme ensina Piñar Manãs, a alegação de desconhecimento ou a violação dos princípios do sistema de proteção dos dados pessoais implica na violação e desconhecimento do próprio direito mencionado:

> Esa consideración del derecho fundamental a la protección de datos explica y justifica el contenido de los principios que configuran su núcleo esencial. Tales principios, cuya violación o desconocimiento implica la violación o desconocimiento del derecho, pueden reconducirse a los siguientes: consentimiento, información, finalidad, calidad de los datos (con especial referencia a la proporcionalidad), seguridad y cont rol independiente. Principios a los que pueden añadirse los de utilización leal de los datos y minimización en el uso de los mismos (éste, por cierto, reconducible también, en mi opinión, al de proporcionalidad). Principios que para ser efectivos

72 MENKE, Fabiano; GOULART, Guilherne Damasio. Segurança da Informação e vazamento de dados. In: DONEDA, Danilo et al (Coord). Tratado de Proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p. 342.

73 Ibid. p. 343

> requieren el reconocimiento, garantía y tutela de los derechos de acceso, rectificación, cancelación y oposición [...].[74]

Constata-se, pois, que os princípios basilares mencionados possuem o condão de envolver os dados pessoais de garantias da forma mais ampla possível, de modo que sejam evitadas exposições que possam atingir também outros direitos fundamentais de grande relevância, como a personalidade e a própria dignidade da pessoa humana.

Além de estabelecer a política de proteção de dados, a LGPD determinou a criação do órgão responsável pelo cumprimento das regras aplicadas ao tema, bem como para fiscalizar e aplicar as sanções cabíveis. Com efeito, não se pode deixar de abordar sobre esta entidade em razão de sua importância para compreender a realidade nacional do processo de fiscalização e responsabilização dos agentes de tratamento em face da violação dos dados pessoais.

2.6 Autoridade Nacional de Proteção de Dados

A análise da criação e atuação da Autoridade Nacional de Proteção de Dados – ANPD se tornou primordial para o desenvolvimento do presente estudo, tendo em vista que foi preciso refletir e contextualizar o percurso da autarquia desde o seu surgimento e ao longo de sua atuação até hoje, a fim de que não sejam realizadas conclusões equivocadas sobre a efetivação da fiscalização e aplicação de sanções administrativas em face da violação de dados pessoais.

Em que pese ser uma lei relativamente recente, a LGPD sofreu modificações relevantes. A Lei n.º 13.709, de 14 de agosto de 2018 foi alterada pela Medida Provisória n. 869, de 27 de dezembro de 2018, para inserir a sua definição como Lei Geral de Proteção de Dados Pessoais e criar a ANPD, órgão da administração direta, integrante da Presidência da República. Posteriormente, a referida MP foi convertida na Lei n.º 13.853, de 08 de julho de 2019[75], a qual inseriu a possibilidade do órgão ser transformado em autarquia de natureza especial em até dois anos.

---

74 MANÃS, Piñar. Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilíbrio. Documento de trabajo n.º 147. Madrid: Fundación Alternativas, 2009. Disponível em https://fundacionalternativas.org/publicaciones/?tipos=Documento%20de%20trabajo&palabras=protecci%C3%B3n%20datos. Acesso em 18 jun. 2024.

75 BRASIL. Lei Federal n. 13.853, de 08 de julho de 2019.Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm. Acesso em 23 jul.2024.

Por sua vez, o Decreto 10.474[76], de 26 de agosto de 2020 estabeleceu a estrutura regimental da ANPD, quando então a entidade iniciou as suas atividades. Somente no ano de 2021 a ANPD publicou o primeiro Regimento Interno e a primeira agenda regulatória para execução naquele ano e no seguinte. Em agosto de 2021, os artigos da LGPD que tratam da fiscalização e aplicação das sanções entraram em vigor.

Em 2022, a Lei 14.460[77], de 25 de outubro converteu a MP n.º 1.124, de 13 de junho para alterar a natureza jurídica da ANPD, a qual foi transformada em autarquia de natureza especial. Por meio da edição da MP n.º 1.154 de 1º de janeiro de 2023, convertida na Lei n.º14.600[78], de 19 de junho de 2023, o Ministério da Justiça e Segurança Pública passou a deter a competência para tratamento de dados pessoais. Como consequência, a ANPD sofreu nova alteração por meio do Decreto 11.348[79] de 01º de janeiro de 2023, para que fosse finalmente vinculada ao Ministério da Justiça e Segurança Pública.

A ANPD, dentre outras atribuições, possui a responsabilidade de fiscalizar e aplicar as sanções após a deflagração de processo administrativo, sendo garantidos aos responsáveis pela violação, o contraditório, ampla defesa e direito a recurso da decisão sancionadora. O órgão também possui como atribuição construir uma política de proteção de dados que balizará a criação de códigos internos de conduta por parte das organizações.[80]

Além disso, desde o início de suas atividades, a ANPD atua de maneira significativa em sua finalidade preventiva, por meio da publicação de diversas resoluções, guias orientativos e enunciados, com o objetivo de facilitar a instrução da sociedade e agentes de tratamento de dados pessoais sobre o cumprimento das normas e requisitos previstos na LGPD.[81]

---

76 BRASIL. Decreto n.º 10.474, de 26 de agosto de 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10474.htm. Acesso em: 23 de jul 2024.

77 BRASIL. Lei Federal n.º 14.460, de 25 de outubro de 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Lei/L14460.htm. Acesso em 23 de jul. 2024.

78 BRASIL. Lei Federal n.º 14.600, de 19 de junho de 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Lei/L14460.htm. Acesso em 23 de jul 2024.

79 BRASIL. Decreto n.º 11.348 de 01º de janeiro de 2023. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11348.htm. Acesso em 23 de jul 2024.

80 BRASIL. Lei Federal n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Disponível em http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 21 de jul. 2023., arts 55-A e. 55-J, inciso IV.

81 ANDP. Balanço 3 anos. Brasília, 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/anpd_balanco_tres_anos.pdf. Acesso em 23 de jul 2024. p 11.

Como mencionado anteriormente, a autarquia possui competência para promover orientação à sociedade com o objetivo de prevenir a violação dos dados pessoais. Além disso, suas atribuições incluem a atuação repressiva para promover a fiscalização, apuração e aplicação das sanções cabíveis. Por sua vez, as sanções administrativas que podem ser aplicadas, mais do que alcançar a finalidade punitiva, possuem a função de garantir a conformidade do tratamento de dados com as diretrizes estabelecidas pela LGPD, de modo a proteger os direitos dos titulares de dados pessoais. As penalidades devem ser calculadas com base em diversos critérios, incluindo a gravidade da violação, o porte econômico da organização, o alcance e a sensibilidade dos dados envolvidos, entre outros fatores.[82]

A ANPD pode tomar conhecimento de irregularidades no tratamento de dados por meio de denúncias ou petição do próprio titular de dados pessoais. A LGPD ainda prevê a obrigatoriedade dos agentes de tratamento realizarem a comunicação de incidentes de segurança[83] que possam causar riscos ou danos aos titulares.

A autarquia ainda pode estabelecer outras medidas corretivas, como a obrigatoriedade de adoção de políticas e procedimentos de segurança de dados, realizar auditorias de conformidade ou promover programas de educação e treinamento em proteção de dados.

Como foi possível constatar, a ANPD possui poucos anos de efetivo exercício de suas atribuições e ainda passa por algumas dificuldades estruturais, como a insuficiência de quadro de profissionais. A autarquia ainda não realizou concurso público para formação de quadro próprio, sendo que atualmente parte da equipe é composta de servidores lotados na ANPD por meio de requisições feitas a órgãos federais e outros por meio de recrutamento para ocupação de cargo comissionado executivo e de função comissionada executiva.[84]

O último relatório de monitoramento publicado referente ao primeiro semestre de 2023 aponta ainda outras dificuldades vividas pela autarquia, como a necessidade de adoção de sistemas apropriados para recebimento de requerimentos e emissão de

82 ANDP. Resolução CD/ANDP n.º 4, de 24 de fevereiro de 2023. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077. Acesso em 23 de jul 2024.

83 Incidente de segurança é um evento adverso confirmado que comprometa a confidencialidade, integridade ou disponibilidade de dados pessoais. Pode decorrer de ações voluntárias ou acidentais que resultem em divulgação, alteração, perda ou acesso não autorizado a dados pessoais, independentemente do meio em que estão armazenados. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANDP). Comunicação de incidente de segurança. Brasília, 2022. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acesso em 23 de jul 2024.

84 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANDP). Relatório de Ciclo de Monitoramento. 1º semestre de 2023. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/remuneracao-e-subsidios-de-servidores-e-empregados-publicos. Acesso em 23 de jul 2024.

relatórios, necessidade de conclusão de processos de fiscalização ainda em andamento para que seja determinada a adequação dos agentes de tratamento; necessidade de mapeamento de fluxos e simplificação de processos e de ações de auditoria, capacitação de servidores, dentre outros. [85]

Os aprimoramentos apontados podem ser naturalmente esperados para uma entidade criada recentemente, sobretudo quando são analisados os números de processos instaurados e concluídos. Os referidos dados serão oportunamente apresentados mais à frente do presente estudo, ocasião em que serão analisadas as sanções atualmente previstas pela LGPD e aplicadas pela autarquia.

2.7 Tratamento de dados e seus agentes

A fim de complementar a compreensão do sistema de proteção de dados vigente no Brasil, importa abordar sobre a definição de tratamento de dados, tendo em vista que as violações referidas decorrem em grande parte da falha das instituições na gestão dos dados pessoais. A LGPD elenca o seu conceito no art. 5º, inciso X:[86]

> Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

Como se pode entender pela definição acima, o tratamento dos dados pessoais engloba todo a manuseio dessas informações, desde a sua coleta, utilização até à sua guarda. Por sua vez, o art. 7º prevê as hipóteses permitidas para o tratamento de dados e a forma de sua realização, exigindo o consentimento expresso do titular[87]. A lei ainda destaca que o tratamento de dados deve obedecer aos

85 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANDP). Relatório de Ciclo de Monitoramento. 1º semestre de 2023. Brasília, 2023.Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/remuneracao-e-subsidios-de-servidores-e-empregados-publicos. Acesso em 23 de jul 2024. p. 46.

86 BRASIL. Lei Federal n. 13.709, de 14 de agosto de 2018. Disponível em http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 21 de jul. 2023.

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

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

princípios mencionados anteriormente, como a finalidade, boa-fé e o interesse público que justificam sua disponibilização.[88]

Além de estabelecer as hipóteses permitidas, a LGPD ainda prevê quando o tratamento de dados pessoais será considerado irregular, ou seja, quando deixar de observar as normas legais ou quando deixar de oferecer a segurança esperada. A configuração do tratamento irregular dependerá de determinadas circunstâncias, como o modo de sua realização, o resultado e os riscos esperados, entre outros.[89]

Compreendidas as hipóteses autorizadas para o tratamento de dados, bem como das que se enquadram como tratamento irregular, importa estudar a respeito dos responsáveis pela gestão dos dados pessoais no âmbito das organizações, denominados agentes de tratamento. A LGPD define duas figuras, o controlador e o operador. O primeiro pode ser uma pessoa natural ou jurídica de direito público ou privado responsável pela tomada de decisões a respeito do tratamento de dados. O operador, por sua vez, pode ser uma pessoa natural ou jurídica de direito público ou privado que realiza o tratamento de dados em nome do controlador.[90]

O art. 38, parágrafo único, da LGPD determina a obrigatoriedade do controlador fornecer à ANPD relatório de impacto à proteção de dados pessoais, com a descrição das operações de tratamento de dados, dos tipos de dados coletados, metodologia utilizada para a coleta e para a garantia das informações. O controlador também deverá informar à autarquia a sua análise em relação a adoção de medidas, salvaguardas e mecanismos de mitigação de risco implementadas.

Entre os deveres que a lei determina ao controlador, está a comunicação à ANPD e ao titular dos dados pessoais a ocorrência de incidente de segurança que

---

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem)

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária

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

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. Ibid.

88 Ibid.

89 Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

I - o modo pelo qual é realizado;

II - o resultado e os riscos que razoavelmente dele se esperam;

III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano. Ibid.

90 Art. 5º, incisos VI, VII e IX da LGPD. BRASIL. Lei federal n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Disponível em http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 21 de jul. 2023.

possa acarretar risco ou danos. De acordo com a gravidade do incidente, poderá ser exigida a comprovação da adoção de medidas técnicas capazes de tornar os dados afetados de forma ininteligível.[91]

A respeito dos agentes de tratamento, a ANPD publicou o Guia Orientativo para definições do controlador, operador e do encarregado.[92] Segundo o documento, o controlador, além de tomar as principais decisões a respeito do tratamento de dados, será responsável por definir a sua finalidade, natureza dos dados a serem tratados, prazo de duração do tratamento, além de outras circunstâncias.

A respeito da identificação do controlador, o guia esclarece:

> A identificação do controlador deve partir do conceito legal e dos parâmetros auxiliares indicados neste Guia, sempre considerando o contexto fático e as circunstâncias relevantes do caso. **O papel de controlador pode decorrer expressamente de obrigações estipuladas em instrumentos legais e regulamentares ou em contrato firmado entre as partes. Não obstante, a efetiva atividade desempenhada por uma organização pode se distanciar do que estabelecem as disposições jurídicas formais, razão pela qual é de suma importância avaliar se o suposto controlador é, de fato, o responsável pelas principais decisões relativas ao tratamento**. (grifo nosso)[93]

O Guia ainda informa que não são controladoras as pessoas naturais que estão subordinadas à organização ou membros de seus órgãos, como sócios, administradores, servidores, sendo que a definição legal dessa figura consiste em um "comando legal que atribui obrigações específicas à pessoa jurídica, de modo que esta assume a responsabilidade pelos atos praticados por seus agentes e prepostos em face dos titulares e da ANPD".[94]

No entanto, tal conclusão apresentada merece uma ressalva, uma vez que o controlador como pessoa jurídica será representado por uma ou mais pessoas naturais que devem responder pelas atividades da empresa. O dirigente não pode ser eliminado do processo de identificação da responsabilidade por eventuais

91 Lei federal n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Disponível em http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 24 de out. 2024.

92 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado. Brasília, 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf. Acesso em 20/07/2023.

93 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado, 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf. Acesso em 20/07/2023.p 8.

94 Ibid.p. 9.

inobservâncias das normas previstas na LGPD e em outras leis que podem regulamentar o tratamento de dados pessoais.

Portanto, o controlador de dados pessoais será aquele que detém o poder de decisão e direção sobre todo o processo de tratamento de dados, desde a concepção do produto ou serviço, ao longo da execução e, ainda, após a sua finalização.

Cabe destacar que a LGPD fez previsão expressa de equiparação entre o operador e o controlador. Aquele pode responder solidariamente pelos danos causados nas hipóteses de descumprimento das suas obrigações legais ou quando não seguir as instruções lícitas do controlador.[95]

A LGPD, com redação alterada pela Lei n.º 13.853, de 2019, ainda inseriu a figura do encarregado (art. 5º, inciso VIII), que consiste na "*pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)*".[96]

O art. 41, § 2º da LGPD estabelece as atividades do encarregado: a) aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; b) receber comunicações da autoridade nacional e adotar providências; c) orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e d) executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. Ainda destaca-se que normas complementares poderão ser estabelecidas pela Autoridade de Proteção de Dados sobre a definição e atribuição do encarregado.[97]

Realizada a análise sobre os agentes de tratamento e suas atribuições, a afirmação pela eventual responsabilização pelo tratamento indevido ou ilícito de dados pessoais dependerá da análise concreta das suas condutas e decisões para a verificação de eventual responsabilidade. Tais considerações serão primordiais para o desenvolvimento do estudo proposto neste trabalho.

---

95 Artigo 42, § 1º, I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei; BRASIL. Lei federal n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Disponível em http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 21 de jul. 2023.

96 Ibid.

97 Ibid. Art. 41.

2.8 Análise de dados sobre a aplicação da LGPD.

Conforme mencionado anteriormente, a LGPD foi publicada em 2018 e entrou em pleno vigor somente após dois anos. Decorridos quase quatro anos de existência, a ANPD tem cumprido as suas atribuições como órgão fiscalizador e sancionador em face das violações da proteção de dados pessoais. O assunto também não escapou ao Judiciário, que foi acionado para se posicionar quanto à aplicação da referida lei em diversas temáticas.

A LGPD estabeleceu a responsabilidade do controlador e do operador pelos danos decorrentes do tratamento irregular de dados, seja na esfera patrimonial, moral, individual ou coletiva. A lei estabelece, ainda, a responsabilidade entre os controladores que estiverem diretamente ligados ao tratamento irregular, bem como o operador. [98]

Segundo a legislação citada, o tratamento será considerado irregular quando não fornecer a segurança esperada pelo titular dos dados, considerando circunstâncias relevantes, como: a) o modo pelo qual é realizado; b) o resultado e os riscos que razoavelmente dele se esperam; c) as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.[99]

O art. 52 do mesmo diploma define as sanções aplicáveis após procedimento instaurado pela ANPD, quais sejam: advertência, multa de até 2% (dois por cento) do faturamento da pessoa jurídica, limitada a R$50.000.000,00 (cinquenta milhões de reais) por infração, multa diária, publicização da infração, bloqueio dos dados atingidos pela infração, eliminação de dados, suspensão parcial do funcionamento do banco de dados, suspensão do exercício de atividade de tratamento dos dados pessoais pelo prazo máximo de seis meses e proibição parcial ou total de tratamento de dados.

Após o início das suas atividades, a ANPD apresentou dois relatórios de Ciclo de Monitoramento, o primeiro referente ao ano de 2022 e o segundo relativo ao primeiro semestre de 2023. No ano de 2022, a autarquia recebeu 1.045 (mil e quarenta e cinco) requerimentos entre denúncias e petições de titulares.

98Art. 42 da LGPD. BRASIL. Lei federal n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Disponível em http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 21 de jul. 2023.

99 Ibid. Art. 44 da LGPD..

De acordo com dados fornecidos pela autarquia no Relatório de Ciclo de Monitoramento do primeiro semestre de 2023, a Coordenação Geral de Fiscalização – CGF - recebeu 496 (quatrocentos e noventa e seis) requerimentos, sendo 167 (cento e sessenta e sete) petições de titulares e 329 (trezentos e vinte e nove) denúncias. Consta no relatório que do total mencionado, foram instaurados apenas dois processos de fiscalização e um processo administrativo sancionador por violações à LGPD.[100]

O relatório ainda menciona que 43% (quarenta e três por cento) das petições de titulares não foram analisadas por ausência do cumprimento dos requisitos para o seu recebimento e/ou por se tratar de questão que não abrange a competência da ANPD. Outro dado relevante refere-se às respostas de pedido de manifestação dos controladores. Das 91 (noventa e uma) requisições encaminhadas, 25,2% (vinte e cinco, vírgula dois por cento) não foram respondidas com as informações solicitadas pela Autoridade.

Reunidos os números de 2022[101] e 2023, o total foi de 09 (nove) processos sancionadores dentre os quais somente um foi finalizado com aplicação de multa simples e advertência. Os demais ainda aguardavam decisão terminativa até o fechamento do relatório.

Consta do Balanço dos três anos da ANPD, que após a publicação da norma sobre dosimetria das sanções[102], a autoridade emitiu sanção em outros dois processos administrativos sancionadores em face de agentes públicos e privados e sete processos encontravam-se ainda em fase de análise.

No sítio da ANPD atualizado em julho de 2024, foram apresentados os números de comunicados de incidentes de segurança recebidos. No ano de 2023, foram 352 (trezentos e cinquenta e dois) e até junho de 2024, foram recebidos 152 (cento e cinquenta e dois) comunicados. O acumulado de todo o período desde 2021 soma 965 (novecentos e sessenta e cinco) comunicados.[103] Quanto aos requerimentos

100BRASIL. ANDP. Relatório de Ciclo de Monitoramento. 1º semestre de 2023. Acesso em 14.05.2023. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/2023-11-07-relatorio-do-ciclo-de-monitoramento-2023-versao-final.pdf

101BRASIL. ANDP. Relatório de Ciclo de Monitoramento de 2022. Acesso em 14.05.2023. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.gov.br/anpd/pt-br/assuntos/noticias/2023-08-17-relatorio-do-ciclo-de-monitoramento-2022.pdf

102 BRASIL. ANDP. Resolução CD/ANDP n.º 4, de 24 de fevereiro de 2023. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077. Acesso em 23 de jul 2024.

103 BRASIL. ANDP. Números da fiscalização. Disponível em https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao. Acesso em 23 de jul 2024.

recebidos pela ANPD, em 2023 foram 1.138 (mil cento e trinta e oito). Por sua vez, até junho de 2024, foram 615 (seiscentos e quinze) ocorrências.

Em comparação, a Agência Espanhola de Proteção de Dados – AEPD, que completou 30 anos de existência, recebeu 21.590 (vinte e uma mil quinhentos e noventa) reclamações em 2023, com aumento de 43% (quarenta e três por cento) em relação ao ano anterior. Do total de reclamações recebidas, 20.391 (vinte mil trezentos e noventa e uma) foram resolvidas no mesmo ano, com uma taxa de 94% (noventa e quatro por cento) de efetividade.[104] Deste total de reclamações, 492 (quatrocentos e noventa e duas) foram concluídas com procedimento sancionador.[105]

Da análise dos números acima apresentados, em que pese a evolução das normas de proteção dos dados pessoais no Brasil, a realidade da estatística fornecida pelos Relatórios indica uma baixa efetividade na fiscalização e conclusão dos procedimentos sancionadores. O documento apresenta as justificativas sobre a atuação no período analisado e indica diversas causas, como a falta de sistema informatizado próprio para recebimento e processamento dos requerimentos, a escassez de recursos humanos para a análise dos processos de fiscalização e repressão de infrações, entre outras.

Em razão das dificuldades relatadas pela ANPD, os requerimentos de titulares e denúncias recebidos no primeiro semestre de 2023 não haviam sido analisados em sua totalidade. Ademais, a ausência de um canal simplificado para recebimento dos documentos dificultou o acesso pelos titulares dos dados pessoais. Outro ponto preocupante apontado pelo último relatório refere-se à indicação de criação de uma Comissão de Sansões Administrativas para que seja viabilizada a fixação das atribuições sancionatórias da ANPD.[106]

Conforme explanado, a autarquia possui como atribuição principal garantir a efetiva aplicação da LGPD, de modo a contribuir para o fortalecimento da confiança dos cidadãos nas organizações que tratam seus dados pessoais e para promover um ambiente de negócios seguro e transparente. Contudo, até o momento, a ANPD ainda não demonstrou uma atuação satisfatória no que tange aos procedimentos de

---

104 Do total apresentado, 13.791 (treze mil, setecentos e noventa e uma) reclamações não foram admitidas por ausência de requisitos de admissibilidade, principalmente por não apresentarem indícios da existência de uma infração de competência da AEPD. ESPANHA. AEPD. Memoria Anual 2023. Disponível em https://www.aepd.es/memorias/memoria-aepd-2023.pdf. Acesso em 23 de jul 2023. p. 132.

105 ESPANHA. AEPD. Memoria Anual 2023. Disponível em https://www.aepd.es/memorias/memoria-aepd-2023.pdf. Acesso em 23 de jul 2023. p. 131.

106 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANDP). Relatório de Ciclo de Monitoramento. 1º semestre de 2023. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/2023-11-07-relatorio-do-ciclo-de-monitoramento-2023-versao-final.pdf. Acesso em 14.05.2023.

responsabilização pelo tratamento irregular de dados pessoais bem como da conclusão dos processos sancionadores.

Não se pode deixar de salientar que, em razão do pouco tempo de existência e, considerando as dificuldades que ainda enfrenta, a ANPD vem cumprindo com efetividade seu papel de órgão orientador na promoção do conhecimento e educação da sociedade a respeito da LGPD, por meio da publicação de diversos instrumentos com o objetivo de conscientizar os titulares de dados pessoais dos seus direitos, bem como os agentes de tratamento em relação aos seus deveres.

No entanto, seu aperfeiçoamento se mostra necessário, tanto em relação ao aumento do corpo de servidores, quanto no investimento de sistemas para otimização dos seus fluxos de trabalho. Diante das diversas atribuições como órgão orientativo, normativo, fiscalizatório e sancionador, a ANPD necessita expandir sua atuação com efetividade, na medida em que se constata o aumento de violações dos dados pessoais.

Ao longo dos últimos anos, o Judiciário também foi chamado a se posicionar quanto à aplicação da LGPD no que tange ao descumprimento das normas de proteção de dados pessoais.

Aliás, um julgamento de grande repercussão nesta temática ocorreu após a publicação da LGPD e antes da sua entrada em vigor, qual seja, a Ação direta de inconstitucionalidade – ADI 6387, a qual discutiu a validade constitucional da MP 954/2020 sobre compartilhamento de dados dos usuários de serviço telefônico fixo e móvel pelas empresas de telefonia com Instituto Brasileiro de Geografia e Estatística-IBGE.[107]

A Medida Provisória n.º 954 publicada no dia 17 de abril de 2020 teve como objeto autorizar o fornecimento da relação de nomes, números de telefone e dos endereços dos clientes das empresas de telefonia ao IBGE para o fim de produção estatística oficial, “com o âmbito de realizar entrevistas de caráter não presencial no âmbito de pesquisas domiciliares”, durante a situação de emergência de saúde pública causada pela pandemia do COVID-19.[108]

---

107 BRASIL. Supremo Tribunal Federal. (Plenário). Ação Direta de Inconstitucionalidade n.º 6387. Relatora: Ministra Rosa Weber, 07 de maio de 2020. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur436273/false. Acesso em: 27 out 2024.

108 BRASIL. Medida provisória nº 954, de 17 de abril de 2020. Dispõe sobre compartilhamento de dados por empresas de telecomunicações durante a emergência de saúde pública. Brasília, DF: Presidência da República, 2020. Disponível em: https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/141619. Acesso em 27 out. 2024.

Os fundamentos apresentados pelo Conselho Federal da Ordem dos Advogados do Brasil, órgão que propôs a ADI,[109] incluíram a inconstitucionalidade formal, em razão do desrespeito aos requisitos constitucionais para a edição de Medida Provisória, bem como a alegação de inconstitucionalidade material, diante da violação dos direitos constitucionais da dignidade da pessoa humana, inviolabilidade da intimidade, da vida privada, da honra e imagem, do sigilo de dados e da autodeterminação informativa, conforme os artigos 1º, inciso III, artigo 5º, incisos X e XII, todos da Constituição da República.

O autor da ação alertou para a maneira genérica e imprecisa com a qual a MP 954/2020 apresentou a finalidade do compartilhamento de dados com o IBGE, com referência apenas sobre a realização de entrevistas domiciliares não presenciais durante o período da pandemia. A MP não apontava as especificidades sobre o objetivo das pesquisas, bem como a modalidade de sua execução. Além desses questionamentos, foi levantada a ausência das razões que justificassem a necessidade do compartilhamento dos dados para a pesquisa.[110]

O julgamento da medida cautelar de relatoria da Ministra Rosa Weber e referendado pelo plenário do Supremo Tribunal Federal, suspendeu a eficácia da referida MP e representou um marco histórico para a definição do direito fundamental à autodeterminação informativa como corolário do direito fundamental à privacidade.

Segundo assentado nas razões invocadas pelo autor da ação, o direito à autodeterminação individual pressupõe a garantia da liberdade de decisão dos indivíduos sobre “as ações a serem procedidas ou omitidas e, inclusive, a possibilidade de se comportar realmente conforme tal decisão”, argumentando a necessidade de proporcionalidade na intervenção estatal legislativa quando dos critérios de compartilhamento do uso de dados pessoais.[111]

Em seu voto, a Ministra Rosa Weber desenvolveu sua fundamentação na ausência de disposição na MP 954/2020 sobre a finalidade e o modo de disponibilização dos dados objetos da norma, desatendendo o devido processo legal para a sua edição. Ainda destacou que não imergia interesse público legítimo no

109 O Conselho Federal da OAB propôs a primeira ADI que possuía o objetivo de questionar a MP 954/2020. Contudo, outras quatro ADI’s foram propostas pelos partidos políticos PSDB, PSB, PSOL e PCdoB, as quais foram julgas conjunto com a ADI 6387 por esta abarcar de forma mais ampla o objeto das demais.

110 BRASIL. Supremo Tribunal Federal. (Plenário). Ação Direta de Inconstitucionalidade n.º 6387. Relatora: Ministra Rosa Weber, 07 de maio de 2020. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur436273/false. Acesso em: 27 out 2024.

111 BRASIL. Supremo Tribunal Federal. (Plenário). Ação Direta de Inconstitucionalidade n.º 6387. Relatora: Ministra Rosa Weber, 07 de maio de 2020. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur436273/false. Acesso em: 27 out 2024.

compartilhamento dos referidos dados, considerando-se a necessidade, adequação e proporcionalidade da medida.

Foi destacada, ainda, a ausência de previsão na norma quanto aos mecanismos e procedimentos de proteção dos dados, a fim de assegurar o seu sigilo, higidez e o anonimato (quando for o caso). Ressaltou-se ainda, que a Medida Provisória não estaria submetida à responsabilização pelo compartilhamento dos dados, justamente em razão de que, à época do julgamento a LGPD não estava em vigor.

A decisão de suspensão da medida provisória pela Ministra Rosa Weber foi submetida a referendo do plenário, que passou a analisar a amplitude e abrangência dos direitos individuais em questão (intimidade, vida privada e sigilo de dados) em razão da sua relatividade. Apesar de serem direitos de importância ímpar no Estado Democrático de Direito, são aplicados os princípios da relatividade ou da convivência das liberdades públicas. Em seu voto, o Ministro Alexandre de Moraes destacou que, no conflito entre direitos fundamentais, o intérprete da Constituição deve se valer dos princípios da concordância prática ou da harmonização de forma a combinar os bens jurídicos conflitantes.

Como salientou a Ministra Rosa Weber em seu voto, inclusive utilizando o conhecido artigo de Harvard chamado *The Right to Privacy*, escrito por juízes da Suprema Corte dos Estados Unidos:

> [...] as mudanças políticas, sociais e econômicas demandam incessantemente o reconhecimento de novos direitos, razão pela qual necessário, de tempos em tempos, redefinir a exata natureza e extensão da proteção à privacidade do indivíduo. Independentemente, do seu conteúdo, mutável com a evolução tecnológica e social, permanece como denominador comum da privacidade e da autodeterminação o entendimento de que a privacidade somente pode ceder diante de justificativa consistente e legítima. [...][112]

Ainda podem ser destacados alguns fundamentos apresentados no voto do Ministro Luiz Fux, que mencionou o julgamento proferido pelo Tribunal Constitucional Alemão sobre a Lei do Censo de 1983, a Carta de Direitos Fundamentais da União Europeia, a respeito do direito de que todas as pessoas possuem à proteção de dados pessoais, bem como citou o julgado do Tribunal de Justiça da União Europeia sobre

112 BRASIL. Supremo Tribunal Federal. (Plenário). Ação Direta de Inconstitucionalidade n.º 6387. Relatora: Ministra Rosa Weber, 07 de maio de 2020. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur436273/false. Acesso em: 27 out 2024. p. 21.

Digital Rights Ireland, no qual destacou a existência do direito fundamental à proteção dos dados pessoais.[113]

Em conclusão, o STF, no referido julgamento, fixou que:

> [...] a proteção de dados pessoais e autodeterminação informativa são direitos fundamentais autônomos, extraídos da garantia da inviolabilidade da intimidade e da vida privada (art. 5º, X), do princípio da dignidade da pessoa humana (art. 1º, III) e da garantia processual do habeas data (art. 5º, LXXII), previstos na Constituição Federal de 1988.[114]

Esse julgamento foi considerado, como consta no próprio acórdão, um paradigma para o reconhecimento do direito à autodeterminação informativa como um direito fundamental autônomo do indivíduo, sendo parcela fundamental do seu direito ao desenvolvimento da personalidade.

Importa mencionar que antes do julgamento acima analisado, o STF mencionou a existência de um direito fundamental à autodeterminação informativa no ano de 2015, no julgamento do Recurso Extraordinário 673707/MG, de relatoria do Ministro Luiz Fux a respeito do direito ao habeas data para obtenção de acesso às informações constantes de sistemas informatizados de controle de pagamentos de tributos.[115]

Na ocasião de seu julgamento, o Ministro Gilmar Mendes, na discussão sobre o levantamento de informações, mencionou a existência do direito à autodeterminação informativa no Brasil, ao passo que, à época, concluiu que havia discussões a seu respeito no campo de direito material no país. Como bem indicado pelo Ministro, o direito à autodeterminação foi criado pela Corte Constitucional Alemã como um desdobramento do direito de personalidade.[116]

No referido julgamento, não houve o reconhecimento desse direito à autodeterminação informativa como ocorreu em 2020 no julgamento da ADI 6387. Dessa forma, constata-se que o Supremo Tribunal Federal reconheceu um direito fundamental não previsto expressamente na Constituição Federal ou em legislação infraconstitucional em vigor à época do julgamento, mas que sua existência no Direito

113 BRASIL. Supremo Tribunal Federal. (Plenário). Ação Direta de Inconstitucionalidade n.º 6387. Relatora: Ministra Rosa Weber, 07 de maio de 2020. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur436273/false. Acesso em: 27 out 2024. p. 37

114 Ibid.

115 BRASIL. Supremo Tribunal Federal. (Plenário). Recurso Extraordinário n.º 673707/MG. Relator: Ministro Luiz Fux, 17 de junho de 2015. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=9487405. Acesso em 27 out. 2024.

116 BRASIL. Supremo Tribunal Federal. (Plenário). Recurso Extraordinário n.º 673707/MG. Relator: Ministro Luiz Fux, 17 de junho de 2015. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=9487405. Acesso em 27 out. 2024.

foi justificada pela interpretação quanto aos desdobramentos dos direitos de personalidade à privacidade e intimidade.

No âmbito de competência do Superior Tribunal de Justiça, dentre diversos julgamentos que envolvem a discussão da violação do direito à proteção de dados pessoais, destaca-se o Recurso Especial 2.077.278/SP, de relatoria da Ministra Nancy Andrighi, no qual, a Terceira Turma proferiu entendimento de que a instituição financeira responde por defeitos na prestação de serviço decorrentes do tratamento indevido de dados pessoais bancários na hipótese em que forem utilizados por terceiros para a prática de golpes contra o consumidor.[117]

Na origem, cuidava-se de ação declaratória de inexigibilidade de débito por vazamento de dados bancários, cumulada com indenização por danos morais e repetição de indébito. A autora alegou que, em razão de uma dívida com a instituição financeira, entrou em contato por e-mail para tentativa de negociação do débito. Posteriormente, uma pessoa, se passando por funcionário do banco, encaminhou boleto bancário emitido para quitação do débito, o qual foi pago pela vítima. No caso em questão, o estelionatário detinha informações pessoais da autora, inclusive a respeito do contrato objeto da negociação. Neste passo, a vítima não desconfiou do golpe por entender que havia manifestado primeiramente o interesse em realizar a quitação do seu débito.

No julgamento, a relatora do recurso especial destacou que “não há como afastar a responsabilidade da instituição financeira pela reparação dos danos decorrentes do famigerado “golpe do boleto”, tendo em vista que foi constatado que os estelionatários detinham informações de dados sigilosos sobre a vítima.[118]

No acórdão, a Terceira Turma sedimentou o entendimento já consolidado naquela Corte quanto à configuração de responsabilidade objetiva da instituição financeira em decorrência das falhas na prestação de serviço ao consumidor. O CDC estabelece o respeito à dignidade, saúde e segurança, proteção dos interesses econômicos em atendimento ao reconhecimento da posição de vulnerabilidade do consumidor na relação de consumo. Tal responsabilidade é justificada principalmente

117 BRASIL. Superior Tribunal de Justiça. (Terceira Turma). Recurso Especial n.º 2077278. Relatora: Ministra Nancy Andrigui, 09 de outubro de 2023. Disponível em: https://scon.stj.jus.br/SCON/pesquisar.jsp?preConsultaPP=&pesquisaAmigavel=+%3Cb%3E2.077.278%3C%2Fb%3E&acao=pesquisar&novaConsulta=true&i=1&b=ACOR&livre=2.077.278&filtroPorOrgao=&filtroPorMinistro=&filtroPorNota=&data=&operador=e&thesaurus=JURIDICO&p=true&tp=P&processo=&classe=&uf=&relator=&dtpb=&dtpb1=&dtpb2=&dtde=&dtde1=&dtde2=&orgao=&ementa=&nota=&ref=.. Acesso em 27 out 2024.

118 Ibid. p. 02

em decorrência do risco do empreendimento que a instituição tem a obrigação de assumir. [119]

A propósito, o entendimento sobre a responsabilidade objetiva das instituições bancárias foi sedimento no Tema Repetitivo 466/STJ[120] que, posteriormente originou a Súmula 479 do mesmo tribunal: “As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias.”[121]

O acórdão mencionado alhures destacou, no entanto, que a responsabilidade da instituição financeira depende da comprovação do nexo causal entre a conduta dos criminosos e o uso dos dados sobre as operações financeiras vazados. Desse modo, se faz necessária a determinação da origem exata do vazamento de dados.[122]

Por fim, importante destacar que em outro julgamento o STJ se posicionou quanto à necessidade de comprovação do dano para acarretar a condenação ao pagamento de indenização por danos morais. O fundamento residiu na diferenciação entre dados pessoais comuns (nome completo, RG, gênero, datada de nascimento, idade, telefone fixo, telefone celular e endereço) e os dados pessoais sensíveis (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 pessoa natural).[123]

No caso julgado, a autora alegou exposição dos dados pessoais comuns, os quais, segundo o entendimento do STJ, não possuem o condão, por si só, de acarretar na indenização por danos morais, pois foi considerado como falha indesejável. Ao

---

119 O acórdão ainda ressaltou que “A prestação do serviço de qualidade pelos fornecedores abrange o dever de segurança, que, por sua vez, engloba tanto a integridade psicofísica do consumidor, quanto sua integridade patrimonial. Note-se que o art. 8º do CDC admite que se coloquem no mercado apenas produtos e serviços que ofereçam riscos razoáveis e previsíveis, isto é, que não sejam excessivos ou potencializados por falhas na atividade econômica desenvolvida pelo fornecedor (MIRAGEM, Bruno. Tendências da responsabilidade das instituições financeiras por danos ao consumidor. Revista de Direito do Consumidor, São Paulo, col. 87, 2013, p. 51-91). Ibid. p.11.

120 BRASIL. Superior Tribunal de Justiça. (Segunda Seção). Tema repetitivo 466. 12 de setembro de 2011. Disponível em: https://processo.stj.jus.br/repetitivos/temas_repetitivos/pesquisa.jsp?novaConsulta=true&tipo_pesquisa=T&sg_classe=REsp&num_processo_classe=1197929. Acesso em 27 out 2024. Tese afirmada: ss instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias.

121 BRASIL. Superior Tribunal de Justiça. (Segunda Seção). Súmula 479. 01 de agosto de 2012. Disponível em: https://processo.stj.jus.br/SCON/sumstj/toc.jsp?sumula=479.num. Acesso em 27 out 2024.

122 BRASIL. Superior Tribunal de Justiça. (Terceira Turma). Recurso Especial n.º 2077278. Relatora: Ministra Nancy Andrigui, 09 de outubro de 2023. Disponível em: https://scon.stj.jus.br/SCON/pesquisar.jsp?preConsultaPP=&pesquisaAmigavel=+%3Cb%3E2.077.278%3C%2Fb%3E&acao=pesquisar&novaConsulta=true&i=1&b=ACOR&livre=2.077.278&filtroPorOrgao=&filtroPorMinistro=&filtroPorNota=&data=&operador=e&thesaurus=JURIDICO&p=true&tp=P&processo=&classe=&uf=&relator=&dtpb=&dtpb1=&dtpb2=&dtde=&dtde1=&dtde2=&orgao=&ementa=&nota=&ref=.. Acesso em 27 out 2024.

123 BRASIL. Superior Tribunal de Justiça. (Segunda Turma). Agravo em Recurso Especial n.º 2130619. Relator: Ministro Francisco Falcão, 10 de mar de 2023. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202201522622&dt_publicacao=10/03/2023. Acesso em 27 out 2024.

contrário quando ocorre vazamento de dados pessoais sensíveis, que merece tratamento diferenciado, conforme art. 5º, II da LGPD.[124]

Seria possível citar ainda diversos outros julgados relacionados à aplicação da LGPD, contudo, a fim de progredir as reflexões necessárias ao atingimento dos objetivos propostos, se torna pertinente avançar com a temática por meio de uma abordagem geral sobre a relação entre o sistema de proteção de dados pessoais e outras áreas do direito. Como visto nos exemplos acima, o tema possui conexão com diversos ramos, o que será discutido nas próximas linhas.

Conforme será demonstrado, a constatação da possibilidade e necessidade de interação entre o microssistema de proteção de dados e outros ramos de direito não exclui a imprescindibilidade do aprimoramento dos mecanismos atuais de prevenção e repressão já existentes na esfera administrativa de competência da ANPD em face de vazamentos e tratamentos irregulares de dados pessoais.

Como em outros sistemas normativos existentes, a política de proteção de dados pessoais não pode ser considerada de forma isolada no atual cenário jurídico nacional. Sistemas específicos podem ser aplicados em complementação a outros sem que isso acarrete desrespeito aos princípios vigentes, como o da especialidade. A seguir, serão apresentadas algumas reflexões sobre a possibilidade de contribuição de outros ramos, notadamente o direito penal, no sistema nacional de proteção de dados pessoais.

124 BRASIL. Superior Tribunal de Justiça. (Segunda Turma). Agravo em Recurso Especial n.º 2130619. Relator: Ministro Francisco Falcão, 10 de mar de 2023. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202201522622&dt_publicacao=10/03/2023. Acesso em 27 out 2024.

3 A PROTEÇÃO DE DADOS PESSOAIS E SUA RELAÇÃO COM OUTROS RAMOS DOS DIREITO.

Conforme exposto no capítulo anterior, a presença de legislação própria no Brasil sobre proteção de dados pessoais remonta a um período recente. Além do Marco Civil da Internet e a LGPD, é possível citar o Código de Defesa do Consumidor que já trazia em seu bojo a proteção das informações e direito de acesso e retificação de banco de dados dos consumidores.

No entanto, com o crescente aumento no tratamento de dados pessoais por instituições públicas e privadas, a proteção dessas informações deverá se tornar uma das prioridades em suas atividades, sejam estas de caráter econômico ou não. As legislações acima citadas, principalmente a LGPD, preveem o estabelecimento de regras para a coleta, processamento, tratamento, armazenamento e tudo mais que possa ser realizado com os dados pessoais, bem como estabelece as penalidades administrativas em face do seu tratamento irregular.

Mas não é somente nessas legislações que se verifica um movimento de adequação normativa à nova realidade da sociedade da informação. No campo do Direito Processual Penal, em especial das investigações criminais, é possível citar a Lei n.º 9.296 de 24 de julho de 1996, que regulamenta a realização de interceptação telefônica para fins de obtenção de prova. Como se refere a uma mitigação do direito fundamental ao sigilo das comunicações, a referida legislação prevê situações excepcionais para a realização da interceptação.[125]

A Lei n.º 11.343 de 2006[126], chamada de Lei de Drogas autoriza a interceptação de comunicações telefônicas e o acesso aos dados cadastrais e registros telefônicos para fins de investigação de tráfico de drogas, mediante ordem judicial.

A Lei nº 12.850/2013[127] - Lei de Combate às Organizações Criminosas - prevê a possibilidade de captação ambiental de sinais eletromagnéticos, ópticos ou acústicos, acesso a registros de ligações telefônicas e dados cadastrais, interceptação de comunicações telefônicas e telemáticas, entre outros. Ainda prevê a possibilidade de acesso a dados cadastrais, registros de ligações telefônicas e de mensagens de

125 BRASIL. Lei Federal n.º 9.296 de 24 de julho de 1996. Disponível em https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em 26 de jul. 2024.

126 BRASIL. Lei Federal n.º 11.343 de 23 de agosto de 2006. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11343.htm. Acesso em 26 de jul. 2024.

127 BRASIL. Lei Federal n.º 12.850, de 02 de agosto de 2013. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em 26 de jul. 2024.

texto, entre outros. São alguns exemplos de legislações que preveem a coleta e uso de dados para a promoção de investigação criminal, todas mediante autorização judicial.

Cite-se, ainda, o Projeto de Lei 1.515/2022 para aprovação da Lei de Proteção de Dados Penal, que tem como ementa: “Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais.”[128] O PL prevê princípios, diretrizes e hipóteses para o tratamento e compartilhamento de dados de pessoas investigadas e de todas as demais figuras envolvidas na apuração de fatos delituosos, como as informações de testemunhas e vítimas. [129]

O projeto ainda estabelece a obrigatoriedade por parte dos órgãos de investigação de adoção de medidas físicas, técnicas e administrativas que objetivam a proteção dos dados pessoais contra acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda ou qualquer tratamento inadequado ou ilícito.[130]

O estabelecimento das regras previstas no referido PL representa um avanço na busca pela proteção de dados contra eventuais abusos perpetrados no âmbito das investigações criminais e propõe a regulamentação sobre questões importantes até então não abordadas. Muito se discute sobre o respeito aos direitos fundamentais do investigado e demais envolvidos nos procedimentos de apuração de crimes.[131]

O PL teve seu último andamento ocorrido em 20 de janeiro de 2022 quando a mesa diretora estabeleceu a criação de Comissão Especial para realização da análise da matéria, a qual ainda não foi criada.[132]

Em que pese o presente trabalho não possuir o foco na análise do campo processual, tais informações são de grande relevância para demonstrar a necessidade de ampliação da sistemática de proteção de dados pessoais para outras

---

128 BRASIL., PL 1515, 2022. Câmara dos Deputados. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2326300#tramitacoes. Acesso em 02/08/2023.

129 Ibid. art. 30.

130 O PL não exclui a possibilidade de responsabilização civil e penal pelo descumprimento de suas determinações, conforme art. 52, § 2º Se o mesmo fato constituir simultaneamente crime e infração administrativa contra a mesma pessoa natural, o procedimento administrativo será suspenso quando iniciada medida de investigação de infração penal, retomando-se caso não sobrevenha sentença declarando a inexistência material do fato ou sua prática em legítima defesa, estado de necessidade, exercício regular de um direito ou cumprimento de um dever. § 3º A responsabilização administrativa não afastará a civil e a penal. Ibid.

131 WOLTER, Jürgen. O inviolável e o intocável no direito processual penal: reflexões sobre dignidade humana. São Paulo. Marcial Pons, 2018. p. 159.

132 BRASIL., PL 1515, 2022. Câmara dos Deputados. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2326300#tramitacoes. Acesso em 02/08/2023.

áreas do direito, tendo em vista que a tecnologia alterou o modo de realização de diversas atividades, inclusive as do próprio Poder Judiciário e da polícia judiciária.

No tocante à esfera do direito material, quanto à responsabilização pelo tratamento irregular de dados pessoais, um dos objetivos específicos deste estudo consiste em analisar a possibilidade de interação do microssistema de proteção de dados com o Direito Penal. Para alcançar as conclusões necessárias, torna-se primordial levantar reflexões sobre os fundamentos doutrinários que permitem uma intersecção entre diferentes áreas do direito. Este será o propósito da próxima seção.

3.1 O critério hermenêutico do diálogo das fontes.

No decorrer no tempo, a construção das normas no ordenamento jurídico sofreu uma descodificação provocada pela edição de diversas leis esparsas, fenômeno denominado de pluralismo pós-moderno de fontes. Assim, surgiram microssistemas jurídicos que podem, em uma análise precipitada, serem interpretados como conflitantes entre si. No entanto, eles necessitam ser coordenados por meio de métodos de aplicação das normas.[133]

Diversos critérios foram estabelecidos pela doutrina para definição de uma aplicação lógica das leis, conforme a sua hierarquia, especialidade, temporalidade, entre outros. Ocorre que, ao longo do tempo, diante da inovação legislativa em tantas áreas distintas do Direito, surgiu a preocupação com efetividade dos direitos fundamentais, principalmente em relação aos grupos mais vulneráveis. Nesse contexto, abriu-se uma reflexão para a busca de métodos de aplicação das leis que alcançassem o respeito à dignidade da pessoa humana.

> Em um mundo pluralístico, como o que vivemos, todas as teorias que ajudam a ressaltar a dignidade da pessoa humana, o direito à saúde, à vida, à qualidade, à proteção diferenciada de grupos mais vulneráveis de nossa sociedade de risco, deve ser destacada.[134]

A teoria do diálogo das fontes consiste em uma abordagem interpretativa originada na Alemanha pelo professor Erik Jayme para harmonizar a aplicação

133 VALENTE, Victor Augusto Estevam. A proteção de dados pessoais no direito penal: uma análise crítica da criminalização nas perspectivas constitucional e de política criminal. São Paulo: D'Plácido, 2022. p. 71.

134 MARQUES, Claudia Lima. O "diálogo das fontes" como método da nova teoria do direito: um tributo a Erik Jayme. In: Diálogo das fontes. Do conflito à coordenação de normas do direito brasileiro. MARQUES, Claudia Lima (coord). São Paulo: Revista dos Tribunais, 2012. p. 21.

134 Ibid. p. 23.

simultânea, coerente e coordenada de diferentes fontes legislativas nacionais e internacionais, leis gerais e especiais que são igualmente vigentes, nas quais não se mostra possível a aplicação de soluções clássicas das antinomias, como a revogação, derrogação ou ab-rogação.[135] A referida teoria possui uma força simbólica na contribuição da aplicação das normas valorativas de direitos humanos.

A adoção da teoria do diálogo das fontes visa propor soluções para priorizar a dignidade da pessoa humana, nos valores constitucionais e nos direitos fundamentais, de modo a interpretar sistematicamente as diversas fontes normativas e, assim, evitar a insegurança na aplicação das leis.

Segundo os defensores desta teoria, há uma crítica quanto ao discurso metodológico rígido tradicional de aplicação das normas, ao passo que devem ser adotadas técnicas de plasticidade, harmonia e aproveitamentos recíprocos entre elas.

> [...] Diálogo é sinônimo de convivência ou aproveitamento (influências) recíprocas, que quebra o tom autoritário dos paradigmas tradicionais, como *lex specialis, lex generalis, lex superior*. No di-a-logos há convivência de paradigmas. Superam-se os muros e divisórias entre fontes, há porosidade e entrelaçamento, influências recíprocas e convivência de valores e lógicas. [...][136]

No Brasil, a Professora Claudia Lima Marques defende a aplicação desta teoria na busca de uma interpretação integrada e coerente do ordenamento jurídico, respeitando a hierarquia e a especificidade das normas. Seus estudos apontam a aplicabilidade da teoria principalmente no campo do direito do consumidor, mas destacam a possibilidade de sua adoção em outras áreas.

A teoria do diálogo das fontes defende que deve-se alcançar uma interpretação que permita a convivência e a complementação entre as normas, no lugar de se valer dos clássicos critérios de solução de antinomias: hierarquia, especialidade e cronologia. O objetivo consiste em assegurar que todas as normas relevantes possam ser consideradas e aplicadas de maneira harmoniosa, atendendo valores constitucionais e humanos ou fundamentais.

Segundo Claudia Lima Marques, essa teoria se baseia na ideia de que as diferentes fontes normativas devem "dialogar" entre si, de modo que se complementem e se integrem, em vez de se anularem. Esse diálogo pode ocorrer

---

135 MARQUES, Claudia Lima. O “diálogo das fontes” como método da nova teoria do direito: um tributo a Erik Jayme. In: Diálogo das fontes. Do conflito à coordenação de normas do direito brasileiro. MARQUES, Claudia Lima (coord). São Paulo: Revista dos Tribunais, 2012. p. 21.

136 Ibid.

entre normas de diferentes níveis (constitucionais, infraconstitucionais), e ramos do Direito (civil, penal, administrativo, etc.), ou mesmo entre normas internas e internacionais.[137]

> A teoria do diálogo das fontes é, na minha opinião, um método da nova teoria geral do direito muito útil e pode ser usada na aplicação de todos os ramos do direito, privado e público, nacional e internacional, como instrumento útil ao aplicador da lei no tempo, em face do pluralismo pós-moderno de fontes, que não parece diminuir no século XXI. Método é caminho. Metodologia é um processo, uma técnica que generosamente nos guia, nos ajuda a avançar de forma segura, neste esforço de acertar e alcançar uma decisão justa.[138]

A doutrina majoritária brasileira acompanha o entendimento favorável pela aplicação dessa teoria, considerada como uma ferramenta primordial para a aplicação justa das normas jurídicas em um contexto de pluralidade normativa, como é o caso do Brasil. Na jurisprudência dos tribunais estaduais e Superior Tribunal de Justiça é possível identificar centenas de casos em que o diálogo das fontes foi aplicado de forma a integrar as normas e viabilizar o melhor alcance de direitos fundamentais.

A título de elucidação, o Superior Tribunal de Justiça no julgamento do Recurso Especial 1.794.971/SP de Relatoria do Ministro Herman Benjamin se manifestou pela aplicação da teoria do diálogo das fontes entre o Código de Defesa do Consumidor e diversos outros preceitos normativos, como o direito penal, de cunho sanitário, de concorrência, de economia popular, entre outros, que podem ser aplicados para complementar a interpretação das normas consumeristas.[139]

No campo penal, a LGPD não trouxe previsão dessa tutela específica de proteção de dados pessoais mas, em uma análise mais aprofundada, constata-se que não se pode descartar a possibilidade de aplicabilidade de outros sistemas jurídicos nesta seara, tendo em vista a interação entre esses sistemas normativos.

Em que pese a LGPD ter sido um marco no árduo caminho em busca de proteção dos dados pessoais, entende-se que a interação dessa norma com os ramos de direito penal e processual penal é possível e necessária, tendo em vista a grande incidência de vazamento de dados e (ainda) pouca efetividade nos processos de responsabilização e aplicação na esfera administrativa.

---

137 Ibid. p. 23.

138 MARQUES, Claudia Lima. O “diálogo das fontes” como método da nova teoria do direito: um tributo a Erik Jayme. In: Diálogo das fontes. Do conflito à coordenação de normas do direito brasileiro. MARQUES, Claudia Lima (coord). São Paulo: Revista dos Tribunais, 2012. p. 23.

139 BRASIL. Superior Tribunal de Justiça (Terceira Turma). Recurso Especial 1.794.971/SP. 20 de maio de 2021. Relator Ministro Herman Benjamin. Disponível em: https://processo.stj.jus.br/processo/pesquisa/?num_registro=201902426992. Acesso em 29 jul. 2024.

Como informado no início do presente trabalho, notícias de diversos incidentes de vazamento de dados pessoais podem ser encontrados na internet. Destaca-se a notícia do maior vazamento de dados pessoais ocorrido no Brasil, quando foram obtidas informações de 223 (duzentos e vinte e três) milhões de pessoas, inclusive de indivíduos já falecidos. A Polícia Federal instaurou investigação, que resultou na identificação do responsável. Apurou-se que foram vazados dados do Senado Federal, Exército e Tribunal Superior Eleitoral. As informações foram posteriormente disponibilizadas e comercializadas na internet.[140]

Segundo a Associação Brasileira de Internet - ABRANET, em 2022, o Brasil alcançou em 4º lugar no ranking de países que mais sofreram violações de segurança cibernética. No segundo trimestre daquele ano, foram cerca de 3,2 (três milhões e duzentos mil) usuários atingidos com violação de dados.[141]

A violação de dados pessoais, principalmente decorrente de vazamentos de informações são recorrentemente noticiados na internet. Recentemente, o Banco Central apresentou ocorrência de incidente de segurança com dados pessoais vinculados a chaves Pix sobre a responsabilidade da Instituição de Pagamento S.A, 99Pay. Segundo informações encaminhadas pelo BC, os dados obtidos foram de natureza cadastral de cerca de 39 (trinta e nove) mil chaves Pix.[142]

No campo internacional, destaca-se a condenação do grupo *Meta Plataforms Ireland Limited* (Meta IE) à multa de €1,2 (um vírgula dois) bilhões de euros conforme decisão vinculativa proferida pelo Comitê Europeu de Proteção de Dados – EDPB em razão de investigação realizada pela Autoridade Irlandesa de Proteção de Dados (IE-DPA). A maior condenação da história da RGPD decorreu em razão da transferência de dados pessoais do Facebook para os Estados Unidos.[143]

---

140 CNN BRASIL. **PF prende hacker que vazou dados de 223 milhões de brasileiros.** São Paulo, 2024. Disponível em: https://www.cnnbrasil.com.br/nacional/pf-prende-hacker-que-vazou-dados-de-223-milhoes-de-brasileiros/#:~:text=pf%20prende%20hacker%20que%20vazou%20dados%20de%20223%20milh%c3%b5es%20de%20brasileiros,-investiga%c3%a7%c3%a3o%20aponta%20que&text=a%20pol%c3%adcia%20federal%20prendeu%2c%20nesta,entre%20vivos%20e%20j%c3%a1%20falecidos. acesso em 29 de jul. 2024.

141 ASSOCIAÇÃO BRASILEIRA DE INTERNET. (ABRANET). **Vinte e cinco contas sofrem violação de dados por minuto no Brasil**. São Paulo, 2022. Disponível em: https://www.abranet.org.br/Noticias/Vinte-e-cinco-contas-sofrem-violacao-de-dados-por-minuto-no-Brasil-3966.html?UserActiveTemplate=mobile%2Csite. Acesso em 03 mai.2024

142 ASSOCIAÇÃO BRASILEIRA DE INTERNET. (ABRANET). **Banco Central: vazaram dados de 39 mil chaves Pix do 99Pay**. São Paulo, 2024. Disponível em: https://www.abranet.org.br/Noticias/Banco-Central%3A-vazaram-dados-de-39-mil-chaves-Pix-do-99Pay-5022.html. Acesso de 29 de jul. 2024.

143 EDPB. 1.2 billion euro fine for Facebook as a result of edpb binding decision. Bruchelas, Belgica, 2023. Disponível em https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_pt. Acesso em 29 de jul. 2024.

Esses exemplos e outros que podem ser citados demonstram a magnitude dos prejuízos que os usuários podem sofrer em razão da violação dos dados pessoais. Diante da relevância do direito à proteção de dados pessoais, inclusive incorporado atualmente como um direito fundamental na Constituição Federal, importa responder ao questionamento quanto à possibilidade de considerar os dados pessoais como um bem jurídico-penal, assunto que será abordado em seguida.

Valente propõe a aplicabilidade deste critério hermenêutico a fim de possibilitar uma interação e sincronização dos princípios integradores do microssistema de proteção de dados pessoais previstos na LGPD com os demais sistemas jurídicos existentes. Tal entendimento é corroborado pelo art. 64 da referida lei, segundo o qual prevê que os direitos e princípios dispostos na LGPD não excluem outros previstos em outras legislações.[144]

O diálogo das fontes deve ter como base a Constituição Federal, de onde emergem diversos princípios e direitos correlacionados ao tema, como dignidade da pessoa humana, direito à vida privada, à proteção de dados, dentre outros. Assim, a interpretação da proteção de dados pessoais deve ser realizada com a interação entre diversos ramos, tais como o direito civil, consumidor, bem como o direito penal e processual penal, a fim de proporcionar maior efetividade na proteção dos dados dos seus titulares.[145]

> Entendemos, destarte, que a confluência desses métodos possibilita que seja identificado o nível de relação entre o direito penal e o regime de proteção de dados no Brasil. Cabe dizer, propicia que sejam verificadas as convergências entre ambos e, em caso de necessidade de intervenção criminal, sejam sugeridas alternativas para uma política criminal calcada na intervenção mínima e na interação do direito material com o sistema de proteção de dados pessoais, este fundado no direito fundamental previsto no art. 5º, inciso LXXIX, da Constituição de 1988 e na Lei nº 13.709/18 (LGPD).[146]

Ressalte-se que o diálogo das fontes reforça a integração entre as normas nacionais e internacionais, de modo a efetivar progressivamente o respeito aos direitos humanos e fundamentais. Como já ressaltado, a União Europeia exerce grande influência para a normatização brasileira no tema de proteção de dados

144 A redação do art. 64 assim dispõe: Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

145 VALENTE, Victor Augusto Estevam. A proteção de dados pessoais no direito penal: uma análise crítica da criminalização nas perspectivas constitucional e de política criminal. São Paulo: D'Plácido, 2022. p. 73.

146 Ibid. p. 75.

pessoais. A Convenção 108+ (atualização da Convenção 108) do Conselho da Europa possibilita a sua adesão por países não membros. O Brasil se tornou observador da referida norma.[147]

Contextualizada a teoria do diálogo das fontes e sua aplicação crescente pelos tribunais brasileiros entre normas do direito público e privado, inclusive no campo penal, nas próximas linhas serão traçadas considerações sobre a o direito fundamental à proteção de dados pessoais e possibilidade de estabelecê-lo como bem jurídico-penal, a partir da interpretação da função do direito penal.

3.2 A função do direito penal: proteção a bens jurídicos penais.

O principal objetivo do direito penal consiste em impedir a violência na sociedade, tanto que se manifesta por meio de crimes quanto em atos de vingança, pela busca da justiça pelas próprias mãos. Esses dois aspectos envolvem conflitos que são resolvidos pelo uso da força: no crime, ela é exercida pelo autor do delito; na vingança, pela vítima ou por quem a apoia. Em ambos os casos, essa força é imprevisível e descontrolada, podendo, inclusive, atingir terceiros inocentes.

Portanto, pode-se afirmar que a função da lei penal consiste em reduzir essa violência, por meio da previsão de atos que causam crimes e punindo aqueles que reagem com vingança. Assim, o direito penal não se limita apenas a proteger a sociedade contra as ameaças dos delitos; ele também defende os mais fracos — aqueles que foram ofendidos ou ameaçados. Ao regular o uso da força, a lei penal protege as possíveis vítimas da violência e, ao mesmo tempo, assegura que até mesmo os réus e investigados estejam resguardados de reações violentas desproporcionais.

A justificativa para a existência do direito penal reside em sua função de proteção dos direitos dos mais fracos contra abusos. As duas finalidades preventivas — a prevenção de crimes e a contenção de reações violentas — se inter-relacionam, conferindo ao direito penal seu papel essencial como guardião dos direitos fundamentais.[148]

147 UNIÃO EUROPEIA. **Convenção n.º 108+, de 18 de maio de 2018**. Disponível em: https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2. Acesso em 16 nov. 2024.

148 FERRAJOLI, Luigi. Direito e razão: teoria do garantismo penal. 3.ed. ver. São Paulo: Revista dos Tribunais, 2022, p. 271.

Essa legitimidade do direito penal não decorre de uma aprovação democrática, mas sim de um "garantismo" em relação aos direitos fundamentais. O garantismo assegura a proteção dos cidadãos contra a arbitrariedade, estabelece igualdade nas regras e respeita a dignidade e liberdade dos acusados.[149]

Para alcançar uma boa compreensão e justificar o direito penal, é essencial reconhecer que seu objetivo é prevenir mais violências. Ferrajoli explica a mudança de sentido do bem jurídico penal ao longo da história. Originalmente, no contexto do Iluminismo, o objeto do delito era considerado um direito subjetivo natural, essencial à proteção da vida, liberdade, saúde e bens. Com o tempo, essa visão se ampliou, reconhecendo que qualquer bem deve ser protegido pelo Estado, sobretudo quando isso só é possível através de ameaças de punição. A Escola Clássica italiana também defendia que o delito deveria ser algo que causa dano ao bem-estar alheio.[150]

Na segunda metade do século XIX, com o crescimento de reações anti-iluministas, os conceitos passaram a perder suas funções axiológicas. O foco se deslocou dos interesses individuais para os interesses do Estado, inicialmente relacionado à proteção de valores que o Estado considerava dignos e, posteriormente, simplesmente à obediência. A ideia de Hegel, que via o direito penal como a representação do direito universal, foi central nesse processo. Assim, os interesses individuais foram gradualmente encobertos pelos interesses do Estado e pela abstração do direito como tal.

O conceito de bem jurídico ainda se referia a algo que o legislador reconhecia como valor, mas as orientações mais autoritárias acabaram por diluir essa ideia, transformando-a em algo que se confundia com a norma jurídica e os interesses do Estado. Isso culminou em uma visão onde o direito penal servia para proteger o interesse do Estado, muitas vezes à custa dos direitos individuais, levando a uma justificação que ligava delitos à desobediência ao soberano.

Com o movimento espiritualista e irracionalista no início do século XX, o conceito de bem se tornou ainda mais desmaterializado, passando a ser visto como critérios éticos ou culturais, cuja violação era associada a comportamentos imorais. Assim, nasceu uma nova confusão entre direito e moral, levando a uma substituição dos conceitos jurídicos por ideias de "violação do dever" e "infidelidade" ao Estado.

149 FERRAJOLI, Luigi. Direito e razão: teoria do garantismo penal. 3.ed. ver. São Paulo: Revista dos Tribunais, 2022, p. 272

150 Ibid. p. 373.

Somente após a Segunda Guerra Mundial a definição de bem jurídico retomou o seu sentido garantista, principalmente pela retomada das referências semânticas a situações objetivas, independentes ou anteriores à própria norma jurídica. Tal redefinição devolveu a função axiológica do bem jurídico.[151]

Como parte integrante do sistema normativo brasileiro, o direito penal possui como função a regulação da sociedade para proteção de bens jurídicos mais relevantes. Ao passo que o direito civil e outros ramos do direito privado possuem o condão de regular as relações em diferentes esferas (família, consumidor, empresarial, entre outros), o direito penal atua, principalmente, por meio do estabelecimento de normas incriminadoras. Ou seja, a definição legal de comportamentos proibidos e as sanções cabíveis em caso de cometimento dessas condutas. Alguns princípios denotam as suas características mais importantes, como o princípio da intervenção mínima, da reserva legal e da fragmentariedade.

Em linhas gerais, o direito penal será aplicado quando outros ramos do direito não forem suficientes para atingir o fim pelo qual se destinam. Assim, afirma-se que o direito penal deve ser a "*ultima ratio".* Em razão das espécies de reprimendas passíveis de serem aplicadas, as quais podem atingir a liberdade do indivíduo, constitui pressuposto da aplicação da pena a existência de uma previsão legal da conduta como crime e sua respectiva pena.

Na busca pela definição do conteúdo material de crime, a doutrina passou a questionar o fundamento da teoria positivista segundo o qual crime seria somente aquilo que o legislador considerasse como tal, ou seja, um conceito estritamente formal do crime. O questionamento que se fazia consistia em identificar a fonte de onde se extrai a legitimidade para considerar que certas condutas podem ser consideradas crimes. Dever-se-ia encontrar um fundamento pelo qual pudesse identificar a função e os limites do direito penal.[152]

Ferrajoli destaca a existência de uma doutrina a qual estabelece critérios de política criminal voltada à justificação externa dos tipos penais. Esses critérios buscam estabelecer uma correspondência entre a prevenção de crimes e a tutela de bens jurídicos. O primeiro critério consiste na justificação das proibições somente em casos de ataques concretos (aqui entendidos como o dano causado ou perigo de dano) a bens fundamentais, ou seja, os direitos fundamentais. Nesse aspecto deve-se somar

151 FERRAJOLI, Luigi. Direito e razão: teoria do garantismo penal. 3.ed. ver. São Paulo: Revista dos Tribunais, 2022, p. 274.

152 DIAS, Jorge de Figueiredo. **Direito Penal. Parte Geral**. Tomo I, 1.ed.São Paulo: Revista dos Tribunais, 2007.p.106.

à necessidade de constatação de que o bem somente justifica uma proteção penal quando o seu valor for maior do que o bem privado em razão de uma aplicação de pena.[153]

Além disso, há um outro critério político de caráter axiológico, que decorre do princípio da utilidade e o da distinção entre direito e moral, qual seja, além dos tipos penais serem destinados à tutela de bens jurídicos, eles devem ser idôneos. Em outras palavras, a proibição deve alcançar a eficácia intimidatória necessária para surtir o efeito preventivo na norma.

Da perspectiva positivista-legalista à perspectiva positivista-sociológica e, após, a moral (ético)-social, surgiu a perspectiva lógico-funcional e racional. Esta concluiu que a definição material de crime não poderia ser encontrada nas teorias até então existentes, mas que deveria ser imposta a compreensão da função do direito penal. Foi denominada também como racional na medida que resulta da função de "tutela subsidiária (ou de *ultima ratio*) de bens jurídicos dotados de dignidade penal (de "bens jurídicos-penais")". [154]

Nesse sentido, a razão de existir do direito penal seria a proteção de bens-jurídicos, definidos como aqueles direitos que possuem a relevância necessária para serem incorporados ao rol de proteção deste ramo jurídico. Nas próximas linhas será apresentado o conceito de bem jurídico, bem como ocorreu seu surgimento e incorporação pela doutrina pátria.

3.3 Proteção de dados pessoais como um bem jurídico-penal.

Sob uma perspectiva histórica, a doutrina do bem jurídico surgiu no século XIX com o objetivo de limitar o legislador, sendo considerada uma evolução da teoria garantista anterior defendida por Feuerbach, que considerava o delito como lesão a um direito subjetivo.[155]

Atualmente, o princípio da exclusiva proteção de bens jurídicos é acolhido por quase toda a doutrina. Por este princípio, considerado como um dos pilares da teoria do delito, o crime constitui lesão ou perigo de lesão ao bem jurídico. Esta teoria se

153 FERRAJOLI, Luigi. Direito e razão: teoria do garantismo penal. 3.ed. ver. São Paulo: Revista dos Tribunais, 2022, p. 379.

154 DIAS, Jorge de Figueiredo. Direito Penal. Parte Geral. Tomo I, 1.ed.São Paulo: Revista dos Tribunais, 2007. p. 114.

155 PRADO, Luiz Regis. Bem jurídico-penal e Constituição. 8.ed. rev.atual.amp. Rio de Janeiro: Forense, 2019. p. 21.

torna essencial para fornecer à tutela penal a previsão de lesão de um bem material, extraído do mundo do ser.[156]

Figueiredo Dias apresenta uma reflexão sobre o conceito e alcance do bem jurídico politicamente tutelável. Segundo o professor, este bem jurídico-penal somente existirá se representar no campo social um valor concretamente reconhecido.[157]

Importante apresentar a lição do autor supracitado sobre a evolução da compreensão do conceito de bem jurídico que, em suas palavras, pode ser definido como "*a expressão de um interesse, da pessoa ou da comunidade, na manutenção ou integridade de um certo estado, objeto ou bem em si mesmo socialmente relevante e por isso juridicamente reconhecido como valioso".*[158]

Por sua vez, Luiz Regis Prado explica que o bem jurídico-penal existe onde possa ser refletido em um valor jurídico constitucionalmente reconhecido, de modo a concluir que ele preexiste ao ordenamento jurídico-penal. Em outras palavras, somente bens jurídicos de nível jurídico-constitucional podem ser legitimamente protegidos pelo Direito Penal.[159] O professor esclarece:

> Em termos conceituais, o bem jurídico vem a ser um ente (dado ou valor social, entidade dotada de valor), material ou imaterial, haurido do contexto social, de titularidade individual ou metaindividual, essencial para a coexistência e o desenvolvimento do homem em sociedade, previsto explícita ou implicitamente no texto constitucional, ou, ao menos, com ele não colidente ou incompatível, e, por isso, jurídico-penalmente protegido.[160]

Uma das questões centrais da ciência do Direito Penal consiste na definição se determinado comportamento será enquadrado ou não como um crime. Segundo explica Claus Roxin, *"a penalização de um comportamento necessita, em todo caso, de uma legitimação diferente da simples discricionariedade do legislador*"[161]

O autor alemão define os bens-jurídicos como "*circunstâncias reais dadas ou finalidades necessárias para uma vida segura e livre, que garanta todos os direitos humanos e civis de cada um na sociedade ou para o funcionamento de um sistema estatal que se baseia nesses objetivos.*"[162]

---

156 Ibid. p. 22.

157 DIAS, Jorge de Figueiredo. Direito Penal. Parte Geral. Tomo I, 1.ed.São Paulo: Revista dos Tribunais, 2007.p.120.

158 Ibid .p.114.

159 PRADO, Luiz Regis. Bem jurídico-penal e Constituição. 8.ed. rev.atual.amp. Rio de Janeiro: Forense, 2019. p. 120.

160 Ibid. p. 39

161 ROXIN, Claus. A proteção de bens jurídicos como função do Direito Penal. Rio Grande do Sul: Livraria do Advogado, 2009. P.11.

162 Ibid. p.19

Nesse sentido, não apenas a existência de um bem jurídico dotado de dignidade penal deve ser exigida para a criminalização de certa conduta, mas a necessidade da tutela penal, pois deve estar caracterizada a indispensabilidade da intervenção estatal, consistindo na *ultima ratio* do direito penal.[163]

Portanto, ao lado do princípio da proteção do bem-jurídico, torna-se imprescindível a vinculação do princípio da subsidiariedade, de modo que só pode ser aplicada uma sanção penal quando não forem suficientes outras medidas nas esferas civil e administrativa.[164]

A tutela penal dos dados pessoais é, pois, respaldada pela relevância do bem jurídico tutelado, calcada nos princípios basilares da intervenção mínima, fragmentariedade em uma proporcionalidade na intervenção criminal.[165]

A política criminal possui como função instrumental a proteção a bens jurídicos-penais, que vêm sendo objeto de desmaterialização ao longo do tempo. Assim, os bens jurídicos denominados espiritualizados, ainda que possuam natureza supraindividual, representam finalidades individuais, reclamando a sua proteção. Assim, a tutela penal dos dados pessoais se encontra legitimada constitucionalmente pelo princípio da proteção do bem jurídico-penal.[166]

A partir da compreensão da subsidiariedade do Direito Penal como “remédio sancionador extremo”, que somente poderá intervir quando os demais ramos do direito se apresentarem como insuficientes ou ineficientes, é possível concluir que o Direito Penal não busca se contrapor aos ilícitos previstos em outras áreas do direito. Dito de outro modo, não cabe ao Direito Penal constituir ilícitos que não guardem correspondência com os demais ramos, uma vez que o ilícito deve ser único no Ordenamento Jurídico.[167]

O Direito Penal brasileiro vem caminhando a passos lentos para se adequar à nova realidade criminal no tocante aos comportamentos que acarretem a violação dos dados pessoais. O Código Penal sofreu alteração pela Lei n. 12.737 de 30 de novembro de 2012 – a chamada lei Carolina Dieckmann – primeira legislação que fez previsão de crime cibernético:

---

163 DIAS, Jorge de Figueiredo. Direito Penal. Parte Geral. Tomo I, 1.ed.São Paulo: Revista dos Tribunais, 2007.p.114.

164 ROXIN, Claus. A proteção de bens jurídicos como função do Direito Penal. Rio Grande do Sul: Livraria do Advogado, 2009. P 29.

165 VALENTE, Victor Augusto Estevam. A proteção de dados pessoais no direito penal: uma análise crítica da criminalização nas perspectivas constitucional e de política criminal. São Paulo: D’Plácido, 2022. p. 91.

166 Ibid. p. 93.

167 LUZ, Ilana Martins. A responsabilidade penal por omissão e os programas de compliance. 2017. Tese (Doutorado) – Universidade de São Paulo, São Paulo, 2017. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2136/tde-15032021-232238/. Acesso em: 31 maio 2024.p. 202.

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.[168]

Ainda poderia ser citado o § 3º do mesmo dispositivo, segundo o qual trouxe a penalização se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido. Inclusive o § 4º do artigo prevê o aumento de pena de um a dois anos se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

A lei que recebeu o nome da atriz foi aprovada após Carolina Diekmann ter sofrido tentativa de extorsão de criminosos que invadiram seu computador e subtraíram 36 (trinta e seis) fotos íntimas. Ao não ceder à chantagem, as fotos foram divulgadas na internet, acarretando em uma grave violação à intimidade da artista em razão da grande repercussão gerada nas mídias.[169]

Além dos crimes comuns que podem ser cometidos no ambiente virtual, como estelionato, extorsão, injúria, calúnia, difamação e falsificação de cartão de crédito e débito, dentre outros, percebe-se que a tutela penal desses ilícitos abarca outros bens jurídicos (patrimônio e a honra), podendo admitir que, de forma mediata, os dados pessoais podem ser considerados.

Segundo a teoria tripartida do crime, este constitui a soma de três substratos, quais sejam, fato típico, antijuridicidade e culpabilidade. Por sua vez, para a configuração do fato típico, além dos elementos essenciais da conduta, resultado e nexo de causalidade, é imprescindível a presença da tipicidade, como requisito essencial para que seja respeitado o princípio da reserva legal. Em que pese a necessidade de estar presente a tipicidade formal (previsão de uma conduta como crime e sua respectiva pena), é consenso na doutrina e jurisprudência que esse requisito não é suficiente, principalmente em razão da subsidiariedade do direito penal. Explique-se: além da previsão legal, o comportamento deve possuir a

168 BRASIL. Lei 12.737 de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Acesso em 31 mai. 2024.

169 SENADO FEDERAL. Dez anos de vigência da Lei Carolina Dieckmann: a primeira a punir crimes cibernéticos. Disponível em https://www12.senado.leg.br/radio/1/noticia/2023/03/29/dez-anos-de-vigencia-da-lei-carolina-dieckmann-a-primeira-a-punir-crimes-ciberneticos. Acesso em 31 mai. 2024

tipicidade material, ou seja, a efetiva lesão ou risco de lesão a um bem jurídico-penal. Por meio esse entendimento que surgiram alguns institutos como o princípio da insignificância como causa de absolvição pela atipicidade do fato.

Conforme apontado pelo Supremo Tribunal Federal a respeito da tipicidade material,

> [...] a existência de um Estado Democrático de Direito passa, necessariamente, por uma busca constante de um direito penal mínimo, fragmentário, subsidiário, capaz de intervir apenas e tão-somente naquelas situações em que outros ramos do direito não foram aptos a propiciar a pacificação social. O fato típico, primeiro elemento estruturador do crime, não se aperfeiçoa com uma tipicidade meramente formal, consubstanciada na perfeita correspondência entre o fato e a norma, sendo imprescindível a constatação de que ocorrera lesão significativa ao bem jurídico penalmente protegido.[170]

A afirmação de que determinado direito possui dignidade penal, com a necessidade de intervenção do direito penal, a partir da criação pelo legislador de tipos incriminadores e suas respectivas sanções exige um caminho profundo de reflexão e cuidado, para que não sejam desrespeitados princípios norteadores de proteção à dignidade da pessoa humana e do Estado Democrático de Direito.

Não se pretende com este trabalho esgotar os fundamentos que justificam a conclusão de que os dados pessoais são bens jurídicos-penais. Contudo, ao que parece, após os estudos apontados até o momento, em razão da progressiva relevância que tal direito fundamental tem adquirido nos tempos atuais, torna-se, no mínimo, inadiável a ampliação de investigação sobre o tema, de modo a propiciar a evolução do direito em consonância com as mudanças da sociedade.

Em que pese o progresso quanto à normatização do tratamento de dados e previsão de adoção de protocolos de segurança, boas práticas e governança, há ainda um longo caminho pela frente no tocante à tutela penal dos dados pessoais, tendo em vista a mudança de conduta dos agentes, que se aproveitam das facilidades implementadas com a oferta de produtos e serviços por diversos meios informatizados, ocasião em que os dados pessoais dos usuários/consumidores são expostos a diversas vulnerabilidades.

Após a análise do cenário atual apresentado no final do capítulo anterior, verifica-se que, em que pese a LGPD possuir a previsão de um sistema de fiscalização

170 STF. Acórdão **HC 107638/PE**. Relator(a): Min. CÁRMEN LÚCIA. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur199231/false. Acesso em 29 de jul. 2024.

e sanções administrativas, esses mecanismos (ainda) se mostram insuficientes para a prevenção e repressão de violações de dados pessoais. Em contrapartida, os dados pessoais têm sido cada vez mais expostos e seus titulares submetidos a riscos de danos materiais, morais, de imagem, entre outros.

Com efeito, a proteção dos dados pessoais foi elevada ao status de direito fundamental na Constituição Federal e representa atualmente um direito autônomo e essencial ao exercício do direito ao desenvolvimento da personalidade. Nesse sentido, pelos fundamentos dogmáticos que foram expostos a respeito da função do Direito Penal na tutela de bens jurídicos, esse novo direito merece maior atenção para alcançar a efetividade de sua proteção.

3.3 Responsabilização penal de pessoas jurídicas no Brasil

A doutrina tradicional e dominante considera como a base fundamental de todo fato-crime a existência de um comportamento humano, seja por meio de uma ação ou uma omissão dirigida a um resultado consistente em uma lesão ou perigo de lesão a um bem-jurídico. Além do comportamento humano, este deve ser típico, ilícito e culpável, conforme o conceito tripartido de crime adotado majoritariamente.[171]

Como primeiro elemento de estudo no tocante ao substrato da tipicidade, a ação pode ser definida como “qualquer comportamento humano, comissivo ou omissivo, abrangendo, pois, a ação propriamente dita, isto é, a atividade que intervém no mundo exterior, como também a omissão, ou seja, a pura inatividade”, praticada sobre o domínio da vontade, que constitui o elemento subjetivo do tipo (dolo ou culpa).[172]

Desse modo, pressupõe-se que a legitimidade ativa necessária para a prática de um crime é a exigência de um ato praticado por uma pessoa natural, sendo, via de regra, vedado à pessoa jurídica responder criminalmente em razão do exercício de suas atividades empresariais. O entendimento se fundamenta na justificativa de que somente a pessoa natural age volitivamente com dolo ou culpa, carecendo as pessoas

171 TOLEDO. Francisco de Assis. Princípios básicos do direito penal. São Paulo: Saraiva, 1994. p. 82.

172 Ibid.

jurídicas desse elemento subjetivo essencial. No entanto, a própria Constituição Federal prevê a possibilidade de imputação de crime contra o Meio Ambiente.[173]

A Constituição Federal ainda prevê a possibilidade de regulamentação de lei para a definição de responsabilidade penal da pessoa jurídica por infrações praticadas contra a ordem econômica e financeira, bem como contra a economia popular.[174]

O tema da responsabilização criminal de pessoa jurídica ainda encontra diversas controvérsias diante da ausência de completa regulamentação sobre a extensão e efeitos de uma eventual condenação. Com efeito, os tribunais, principalmente o Superior Tribunal de Justiça são acionados para realizar a interpretação da lei relacionadas às questões em que os dispositivos legais carecem de clareza.

Em que pese a possibilidade de imputação criminal a empresas ser assunto de grande debate no campo jurídico e acadêmico, certo é que, ao longo dos últimos anos, houve um aumento da discussão sobre a necessidade de expansão das hipóteses de responsabilização da pessoa jurídica, principalmente em decorrência da realidade trazida pela já citada Sociedade do Risco.

O presente trabalho não possui como objeto de estudo a discussão sobre as imputações à pessoa jurídica em face de violações de dados pessoais, inclusive porque não há regulamentação nesse sentido até esta data. Contudo, diante da relevância que o tema de proteção de dados pessoais tem alcançado em razão da ampliação na utilização dos recursos tecnológicos para o exercício das atividades empresariais, entende-se que o tema necessita de atenção criteriosa por parte da academia e do próprio Legislativo.

Primeiramente, não há que se falar no desenvolvimento de argumentos para que se possa justificar a responsabilidade penal da pessoa jurídica em face de violação de dados pessoais (não ao menos neste trabalho). Contudo, diante do arcabouço normativo vigente atualmente, surge o questionamento quanto à possibilidade de imputação de responsabilidade penal aos agentes de tratamento em face de suas responsabilidades legais.

---

173 Segundo o art. 225, da Constituição Federal: § 3º As condutas e atividades consideradas lesivas ao meio ambiente sujeitarão os infratores, pessoas TOLEDO. Francisco de Assis. Princípios básicos do direito penal. São Paulo: Saraiva, 1994. p. 82.físicas ou jurídicas, a sanções penais e administrativas, independentemente da obrigação de reparar os danos causados.

174 Art. 173, § 5º A lei, sem prejuízo da responsabilidade individual dos dirigentes da pessoa jurídica, estabelecerá a responsabilidade desta, sujeitando-a às punições compatíveis com sua natureza, nos atos praticados contra a ordem econômica e financeira e contra a economia popular.

A partir da busca pela resposta a essa pergunta, foram encontrados diversos estudos relevantes a respeito da responsabilidade penal do dirigente da empresa em hipóteses de omissão penalmente relevante, ou seja, quando o responsável se mantém inerte em situações que deveria impedir ou minimizar os danos decorrentes das atividades exercidas pela empresa. Este será o assunto do próximo capítulo, que primeiramente pretenderá discutir sobre o instituto penal da omissão imprópria para, após, adentrar à discussão sobre a possibilidade de aplicação desta modalidade de imputação nos casos de violação de dados pessoais.

4 A OMISSÃO IMPRÓPRIA: TIPICIDADE E ANÁLISE SOBRE A FIGURA DO GARANTE.

Conforme delineado nos capítulos anteriores, não restam dúvidas quanto à importância dos dados pessoais para a sociedade moderna e da necessidade crescente de implementação e aprimoramento de mecanismos de proteção diante das diversas vulnerabilidades que recaem sobre essas informações. Ao passo que o ordenamento jurídico evoluiu nesse sentido com a introdução da proteção de dados como um direito fundamental autônomo na Constituição Federal, constatou-se que é possível afirmar que este direito alcançou a dignidade penal de modo a ser considerado como um bem jurídico-penal merecedor de tutela por este ramo do direito.

Superado o tema sobre a tutela jurídico-penal da proteção de dados, nas próximas linhas serão apresentadas reflexões sobre a aplicabilidade da responsabilidade por omissão no contexto da LGPD e sua intersecção com a lei penal brasileira. À luz do sistema atual de responsabilidade criminal dos dirigentes em face dos tipos penais comissivos por omissão ou também chamados de omissivos impróprios, serão examinadas as atribuições e responsabilidades do controlador de dados (e eventualmente do operador), no sentido de responder ao questionamento sobre a possibilidade de qualificar tais figuras como garantes.

No sistema penal, as normas incriminadoras podem conter enunciados proibitivos, com previsão de um agir (crimes comissivos) ou dispositivos os quais descrevem uma conduta típica consistente em um deixar de agir (omissivos)[175]. Em outras palavras, o tipo pode ser praticado por meio de uma ação proibida ou pela omissão de um comportamento juridicamente exigido.[176]

A partir de uma análise do sistema do fato punível sob o enfoque da metodologia teleológica, a distinção entre a ação e a omissão deve ser determinada pelas valorações políticos-criminais, por meio das quais impõe-se uma natureza normativa e tipicamente condicionada. A estrutura da omissão não será definida pela inatividade do agente (o deixar de agir) por si só, mas em razão da ação juridicamente esperada e devida.[177]

175 TOLEDO, Francisco de Assis. Princípios Básicos de Direito Penal. 5. ed. São Paulo: Saraiva, 2002. p. 116.

176 DIAS, Jorge de Figueiredo. Direito Penal. Parte Geral. Tomo I, 1.ed.São Paulo: Revista dos Tribunais, 2007.p.905.

177 Ibid.p.906.

Por sua vez, os tipos omissivos podem ser próprios ou impróprios. Segundo Assis Toledo, os primeiros consistem em crimes de mera conduta os quais prescindem de nexo causal com o resultado danoso, o autor da infração pode ser qualquer pessoa que se adeque à previsão do tipo penal.[178] Por sua vez, os omissivos impróprios ou também chamados de comissivos por omissão exigem uma relação de dever entre o autor e vítima, de modo que a omissão daquele que atua como garantidor equivaleria a uma ação típica.

A doutrina clássica percorreu um longo percurso na busca pela compreensão e justificação da existência do crime omissivo e a sua equiparação à ação. Na verdade, o tema ainda constitui atualmente um dos pontos mais controversos da teoria do crime. Primeiramente, nos sistemas anteriores ao naturalismo, não havia uma distinção entre ação e omissão, tendo em vista que, assim como defendia Feuerbach, o conceito de delito comissivo seria equivalente ao omissivo, uma vez que para este autor o delito se caracterizava como uma lesão a um direito subjetivo. Por sua vez, a escola hegeliana não percebeu dificuldades ao justificar a existência do tipo omissivo pois, para essa corrente, a ação decorria da vontade do agente e que poderia ser exteriorizada por um ato comissivo ou omissivo, sem prejuízo ao uso desse mesmo critério para ambas modalidades.[179]

Juarez Tavares destaca que a ascensão dos delitos omissivos impróprios somente deu um salto quando houve a mudança na compreensão de que a responsabilidade do agente decorre do resultado produzido em substituição do fundamento da lesão ao direito subjetivo. Dessa forma, a lesão ao bem jurídico passou a ser incorporada na teoria do delito[180]

Martins-Costa menciona a teoria do *aliud agere* elaborada por Luden, segundo a qual adotou a causalidade natural para a configuração da imputação. Para ele, havia uma correspondência entre essas duas espécies, uma vez que mesmo deixando de atuar, juridicamente essa inação seria considerada juridicamente como uma ação. Por meio de sua teoria, houve a separação dos conceitos de delito omissivo próprio e impróprio [181]

178 TOLEDO, Francisco de Assis. Princípios Básicos de Direito Penal. 5. ed. São Paulo: Saraiva, 2002. p. 116.

179 MARTINS-COSTA, Antônio Goya de Almeida. Posição de garantia em direito penal: a problemática da equiparação na omissão imprópria. Rio de Janeiro: Marcial Pons, 2023. p. 32

180 TAVARES. Juarez Estevam Xavier. Teoria dos crimes omissivos. Tese (doutorado). Rio de Janeiro: Universidade do Estado do Rio de Janeiro, 2012. p.26.

181 Como exemplo, o autor cita a mãe que não provê o alimento ao seu filho e este vem a morrer. Na correspondência contrária defendida por Luden, aqui deveria ser considerada uma ação consistente em retirar o alimento do filho. Ibid. p. 36

Por meio desse raciocínio, a omissão seria equivalente a ação, uma vez que em ambos haveria uma causalidade natural, por meio de exteriorização física. Luden acreditava que a omissão de um comportamento esperado representaria a realização de uma ação diversa, contrária à conduta esperada. Essa compreensão baseada na causalidade omissiva não considerava os deveres impostos ao agente para impedir o resultado.

Atualmente, predomina a perspectiva deontológica, por meio da qual os crimes omissivos impróprios pressupõem uma norma denominada de mandado de segundo grau, a qual impõe o dever de agir a alguns grupos restritos de agentes, pessoas que possuem uma "especial relação de proteção com o bem juridicamente tutelado".[182]

Há, pois, um fundamento político-criminal para que seja possível a correspondência de uma conduta comissiva e omissiva, qual seja:

> [...] o de lograr seguramente a conclusão, através de uma autónoma valoração da ilicitude, que, relativamente a um certo tipo de ilícito, o desvalor da omissão corresponde no essencial ao desvalor da acção. E esse será o caso (e aqui deparamos com o fundamento a apontar, do mesmo passo, os seus limites) quando, e apenas quando, sobre o agente recaia um dever de evitar activa ou positivamente a realização típica, rectior, de obstar à verificação do resultado típico [...].[183]

Em outras palavras, a relação entre o agente e o bem jurídico tutelado é regulada por obrigações assumidas em determinadas situações ou expressa em lei ou contrato, de modo que sobre este agente recai uma obrigação positiva de atuar para proteger e evitar o resultado danoso. Quando as obrigações estabelecidas não são cumpridas, o deixar de agir do agente será considerado como a própria ação, devendo ele ser responsabilizado.

Para os crimes comissivos por omissão, o legislador determinou um nexo de causalidade normativo entre a omissão do agente e o resultado.[184] A posição de garantidor será exercida por aquele que possui uma obrigação de conservação, restauração ou reparação do bem jurídico penalmente tutelado. De modo a garantir a compatibilidade do tipo omissivo impróprio com o princípio constitucional da legalidade, Figueiredo Dias entende que é necessário alcançar uma "determinação

182 BITENCOURT, Cezar Roberto. Tratado de Direito Penal. Parte Geral. Vol. 1. 22.ed. rev. e atual. São Paulo: Saraiva, 2016. pag.312.

183 DIAS, Jorge de Figueiredo. Direito Penal. Parte Geral. Tomo I, 1.ed.São Paulo: Revista dos Tribunais, 2007.p.920.

184 TOLEDO, Francisco de Assis. Princípios Básicos de Direito Penal. 5. ed. São Paulo: Saraiva, 2002. p. 116.

rigorosa dos concretos deveres de garantia; e que, consequentemente, o seu catálogo seja o mais estrito e determinado possível".[185]

Nesse contexto, o fundamento político-criminal legitima a existência deste tipo penal de modo a estabelecer uma equiparação da omissão à ação, ao mesmo tempo que oferece limites à sua configuração com a finalidade de que esta comparação não seja indiscriminada. Caso contrário, seria alcançado um alto nível de criminalização inconcebível no atual cenário da ordem jurídica.

Com efeito, o conceito de "garante" é central para a responsabilidade por omissão no direito penal brasileiro. O Código Penal estabelece as hipóteses as quais será encontrada a posição do garante, tendo em vista que nem todo dever jurídico acarretará esse tipo de configuração.[186] O Diploma Penal então prevê em seu art. 13, § 2º que "a omissão é penalmente relevante quando o omitente devia e podia agir para evitar o resultado". Por sua vez, o dever de agir incumbe: a) a quem tenha por lei a obrigação de cuidado, proteção e vigilância (por exemplo, o dever dos pais de proteger seus filhos); b) se de outra forma assumiu a responsabilidade para impedir o resultado (assunção voluntária de um dever de proteção) ou c) se com seu comportamento anterior, criou o risco da ocorrência do resultado.[187]

Percebe-se que somente a constatação da existência do garante não conduzirá à responsabilização automática do agente, pois ele representa um dos requisitos para a configuração de uma conduta comissiva por omissão. Portanto, a imputação de um crime omissivo impróprio exige o cumprimento dos pressupostos da tipicidade, quais sejam:[188]

1) situação típica e a ausência da ação devida;

2) a capacidade de ação do garantidor;

3) o nexo de causalidade normativo ou de evitabilidade;

4) a produção de um resultado e

5) a análise do elemento subjetivo.

A ocorrência da situação típica decorrerá pela constituição dos "pressupostos fáticos que permitem determinar o conteúdo concreto do dever de actuar" [189]. Ou seja,

185 DIAS, Jorge de Figueiredo. Direito Penal. Parte Geral. Tomo I, 1.ed.São Paulo: Revista dos Tribunais, 2007.p.924.

186 TOLEDO, Francisco de Assis. Princípios Básicos de Direito Penal. 5. ed. São Paulo: Saraiva, 2002. p. 117.

187 BRASIL. DECRETO-LEI N. 2.848, de 07 de dezembro de 1940. Disponível em https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm.

188 LUZ, Ilana Martins. A responsabilidade penal por omissão e os programas de compliance. 2017. Tese (Doutorado) – Universidade de São Paulo, São Paulo, 2017. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2136/tde-15032021-232238/. Acesso em: 31 maio 2024.p. 189.

189 DIAS, Jorge de Figueiredo. Direito Penal. Parte Geral. Tomo I, 1.ed.São Paulo: Revista dos Tribunais, 2007.p.924.

nos crimes omissivos impróprios, deve-se constatar a criação de um risco provocado, pelo agente garantidor e responsável pela ocorrência de um resultado típico.

A seguir, serão analisados os fundamentos para a compreensão da figura do garante. Ainda hoje, há diversas discussões na doutrina sobre a definição dos pressupostos necessários para estabelecer os deveres jurídicos necessários à imputação penal pela omissão imprópria, sendo considerada atualmente uma das questões mais controversas na teoria do crime.

Os crimes omissivos impróprios são delitos especiais quanto ao sujeito, tendo em vista que sobre ele pesa um dever especial de impedir a ocorrência de um dano. Nesse contexto, para compreender as hipóteses de configuração do dever do garante, diversas teorias foram criadas a fim de encontrar respostas condizentes com o sistema principiológico do direito penal.

Em linhas gerais, podem ser citadas duas perspectivas dominantes na doutrina sobre a aplicação da responsabilidade por omissão. A primeira denominada de teoria formal, criada por Feuerbach e a Teoria Material, desenvolvida por Kaufmann, Schünemann e Jakobs. A teoria material pode ser subdividida em dois fundamentos: teoria do domínio, defendida por Schünemann e a teoria da função (Jakobs). A seguir são analisadas as características de cada uma delas.

4.1. Teoria dos deveres formais.

A teoria dos deveres formais criada pelo jurista e filósofo alemão Feuerbach consiste no entendimento de que o dever de garante deve estar positivado na lei ou no contrato, a fim de que seja respeitado o princípio da legalidade e, assim, a segurança do direito penal. Trata-se, pois, de uma perspectiva puramente formal quanto ao conceito de garante. Tal teoria foi duramente criticada por parte da doutrina, uma vez que este entendimento foi superado após os valores neokantianos terem sido introduzidos no direito penal moderno.

Segundo Heloísa Estellita, a crítica quanto à teoria dos deveres formais adotada pelo Código Penal decorre da ausência de substrato material de natureza penal para legitimação da responsabilidade criminal pelos delitos. [190]

190 ESTELLITA, Heloisa. Responsabilidade penal dos dirigentes de empresas por omissão: estudo sobre a responsabilidade omissiva imprópria de dirigentes de sociedades anônimas, limitadas e encarregados de cumprimento por crimes praticados por membros de empresa. São Paulo: Marcial Pons, 2017. p. 82.

Com efeito, a referida teoria foi praticamente abandonada pela doutrina e jurisprudência nos dias atuais, tendo em vista que ela estava fundamentada em critérios insubsistentes. Segundo o entendimento de seu criador, a reponsabilidade penal poderia ser justificada em razão da violação de deveres previstos exclusivamente em norma extrapenal, o que acarretaria na violação ao princípio da legalidade. Ademais, a teoria dos deveres formais não reconhecia a ingerência como hipótese de configuração do dever de garantidor por ausência de previsão legal.

Figueiredo Dias reforça que a principal razão para a superação da teoria dos deveres formais decorre da completa renúncia ao conteúdo dos deveres jurídicos, carecendo, portanto, de um critério material de ilicitude da omissão.[191]

Para sanar tais lacunas, a doutrina passou a buscar o fundamento materiais por meio da teoria do domínio sobre a causa do resultado e pela teoria das funções.

4.2 Teoria material.

Diante da fragilidade da teoria de Feuerbach, foi necessário alcançar um fundamento substancial para a configuração da tipicidade da conduta omissiva. Assim, destaca-se a teoria das funções desenvolvida por Armin Kaufmann em 1959, por meio da qual a perspectiva puramente formal foi substituída pela adoção de um critério material. O autor realizou importantes contribuições para o direito penal de modo a fundamentar o dever do garante em razão das relações especiais de proteção. Em outras palavras, os deveres do garante estão atrelados à função de guarda de um bem jurídico concreto ou na vigilância de uma fonte de perigo.[192]

Para alcançar esse elemento essencial de modo a suprir esta lacuna, podem ser aplicados dois critérios materiais distintos para a fundamentação da posição de garantidor: o domínio ou controle sobre o fundamento do resultado e o de competência organizativas e institucionais, conforme serão apresentadas nos próximos parágrafos.

4.2.1 Teoria do domínio ou controle sobre o fundamento do fato.

Bernd Shünemann desenvolveu a denominada teoria do domínio com o objetivo de alcançar uma equivalência entre a ação e omissão, de modo que pudesse

191 DIAS, Jorge de Figueiredo. Direito Penal. Parte Geral. Tomo I, 1.ed.São Paulo: Revista dos Tribunais, 2007.p.935.

192 Ibid. p.937

ser aplicada a mesma pena a ambos os agentes sem que fosse violado o princípio da igualdade. Segundo a teoria, será constatada a omissão penalmente relevante que enseja a imputação delitiva ao garante quando este tiver o domínio fático sobre a causa ou o fundamento do resultado. Aqui, é possível verificar tal hipótese quando o sujeito possui a função de proteger o bem jurídico desamparado ou pelo dever de vigilância sobre uma fonte de perigo. Assim, segundo Shünemann:

> La equiparación de la omisión con la comisión, fundamentada en el dominio del diretor de la empresa, o bien, hablando en general, del superior en la empresa, pues resultar, pues, tanto de su dominio fáctico sobre los elementos peligrosos del establecimiento como también de su poder de mando sobre los trabajadores fundamentado legalmente; con ello, estas subdivisiones de la posición de garante muestran un alcance diferente e según su muy divergente estructura material; esto es: según las condiciones respectivas para la existencia y la extinción del dominio. [193]

Schünemann destaca a importância político-criminal do crime omissivo impróprio no âmbito da criminalidade da empresa, tendo em vista a dificuldade na delimitação e diferenciação entre ação e responsabilidade nas instituições hierárquicas. A organização da responsabilidade na sociedade decorre de uma descentralização da função de poder e de decisão, o que pode acarretar muitas das vezes em uma “irresponsabilidade organizada” que, por consequência, torna complexa a imputação de um fato delituoso dentro da organização, diante da dificuldade em distinguir os verdadeiros responsáveis.[194]

Ao explicar sobre o tema, Figueiredo Dias esclarece que a teoria do domínio sobre o motivo do resultado adveio da teoria das funções e se subdivide em dois critérios: as “relações de guarda pelo desamparo do bem jurídico”, ou seja, quando o agente detém deveres de salvação em razão da sua posição de garantidor; e pelo “domínio material sobre o foco do perigo”, referente às hipóteses em que o agente possui o dever de vigilância sobre uma causa essencial do resultado, que pode ser uma pessoa ou uma coisa. O Professor ressalva que em ambos será determinante o domínio fático exercido sobre o bem-jurídico ou sobre a fonte do perigo.[195]

---

193 SCHÜNEMANN, Bernd. Cuestiones básicas de dogmática jurídico-penal y de política criminal acerca de la criminalidad de empresa. Anuario de derecho penal y ciencias penales. Madrid, v. 41, n. 2, p. 529-558, mai./ago.1988. Disponível em: https://scholar.google.com.br/scholar?hl=pt-BR&as_sdt=0%2C5&q=sch%C3%BCnemann+bernd+Cuestiones+basicas+de+dogmatica+juridico+penal+y+de+politica+criminal+acerca+de+la+criminalidad+de+empresa&btnG=. Acesso em 31 mai. 2024.

194 Ibid. p. 533.

195 DIAS, Jorge de Figueiredo. Direito Penal. Parte Geral. Tomo I, 1.ed.São Paulo: Revista dos Tribunais, 2007.p.937.

No entanto, a aplicação pura da teoria do domínio sob o fundamento do resultado recebeu censuras por parte da doutrina por possibilitar a ampliação da responsabilização criminal com violação dos princípios basilares do direito penal, como intervenção mínima, fragmentariedade e subsidiariedade.[196]

A crítica também se sustenta em face da adoção, pela referida teoria, do entendimento de que seria possível a imputação jurídico-penal em face de normas extrapenais as quais não preveem ilícitos de qualquer natureza, o que seria contrário ao princípio da subsidiariedade, que determina que o direito penal somente deve intervir nas situações em que as demais esferas de responsabilização não forem suficientes ou adequadas para a proteção de determinado bem jurídico.[197]

Figueiredo Dias defende a adoção de uma teoria “material-formal”, concepção adotada por parte da doutrina alemã moderna. O autor explica que os deveres de garantia devem ser considerados conforme a junção das duas teorias, sendo que o aspecto material consiste naquele apresentado por Shünemann combinado com uma fonte formal do dever de garantia:

> A verdadeira fonte dos deveres e das posições de garantia reside em algo muito mais profundo, a saber, na valoração autônoma da ilicitude material, completadora do tipo formal, através do qual a comissão por omissão vem a equiparar-se à acção na situação concreta, por força das exigências de solidariedade do homem para com os outros homens dentro da comunidade.[198]

No entanto, o autor complementa que um aparato de concepções morais não pode substituir os deveres jurídicos, ao passo que “toda manifestação imposta de solidarismo tem de se apoiar em um claro vínculo jurídico”.[199] Ele complementa que o garante pode responder em razão dos deveres de proteção e assistência a um bem desamparado, em decorrência do estabelecimento de relações fáticas, as quais demandam a caracterização de dependência do bem jurídico em face do agente, que podem superar até mesmo as previsões legais. Como por exemplo dessa hipótese, podem ser citadas as relações de proteção familiar.

Os deveres também podem ser derivados da assunção de funções de guarda e assistência de bens jurídicos carentes de proteção. Esta espécie origina-se dos

196 LUZ, Ilana Martins. A responsabilidade penal por omissão e os programas de compliance. 2017. Tese (Doutorado) – Universidade de São Paulo, São Paulo, 2017. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2136/tde-15032021-232238/. Acesso em: 31 maio 2024.p. 204.

197 Ibid. p. 200.

198 DIAS, Jorge de Figueiredo. Direito Penal. Parte Geral. Tomo I, 1.ed.São Paulo: Revista dos Tribunais, 2007.p.938.

199 Ibid.

deveres formais contratuais. Contudo, mais do que a existência de uma relação contratual válida, necessária a situação fática que enseja uma relação de confiança.[200]

A responsabilidade do garante ainda pode repousar em uma terceira hipótese, qual seja, nos deveres de vigilância e segurança em decorrência de uma fonte de perigo - a ingerência. Ou seja, aquele que com seu comportamento cria uma situação de perigo que pode atingir outras pessoas, responderá pelos danos e riscos causados. No entanto, para a configuração do garante nessa hipótese torna-se necessário o cumprimento de certos requisitos. Primeiramente, deve se tratar de um resultado típico objetivamente imputável. O segundo elemento necessário consiste na ilicitude na criação do perigo. Assim, não haverá a responsabilização pela ingerência quando a conduta for justificada.[201]

Figueiredo Dias defende a responsabilidade do garante em razão do seu dever de fiscalização das fontes de perigo no âmbito de domínio próprio, como por exemplo, empresários, comerciantes, indústrias e outros estabelecimentos nos quais seus responsáveis possuem a obrigação de fornecer a segurança necessária aos seus empregados e demais pessoas que podem acessar as fontes de perigo. O fundamento material para essa conclusão decorre do poder de disposição que esses agentes possuem sobre as atividades que exercem, atrelada às características da "sociedade do risco" por meio do qual surge o dever de afastar ou minimizar os perigos de sua atuação.[202]

4.2.2 Teoria da função: competências organizativas e institucionais

Outro critério possível de ser utilizado para justificar materialmente a posição do garantidor foi proposto por Jakobs, que consiste em um fundamento essencialmente normativo.

A primeira vertente leva em consideração os deveres negativos decorrentes das competências de uma organização. Por meio desse critério, o agente será responsável pelos danos alheios gerados em razão do modo de estruturação de sua

200 DIAS, Jorge de Figueiredo. Direito Penal. Parte Geral. Tomo I, 1.ed.São Paulo: Revista dos Tribunais, 2007.p.942.

201 Ibid.p.946

202 Ibid. p. 948

vida, seja por meio do seu próprio corpo ou por intermédio de meios materiais, podendo ser por objetos e pessoas.[203]

Por sua vez, a segunda se fundamenta nas competências administrativas e institucionais do dirigente (competência institucional).[204]

> A responsabilidade por organização exige que o agente infrinja o dever de assegurar que o seu âmbito de organização, ou alguma causa que lhe incumbia evitar, não se amplie de modo a causar danos aos demais. Não obstante, o dever de garantia pode se basear materialmente também na responsabilidade institucional, e nesse caso há violação de um dever positivo, que impõe ao indivíduo dever de solidariedade perante os demais decorrente da entrada voluntária do agente em uma instituição jurídica.[205]

As competências institucionais decorrem de normas e recaem sobre as pessoas que possuem uma relação especial em instituições primordiais. Em outras palavras, a competência por organização está fundamentada em deveres negativos, enquanto a competência institucional se apoia em deveres positivos.

Em resumo, para configuração da responsabilização do garante, além da necessidade de verificação de uma das três hipóteses previstas no art. 13, §2º do Código Penal, será necessário constatar se, na prática, o agente possuía a capacidade para agir e o poder real de evitar o resultado. Ou seja, a mera subsunção formal dos requisitos do referido dispositivo não será capaz de gerar a imputação do fato ao dirigente.

Em que pese a discussão sobre os fundamentos para a equiparação entre ação e omissão perdurarem até hoje na dogmática jurídico-penal, é possível concluir que a teoria criada por Shünemann pode ser aplicada como um fundamento mais plausível para justificar a referida equiparação. Nesse aspecto, o fundamento comum da imputação nas duas formas de condutas puníveis encontra-se na teoria do domínio.[206]

Martins-Costa defende que a utilização do argumento da similitude ou semelhança para justificar essa conclusão, adotado por Roxin, se torna o mais concludente, uma vez que a adoção do domínio sobre o fundamento do resultado para

---

203 ESTELLITA, Heloisa. Responsabilidade penal dos dirigentes de empresas por omissão: estudo sobre a responsabilidade omissiva imprópria de dirigentes de sociedades anônimas, limitadas e encarregados de cumprimento por crimes praticados por membros de empresa. São Paulo: Marcial Pons, 2017. p. 91.

204 Ibid. p. 88.

205 MAYRINK, Renata Pereira. Responsabilidade penal do compliance officer: a omissão imprópria e os pressupostos para a tipicidade. São Paulo: D´Plácido, 2022. p. 61 e 62.

206 MARTINS-COSTA, Antônio Goya de Almeida. Posição de garantia em direito penal: a problemática da equiparação na omissão imprópria. Rio de Janeiro: Marcial Pons, 2023. p. 240.

os crimes omissivos seria equivalente à aplicação do critério do domínio do fato exigido para os crimes comissivos.[207]

De igual forma, Heloisa Estellita acolhe a teoria de Shunemann como a mais acertada. Isso porque, em que pese não ser possível a consideração da norma extrapenal como único fundamento para a determinação da posição do garantidor para fins penais, ela será útil para estabelecer os parâmetros de delimitação dos deveres e ações juridicamente esperadas e exigíveis do agente, tendo em vista que "o ordenamento jurídico espera do agente apenas as condutas que lhe eram juridicamente exigíveis e físico-realmente possíveis, nada mais".[208]

Ainda importa destacar outro argumento que a doutrina se utiliza para defender a teoria de Schünemann, qual seja, o de oferecer um substrato material que viabiliza um controle empírico dos resultados, ou seja, a equiparação da omissão se dará pela constatação concreta a existência do domínio sobre o fundamento do resultado.[209]

Portanto, encerrada a análise sobre a posição de garante, ressalta-se que a sua existência não será suficiente para a configuração da tipicidade no crime omissivo impróprio. Conforme mencionado anteriormente, será necessária a comprovação do nexo de causalidade, da ocorrência do resultado e da presença do elemento subjetivo do garante. Quanto a este último elemento, destaca-se ainda a necessidade de configuração do dolo, refletido no seu conhecimento da situação que o coloca nesta posição e de que devia e podia evitar o resultado danoso.

A doutrina dominante defende atualmente a necessidade de configuração do dolo nos crimes omissivos da mesma forma como é exigido para os tipos comissivos Assim, torna-se imprescindível que o garante conheça a existência do risco e possua a vontade de se omitir diante da situação. O agente garantidor deve prever o resultado como consequência da sua omissão[210]

Nesse sentido, não se pode afastar da análise pormenorizada dos requisitos acima para a conclusão da existência de um crime omissivo impróprio, sob pena de

207 MARTINS-COSTA, Antônio Goya de Almeida. Posição de garantia em direito penal: a problemática da equiparação na omissão imprópria. Rio de Janeiro: Marcial Pons, 2023. p. 240.

208 ESTELLITA, Heloisa. Responsabilidade penal dos dirigentes de empresas por omissão: estudo sobre a responsabilidade omissiva imprópria de dirigentes de sociedades anônimas, limitadas e encarregados de cumprimento por crimes praticados por membros de empresa. São Paulo: Marcial Pons, 2017. p. 87.

209 MARTINS-COSTA, Antônio Goya de Almeida. Posição de garantia em direito penal: a problemática da equiparação na omissão imprópria. Rio de Janeiro: Marcial Pons, 2023. p. 240.

210 DIAS, Jorge de Figueiredo. Direito Penal. Parte Geral. Tomo I, 1.ed.São Paulo: Revista dos Tribunais, 2007.p.955.

permitir uma ampliação excessiva da responsabilidade por esta espécie de imputação, a ponto de gerar a violação dos princípios norteadores do Direito Penal.

Apresentado um panorama conceitual sobre o instituto da omissão imprópria e seus requisitos, na próxima seção serão levantadas reflexões a respeito dos deveres legais do controlador e operador no tratamento de dados, de modo a verificar se será possível afirmar que estes agentes podem ser tratados como garantes nas condutas comissivas por omissão em razão da violação dos direitos à proteção de dados pessoais.

4.3 Agentes de tratamento e a posição de garante.

Conforme apontado na seção anterior, a imputação criminal pela ocorrência de um crime comissivo por omissão perpassa necessariamente pela constatação da existência do agente que detenha uma relação jurídica especial com o bem jurídico, denominado de garante. Sem esta figura, não é possível falar em crime omissivo impróprio e, para isso, a situação fática precisa se adequar a uma das três hipóteses do artigo 13, §2º do Código Penal.

Como recorte para o estudo proposto, interessa a análise da alínea “a” do § 2º do art. 13 do Código Penal, de modo a refletir se, em determinadas situações, residiria a possibilidade de enquadramento do controlador de dados pessoais como garante por omissão imprópria e, por conseguinte, a sua responsabilização pelo tratamento irregular que acarrete uma violação do direito fundamental à proteção de dados.

Primeiramente, a partir da leitura do dispositivo acima citado, verifica-se que o agente será considerado garante quando “tenha por lei obrigação de cuidado, proteção ou vigilância”. Cabe, pois, analisar se há na legislação de proteção de dados pessoais a previsão das referidas incumbências ao controlador.

O capítulo VII da LGPD dispõe sobre a segurança e as boas práticas, com destaque à primeira seção que estabelece normas sobre o sigilo dos dados. Segundo o art. 46,

> Os agentes de tratamento **devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais** de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (grifo nosso)

Ainda segundo a referida legislação, a ANPD deverá estabelecer os critérios técnicos mínimos para o alcance desses deveres por parte dos agentes de tratamento, que deverão ser cumpridos desde a fase de concepção do produto ou serviço e durante a sua execução.

Destaque-se, ainda, o art. 49 do mesmo diploma, segundo o qual os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Indo além, a LGPD determina aos agentes de tratamento ou qualquer outra pessoa que intervenha no processo de tratamento de dados, a obrigação de garantir a segurança da informação prevista na LGPD no tocante aos dados pessoais, mesmo após a finalização do tratamento.[211]

Conforme se extrai das conclusões apresentadas no item anterior sobre os deveres de garante nos termos do art. 13, §2º, alínea “a” do Código Penal, é possível afirmar que a LGPD constitui uma lei em sentido formal que estabelece aos agentes de tratamento um dever expresso de garantia da proteção dos dados pessoais dos seus usuários. A responsabilidade por omissão dos agentes de tratamento quando da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, decorre em função da ação juridicamente esperada e devida pelo agente, em especial o controlador, tornando esta omissão jurídico-penalmente relevante.[212]

Nesse sentido, entende-se que é possível o controlador ser considerado como garante para fins de responsabilização por omissão imprópria, quando, conhecedor da situação de violação, for constatada a ausência da adoção das medidas necessárias para a tutela dos dados pessoais. O controlador consiste no dirigente responsável pela tomada de decisões quanto ao tratamento de dados pessoais. Assim, ele se adequa aos requisitos necessários para figurar como garante.

Por outro lado, como visto anteriormente, o operador é responsável pela realização do tratamento de dados pessoais em nome do controlador, ou seja, seu dever consiste em exercer suas atribuições em cumprimento das normas e dos comandos lícitos do controlador. Inicialmente, a conclusão imediata que poderia ser

211 O artigo 47 da LGPD determina: Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

212 DIAS, Jorge de Figueiredo. Direito Penal. Parte Geral. Tomo I, 1.ed.São Paulo: Revista dos Tribunais, 2007.p.907.

alcançada seria a de que o operador não poderia ser considerado como garante para fins penais. Contudo, se houver o descumprimento de suas obrigações legais, ele poderá ser equiparado ao controlador, nos termos do art. 42, parágrafo primeiro, inciso I da LGPD:

> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

Considerando tal dispositivo, conclui-se que, primariamente, somente o controlador deve ser enquadrado como garante para fins de responsabilização por omissão imprópria, ao passo que o operador somente será considerado como garante se ocorrer uma das hipóteses previstas no inciso acima indicado.

De qualquer modo, o próprio artigo 46 estabelece o dever de segurança e proteção dos “agentes de tratamento” e, segundo a própria lei, nesta expressão estão englobados o controlador e o operador de dados pessoais. Pela interpretação sistemática dos dispositivos do Código Penal e LGPD, o operador não pode ser completamente excluído de uma possível imputação, em que pese o poder de decisão residir nas mãos do controlador.

Com efeito, associado ao contexto dogmático apresentado quanto à imputação pela omissão imprópria, as disposições inseridas pela LPGD a respeito das obrigações dos agentes e terceiros que intervenham no processo de tratamento de dados, constata-se que há fundamentos para afirmar que o controlador e o operador (sem descartar outros agentes, mas que neste estudo proposto fogem ao objeto de pesquisa) se encaixam como garantes em suas atividades corporativas.

Tal entendimento encontra-se em consonância com a adoção da teoria de Shünemann para justificar a existência da posição de garante por meio da análise das obrigações legais expressas dos deveres de segurança e garantia de proteção dos dados pessoais. No entanto, não se pode deixar afastar a necessidade de comprovação do domínio sobre o fundamento do resultado como requisito indispensável à responsabilização do controlador.

Dessa forma, o critério formal da teoria encontra-se presente diante da análise dos dispositivos da LGPD acima mencionados. Por outro lado, a constatação de que o controlador possuía o domínio do resultado, qual seja, a violação dos dados

pessoais, dependerá na análise fática que potencialmente ensejou o tratamento indevido ou ilícito. Somente com a associação desses dois critérios pode-se concluir pela ocupação do controlador de dados na posição de garante no crime omissivo impróprio.

Nesse sentido, será preciso demonstrar que o controlador falhou em adotar medidas de segurança necessárias, o que poderia ter evitado a infração. Os exemplos incluem não realização de auditorias regulares, falhas na capacitação de funcionários ou ausência de políticas claras de proteção de dados.

De modo a elucidar a possibilidade de aplicação prática deste entendimento, imagina-se a hipótese de uma empresa de tecnologia que coleta e armazena dados pessoais de milhões de usuários, incluindo dados sensíveis. O controlador da referida instituição foi comunicado pelo encarregado do tratamento de dados a respeito da necessidade de atualização de softwares e aquisição de novas ferramentas de segurança, pois foram detectadas diversas vulnerabilidades, conforme relatório apresentado.

No referido documento, estava expressa a informação de que os recursos de segurança utilizados pela empresa estavam obsoletos e precisavam ser substituídos urgentemente. Em que pese ter sido advertido sobre os riscos iminentes de vazamento de dados, o controlador conscientemente deixou de adotar as medidas sugeridas em razão do custo necessário para a sua execução. Como era esperado, houve uma invasão dos sistemas da empresa, que acarretou na subtração dos dados pessoais de todos os clientes. Essas informações foram comercializadas na *deepweb* e utilizadas posteriormente para a prática de crimes, como estelionato e outras fraudes.

Pode-se afirmar que, deixando de agir, o controlador assumiu o risco de provocar um resultado danoso. O agente possuía o conhecimento dos seus deveres legais e detinha o domínio sobre fundamento do resultado, uma vez que era o responsável pela tomada de decisão quanto às implementações indicadas pelo encarregado. Nessa situação hipotética, é possível visualizar, em tese, a presença do dolo eventual na conduta omissiva do controlador, podendo ensejar a sua responsabilização pelos crimes ocorridos.[213] A imputação de dolo poderá ser

213 Segundo o art. Art. 18 - Diz-se o crime: I - doloso, quando o agente quis o resultado ou assumiu o risco de produzi-lo. BRASIL. **Decreto 2.848, de 07 de dezembro de 1940**. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 31 de out. 2024.

comprovada por meio de evidências de que o controlador tinha conhecimento de que sua falta de ação poderia resultar na exposição ou subtração de dados pessoais.

Repise-se que o Direito Penal deve intervir somente nas situações em que os demais meios de repressão da conduta ilícita não forem adequados ou suficientes para aquela finalidade, em respeito aos princípios da intervenção mínima e subsidiariedade.

Sem dúvidas, a solução mais indicada a ser adotada consiste na implementação de mecanismos preventivos às violações de dados pessoais, ao passo que as sanções devem ser o último recurso na busca pela tutela desse direito. Contudo, torna-se essencial estabelecer clara e rigorosamente o alcance e os respectivos limites dos tipos penalizadores a serem aplicados quando realmente forem necessários.

Com efeito, além das previsões de diversos conceitos, deveres dos agentes de tratamento, as infrações administrativas e sanções cabíveis a serem aplicadas aos transgressores, a LGPD faz previsão de diretrizes voltadas à prevenção do tratamento inadequado ou ilícito de dados pessoais. Tratam-se de padrões de boas práticas e de governança.

4.4 A sociedade do risco e as boas práticas corporativas para prevenção de crimes.

A transformação digital tem redesenhado a maneira como a sociedade interage, trabalha e consome no dia a dia, influenciada fortemente pelas tecnologias da informação e comunicação. Este fenômeno é notável em áreas como comércio eletrônico, educação à distância e serviços governamentais digitais, que não só facilitam o acesso e a eficiência dessas entidades, mas redefinem a natureza das relações entre indivíduos e organizações.

O progresso técnico-científico característico da modernidade resultou em diversos benefícios à sociedade, mas foi acompanhado por consequências negativas, entre elas, o aumento de vulnerabilidades e o risco de danos. A preocupação com o compartilhamento de dados tornou-se constante.

A esta nova realidade foi atribuída a expressão de “Sociedade do Risco”:

> Modernização significa o salto tecnológico de racionalização e a transformação do trabalho e da organização, englobando para além disto muito mais: a mudança dos caracteres sociais e das biografias padrão, dos estilos e formas de vida, das estruturas de poder e das normas cognitivas. [214]

Com o desenvolvimento do Estado Social, houve uma diminuição da preocupação em relação à insuficiência de produção de riquezas, em razão do crescimento da produtividade humana e tecnológica, ao passo em que houve o aumento da preocupação quanto ao crescimento de novos riscos sociais. A globalização impacta a possibilidade de controle de situações de riscos, pois estes se tornaram mais complexos.

Na então chamada Sociedade do Risco, houve um aumento de estudos e discussões sobre a necessidade de adoção de políticas internas de conformidade por parte das organizações públicas e privadas. Tais padrões de boas práticas possuem o condão de direcionar as instituições na condução de suas atividades dentro da legalidade e do respeito aos princípios constitucionais e legais no seu âmbito de atuação.

Com efeito, a Sociedade do Risco é caracterizada pelo aumento da vulnerabilidade das informações pessoais, expondo indivíduos e instituições a uma variedade de ameaças, como vazamentos de dados e crimes cibernéticos. Este cenário demanda uma resposta concreta das organizações, tanto públicas quanto privadas, para salvaguardar dados sensíveis e garantir a integridade das transações digitais. A implementação de boas práticas de governança se torna essencial, integrando estratégias de mitigação de riscos, políticas de segurança cibernética e conformidade com as regulamentações legais.

Como explanado, esta nova realidade social expandiu a relevância do direito à proteção de dados pessoais, exigindo dos dirigentes das empresas a preocupação com o cumprimento de políticas que, dentre outras funções mais abrangentes, possuem o objetivo de prevenir os danos decorrentes de violações de direitos dos consumidores e usuários.

No Brasil, a LGPD estabelece deveres rígidos sobre o tratamento de dados por empresas e órgãos governamentais, para garantir o direito à privacidade e à proteção dos dados dos cidadãos. Sob este diploma legal, as organizações são obrigadas a aderir a princípios como a transparência, a finalidade e a necessidade, além de

214 BECK, Ulrich. Sociedade de risco. Rumo a uma outra modernidade. São Paulo: 34, 2010. p. 23.

implementar medidas de segurança adequadas para proteger informações sensíveis. Para viabilizar a adoção das boas práticas de segurança, a ANPD pode estabelecer diretrizes para a adoção de padrões técnicos mínimos a serem utilizados desde a fase da concepção do produto ou serviço até a sua realização.[215]

Ainda, para a efetivação na execução de medidas de segurança preventivas, a LGPD prevê que os agentes de tratamento podem formular regras de boas práticas e de governança que "estabeleçam as condições de organização, regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos"[216]

Portanto, surge a necessidade por parte das organizações de promoverem a adequação de procedimentos internos e externos formados a partir de diretrizes que serão estabelecidas dentro de um programa de *compliance.*

> Ao adotar um programa de integridade empresarial, calcado na boa-fé e nos demais princípios do art. 6º da LGPD, o agente controlador previne a ocorrência de eventos danosos à sua imagem, reduz o risco da incidência de sanções administrativas – que podem chegar ao patamar de cinquenta milhões de reais – e se beneficia do acesso a mercados internacionais que condicionam certos negócios jurídicos à adequação dos estatutos da empresa a padrões de segurança digital.[217]

Atualmente, há um predomínio da informatização na maior parte das atividades que demandam o tratamento de dados pessoais. Os recursos tecnológicos garantem maior eficácia o alcance dos objetivos das organizações e também possibilitam a disponibilização de ferramentas de proteção da informação. Contudo, esses sistemas possuem vulnerabilidades que podem ser aproveitadas por agentes maliciosos. Nesse contexto, no ramo da ciência da computação foram criadas práticas para a segurança da informação por meio de atributos de confidencialidade, integridade e disponibilidade.[218]

Para a criação de um programa de segurança da informação, a organização deverá adotar rígidos controles técnicos e administrativos. Estes dizem respeito à

---

215 Art. 46. Lei Federal n. 13.709, de 14 de agosto de 2018. Disponível em http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 21 de jul. 2023.

216 Ibid. Art. 50.

217 LODDER, George Neves. Proteção de dados pessoais e investigação criminal. Autoridade Nacional de Proteção de Dados: questões penais.Brasília:2020. p.121.

218 MENKE, Fabiano; GOULART, Guilherne Damasio. Segurança da Informação e vazamento de dados. In: DONEDA, Danilo et al (coord). Tratado de Proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p. 344.

promoção da conformidade das ações com a LGPD e que objetivam a organização da segurança da informação da empresa. Os controles técnicos se referem ao uso de ferramentas como *firewalls*, antivírus, controle de acessos, criptografias e outras.[219]

Essas medidas de controle da segurança da informação estão previstas no art. 46 da LGPD[220] e consistem na efetivação de um dos princípios basilares da proteção de dados pessoais, qual seja, o princípio da segurança, definido como a "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"[221]

Como explica Arthur de Brito Gueiros, caso a organização decida por não adotar um programa de segurança da informação, mas se em seu setor de atuação houver exigência ou mesmo determinação legal, a responsabilidade poder ser atribuída ao dirigente que se omitiu, havendo "uma sintonia entre a situação de *non-compliance* e a imputação de autoria pela posição de garantidor, fundamentando-se uma omissão punível dos dirigentes".[222]

As boas práticas também podem incluir ações educativas, ferramentas internas para monitoramento e mitigação de riscos. O seu intuito consiste no desenvolvimento e incorporação pelos integrantes da instituição de uma cultura de respeito e cumprimento às normas.

A adequação à LGPD não é apenas uma obrigação legal, mas uma oportunidade para as empresas demonstrarem responsabilidade social e se diferenciarem no mercado. A confiança do consumidor se torna um ativo crucial em um ambiente onde o compartilhamento de informações é inevitável. Assim, as organizações que implementam e mantêm sistemas de governança de dados sólidos não apenas atendem às normas legais, mas também cultivam um ambiente de confiança, demonstrando seu compromisso com o respeito aos direitos dos usuários.

Nesse sentido, a sociedade do risco impõe às organizações públicas e privadas o desafio e a responsabilidade de protegerem as informações em um mundo

219 MENKE, Fabiano; GOULART, Guilherne Damasio. Segurança da Informação e vazamento de dados. In: DONEDA, Danilo et al (coord). Tratado de Proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p. 344.

220 Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. BRASIL. Lei Federal n. 13.709, de 14 de agosto de 2018. Disponível em http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 21 de jul. 2023.

221 Ibid.

222 SOUZA, Arthur de Brito Gueiros. Programas de compliance e a atribuição de responsabilidade individual nos crimes empresariais. In: VITORELLI, Edilson (coord.). Temas atuais do Ministério Público Federal.p.25.

conectado. A implementação de práticas de governança eficazes e a conformidade com legislações são fundamentais não só para mitigar riscos, mas também para promover uma cultura de respeito e proteção aos dados pessoais, essencial para a manutenção da confiança e credibilidade em um mercado digital dinâmico e em constante evolução. A ANPD possui papel crucial nesse movimento de conscientização e incentivo à adoção de boas práticas e governança.

Outro aspecto importante quanto à incorporação desses padrões corporativos para a proteção de dados pessoais refere-se à consolidação de posturas éticas por parte das instituições quanto ao cumprimento das normas sobre o tema. Os mecanismos explicitados acima não podem ser aplicados com o fim único de evitar eventual responsabilização dos agentes de tratamento, mas este deve ser somente uma consequência de uma conscientização sobre o uso ético das informações coletadas, armazenadas e utilizadas posteriormente.

Atualmente há uma crítica crescente quanto à utilização dos dados pessoais coletados para identificação de perfis para direcionamento de publicidade. Os algoritmos traçam as preferências dos usuários e controlam o que pode ser disponibilizado, quase como se lessem seu pensamento para lhes apresentar soluções para os seus problemas a um clique de distância. Não é incomum relatos de que aplicativos de redes sociais “ouvem” as conversas despretensiosas sobre algum produto ou serviço e, como num passe de mágica, o próximo acesso ao aplicativo estará repleto de anúncios sobre aquele assunto mencionado.

Desse modo, surge uma discussão ética que não pode ser ignorada. O Big Data permite o processamento de vastas quantidades de dados, gerando *insights* valiosos para negócios e aprimorando serviços, como a otimização da publicidade. No entanto, à medida que as empresas utilizam dados pessoais em larga escala, a linha entre inovação e violação de privacidade pode se tornar tênue. Questões éticas sobre como os dados são coletados, usados e armazenados são fundamentais. O uso de algoritmos deve ser acompanhado de uma reflexão ética, garantindo que não sejam ultrapassados os limites estabelecidos e resultem em violações de privacidade.

Recentemente tem sido discutida sobre a estratégia adotada por algumas plataformas quanto à realização de cobrança de valores para que os dados pessoais não sejam coletados. O Comitê Europeu de Proteção de Dados – CEPD – emitiu comunicado a respeito da prática anunciada por grandes grupos, a exemplo da Meta, que lançou uma versão *premium* do Facebook e Instagram para a eliminação da

publicidade nos perfis dessas redes sociais. Assim, caso o usuário não tenha interesse em realizar a assinatura deste serviço, ele estará manifestando o consentimento para a coleta dos seus dados.[223]

Em que pese essa estratégia não ser proibida na União Europeia, a discussão sobre a oferta da versão *premium* coloca em evidência a conduta ética das referidas plataformas, as quais estabeleceram um preço para respeitarem a privacidade dos seus usuários.

Outra preocupação que vem crescendo exponencialmente consiste no tratamento de dados no uso de inteligência artificial generativa. Em outra situação que envolve o mesmo grupo empresarial, a ANPD realizou monitoramento e aprovou plano de conformidade para tratamento de dados pessoais pela Meta com a finalidade de realizar treinamento de sistemas de inteligência artificial generativa.

Inicialmente, a autoridade suspendeu o uso de dados pessoais para realização do referido treinamento, tendo em vista que entendeu que tal tratamento poderia provocar risco iminente de danos graves ou de difícil reparação aos usuários das plataformas. Posteriormente, houve a aprovação do Plano de Conformidade, por meio do qual a Meta assumiu o compromisso de adoção de diversas medidas, a fim de viabilizar maior transparência no tratamento dos dados pessoais.[224]

A cada nova ferramenta tecnológica disponibilizada aos usuários, haverá um campo incerto para o aumento dos riscos decorrentes do fornecimento de dados pessoais na rede. As instituições precisam atualizar constantemente os seus mecanismos de segurança para acompanhar essas inovações, de modo que torna ainda mais relevante o estabelecimento de boas práticas e governança corporativas sólidas.

Por todo esse contexto, o cumprimento das normas de proteção de dados precisa caminhar ao lado da constante preocupação com a conscientização das organizações para uma condução ética de suas atividades, cujas deliberações não podem estar lastreadas somente em custos e rentabilidade dos seus negócios. Não é

---

223 EL PAÍS. ¿Puede facebook poner precio a mi privacidad? 2024. disponível em: https://elpais.com/economia/negocios/2024-04-28/puede-facebook-poner-precio-a-mi-privacidad.html. Acesso em 31 out. 2024.

224 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANDP). **Voto Nº 23/2024/DIR-JR/CD. Processo nº 00216.004529/2024-36.** 28 ago. 2024. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/deliberacoes-do-conselho-diretor-1/circuitos-deliberativos-2024/cd-18-2024-votos.pdf. Acesso em 31 out. 2024.

demais relembrar que a LGPD prevê o respeito ao princípio da boa-fé no tratamento de dados.[225]

A fim de enriquecer as reflexões possíveis a respeito da proteção dos dados pessoais, torna-se importante levantar informações sobre a normatização do tema no campo internacional, principalmente no tocante à efetividade dos dispositivos de responsabilização em face do tratamento indevido e ilícito de dados pessoais.

4.5 Cenário internacional sobre proteção de dados pessoais no campo penal

Como mencionado inicialmente, a LGPD representa um divisor normativo no tocante à regulamentação da proteção dos dados pessoais, não somente no que tange à definição de sanções administrativas pela violação do tratamento de dados pessoais, mas por toda a estrutura conceitual e pelo estabelecimento de uma política nacional de proteção dos dados pessoais.

Ainda que seja reconhecida a importância desta evolução legislativa, é fato que nos quase seis anos de vigência de grande parte da LGDP, o cumprimento efetivo de disposições relevantes tardou em razão de diversos fatores, como a criação da ANPD (que completa quatro anos de existência) e a necessidade de regulamentação de dispositivos necessários à sua efetiva atuação, como o estabelecimento de critérios para a aplicação das sanções previstas, dentre outras dificuldades que este novo setor ainda tem enfrentado.

Como destacado, a LGPD foi concebida por inspiração do Regulamento Geral de Proteção de Dados vigente na União Europeia desde o ano de 2018, o que faz sentido debruçar os olhos sobre as experiências dos seus países integrantes para que o ordenamento jurídico pátrio possa aprender com as experiências positivas e se desenvolver nesta seara.

No âmbito da União Europeia, a Diretiva 95/46/CE de 1995 representa um marco importante, pois estabeleceu as bases da proteção de dados pessoais a serem adotadas por seus países membros. A Diretiva introduziu princípios fundamentais nesta temática.[226] Posteriormente, o Regulamento (EU) n.º 2016/679 (RGPD), revogou a Diretiva e trouxe um conjunto de regras mais rigorosas sobre a proteção de dados,

225 Artigo 6º. BRASIL. Lei Federal n. 13.709, de 14 de agosto de 2018. Disponível em http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 21 de jul. 2023.

226 UNIÃO EUROPEIA. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:31995L0046. Acesso em 31 out. 2024.

reforçando os direitos dos indivíduos e impondo obrigações mais severas às organizações.[227]

Na Espanha, está em vigor a Lei Orgânica 03/2018[228], que transpõe o RGPD, mas antes dela, já havia regulamentação do tema no país. A Convenção Europeia n.º 108, de 1981[229], elaborada em Estrasburgo em 28 de janeiro de 1981 e ratificada pela Espanha em 27 de janeiro de 1984, estabelecia a proteção das pessoas em relação ao tratamento automatizado de dados de caráter pessoal. Este foi o primeiro tradado internacional sobre o tema e teve como objetivo proteger os direitos humanos e as liberdades fundamentais das pessoas, independentemente de sua nacionalidade.

Com efeito, a Convenção n.º 108 serviu de parâmetro para que diversos países regulassem a proteção de dados pessoais por meio de legislações internas.

Destaca-se, ainda a LOTARD posteriormente, que foi revogada pela Lei Orgânica n.º 15, de 13/12/1999 - LOPD. Esta, por sua vez, foi criada para que a Espanha pudesse cumprir as diretrizes da Diretiva 95/46/CE da União Europeia.

Na Espanha, a proteção de dados pessoais envolve tanto sanções administrativas quanto sanções penais. A Lei Orgânica de Proteção de Dados e Garantia dos Direitos Digitais (LOPDGDD) prevê um regime robusto de sanções administrativas, que podem ser aplicadas pela Agência Espanhola de Proteção de Dados (AEPD). Essas sanções variam em gravidade e podem incluir multas que vão de 60 euros até 20 milhões de euros, dependendo da infração, conforme estabelecido pelo artigo 83 do RGPD e pelos artigos correspondentes da LOPDGDD.

No que se refere a atuação administrativa, a *Agencia Española de Protecciín de Datos* - AEPD - criada em 1993, possui vasta publicação de documentos, como notas técnicas e guias informativos de caráter educativo, além de ferramentas de auxílio ao cumprimento das normas de proteção de dados.[230]

No sítio eletrônico da AEPD é possível localizar publicações de resoluções derivadas de processos sancionadores desde o ano de 2010, o que demonstra o

227 UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT. Acesso em 31 out. 2024.

228 ESPANHA. Lei Orgânica 03, de 5 de dezembro de 2018. Disponível: http://data.europa.eu/88u/dataset/https-opendata-euskadi-eus-catalogo-linguisticos-ley-organica-32018-de-5-de-diciembre-de-proteccion-de-datos -personales-y-garantia-de-los-derechos-digitales-. Acesso em 24 out. 2024.

229 UNIÃO EUROPEIA. Convenção n.º 108, de 28 de janeiro de 1981. Disponível em: https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2. Acesso em 31 out. 2024.

230 AGENCIA ESPANHOLA DE PROTECCIÓN DE DATOS (AEPD). Innovación y tecnología. Disponível em https://www.aepd.es/areas-de-actuacion/innovacion-y-tecnologia. Acesso em 24 out 2024.

avanço no que se refere à atuação do Estado na fiscalização do tratamento de dados pessoais.

Além das sanções administrativas, a legislação espanhola também contempla sanções de caráter penal no que diz respeito a violações de dados. O Código Penal sofreu uma atualização pela Lei Orgânica n.º 10, de 23 de novembro de 1995 para incluir um capítulo destinado a crimes informáticos, a exemplo da fraude informática, utilização ilícita de cartões eletromagnéticos nos crimes de roubo, violação informática, dano e sabotagem informática, violação de intimidade, dentre outros. [231]

O Código Penal espanhol, em seu artigo 197, prevê penas para ações que envolvem a violação da privacidade e a divulgação não autorizada de dados pessoais. Essas disposições são importantes para garantir que, além das penalizações administrativas, existam consequências penais para comportamentos mais graves, como acessos ilegais a sistemas de informações e a manipulação indevida de dados pessoais.

O artigo 197.2 ainda apresenta descrição típica ainda mais específica pois prevê como crime a apreensão, utilização ou modificação, em prejuízo de terceiro, dados pessoais reservados de outrem que estejam registrados em bando de dados ou meios informáticos, eletrônicos ou telemáticos, ou ainda em qualquer outro tipo de arquivo, seja público ou privado.[232]

Merece destaque, ainda, a disposição contida no artigo 197.4, que prevê a aplicação de aumento de pena no crime de descoberta e revelação de segredos em razão da captação de dados ou fatos descobertos pelos responsáveis pelos banco de dados, meios informáticos, eletrônicos ou telemáticos.[233]

Na análise da aplicação do referido dispositivo, Enrique Anarte Borrallo destaca que o Tribunal Constitucional concebe a proteção de dados como um direito

231 ESPANHA. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Disponível em https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444. Acesso em 24 out. 2024.

232 Art. 197.2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un terceiro. ESPANHA. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Disponível em https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444. Acesso em 24 out. 2024.

233 Artigo 197.º4. 4. Los hechos descritos en los apartados 1 y 2 de este artículo serán castigados con una pena de prisión de tres a cinco años cuando:a) Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros; o b) se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima.

fundamental autônomo, tendo em vista que, por meio deste, são garantidos outros direitos como a dignidade, bem como o desenvolvimento da personalidade.[234]

Outro ponto de grande relevância inserido com a reforma do Código Penal Espanhol promovida pela Lei Orgânica 05/2010 refere-se à inserção da responsabilidade criminal da pessoa jurídica.[235]

O art. 31 do Código Penal Espanhol, modificado pela Lei Orgânica 1/2015 prevê a responsabilidade pessoal do agente que atuar como administrador de fato ou de direito da pessoa jurídica. [236]

O art. 31 bis do mesmo diploma trouxe a definição da responsabilidade da pessoa física que possui o poder de decisão na instituição, ou seja, o administrador e representante da pessoa jurídica e que detém o controle de seu funcionamento. Ainda prevê a responsabilidade da pessoa jurídica em razão de atos praticados por pessoas físicas no exercício da atividade empresarial por sua conta e proveito quando houver a omissão do administrador no tocante ao seu controle e supervisão. Cabe evidenciar a segunda parte do dispositivo:

> b) De los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en beneficio directo o indirecto de las mismas, por quienes, estando sometidos a la autoridad de las personas físicas mencionadas en el párrafo anterior, han podido realizar los hechos por haberse incumplido gravemente por aquéllos los deberes de supervisión, vigilancia y control de su actividad atendidas las concretas circunstancias del caso.[237]

Ou seja, o Código Penal da Espanha fez previsão expressa da imputação penal da pessoa jurídica em razão do não cumprimento dos deveres do seu administrador quanto à fiscalização, vigilância e controle da atividade empresarial. Nesse aspecto, não se trata da responsabilidade do próprio administrador pela omissão imprópria,

---

234 BORRALLO, Enrique Anarte et al. Sobre los limites de la protección penal de datos personales. Revista Derecho y conocimiento, v. 02. 2002. Huelva, Espanha: Universidade de Huelve. Disponível em: https://rabida.uhu.es/dspace/handle/10272/2554?show=full. Acesso em 29 out. 2024. p. 235.

235 PRADO. Luiz Regis. Novo código penal espanhol (lei orgânica 5/2010) responsabilidade penal do ente coletivo - impressões iniciais. Revista de Ciência Penais. vol. 14, p. 431. Jan/2011. Espanha, 2011. Disponível em Agencia espanhola de protección de datos. Innovación y tecnología. Disponível em https://www.aepd.es/areas-de-actuacion/innovacion-y-tecnologia. Acesso em 24. out 2024.http://regisprado.com.br/resources/Artigos/Luiz_Regis_Prado/Novo%20C%C3%B3digo%20Penal%20Espanhol%20(Lei%20Org%C3%A2nica%2052010)%20Responsabilidade%20Penal%20do%20ente%20coletivo%20-%20Impress%C3%B5es%20Iniciais.pdf. Acesso em 24 out. 2024.

236 El que actúe como administrador de hecho o de derecho de una persona jurídica, o en nombre o representación legal o voluntaria de otro, responderá personalmente, aunque no concurran en él las condiciones, cualidades o relaciones que la correspondiente figura de delito requiera para poder ser sujeto activo del mismo, si tales circunstancias se dan en la entidad o persona en cuyo nombre o representación obre. ESPANHA. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Disponível em https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444. Acesso em 24 out. 2024. Art. 30.

237 Em tradução livre: Nos casos previstos neste Código, responderão criminalmente as pessoas jurídicas: b) pelos crimes cometidos, no exercício de atividades sociais e em seu nome e em seu benefício direto ou indireto, por aqueles que, estando sujeitos à autoridade das pessoas mencionadas no número anterior, tenham podido praticar o crime por não ter cumprido gravemente os seus deveres de fiscalização, vigilância e controle da sua atividade, tendo em conta as circunstâncias específicas do caso.

como estudado nas seções anteriores, mas da determinação de responsabilidade da própria pessoa jurídica.

Por outro lado, a alteração realizada em 2015 privilegiou a pessoa jurídica com a previsão de diversas causas de isenção de pena, entre elas, se antes do cometimento da infração penal, ela tiver adotado e executado de forma eficaz um modelo de organização e gestão com vistas à prevenção de crimes.[238]

Nesse aspecto verifica-se o avanço da legislação espanhola com a inserção de incentivo concreto à prática de programas de *compliance*, como forma de alcance da adequação social por uma via preventiva e não somente repressiva.

No entanto, a inovação legislativa espanhola não saiu incólume às críticas doutrinárias, pela confusão quanto às modalidades de responsabilidade direta e indireta (atribuição), bem como em relação à problemática de previsão de responsabilidade por fato de terceiro em afronta aos princípios norteadores do direito penal. Há previsão inclusive de responsabilidade da pessoa jurídica quando não for possível identificar a pessoa natural, assim como a possibilidade de responsabilidade solidária e subsidiária.[239]

Portanto, para traçar um comparativo do sistema normativo da Espanha e Brasil, bem como da atuação de seus órgãos fiscalizadores no cumprimento de suas atribuições de fiscalização e promoção de processos sancionadores, verifica-se, antes de tudo, a necessidade de realizar uma ponderação sobre as especificidades de cada País, principalmente em relação ao tempo de atuação efetiva da AEPD e ANPD.

Como visto, o órgão espanhol possui uma estrutura em funcionamento mais consolidada, que permitiu uma eficiência significativa no cumprimento de suas obrigações. De outro lado, ainda que se possa concluir que a via administrativa tem sido eficaz na busca pela repressão de violações ao tratamento de dados, a Espanha também inovou na matéria criminal no tocante à previsão de novos dispositivos incriminadores. Uma atuação administrativa não impediu a necessidade de evolução legislativa para acompanhar as mudanças na sociedade.

---

238 ESPANHA. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Art. 31 bis, 4. Disponível em https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444. Acesso em 24 out. 2024.

239 PRADO. Luiz Regis. Novo código penal espanhol (lei orgânica 5/2010) responsabilidade penal do ente coletivo - impressões iniciais. Revista de Ciência Penais. vol. 14, p. 431. Jan/2011. Espanha, 2011. Disponível em http://regisprado.com.br/resources/Artigos/Luiz_Regis_Prado/Novo%20C%C3%B3digo%20Penal%20Espanhol%20(Lei%20Org%C3%A2nica%2052010)%20Responsabilidade%20Penal%20do%20ente%20coletivo%20-%20Impress%C3%B5es%20Iniciais.pdf. Acesso em 24 out. 2024.

Essa análise corrobora para o entendimento de que se mostra cabível e necessária a interação entre o sistema de proteção de dados e o direito penal, de modo que este intervenha nas hipóteses em que se mostrarem insuficientes as atuações de outras áreas, em conformidade com o princípio da subsidiariedade.

A legislação sobre proteção de dados em combinação com o Código Penal ressalta a importância da conformidade e da responsabilidade social corporativa na administração de dados pessoais, exigindo que as empresas implementem medidas específicas para proteger essas informações e evitar possíveis danos aos titulares de dados pessoais.

5 CONSIDERAÇÕES FINAIS

A globalização e a facilitação do acesso da população às tecnologias de informação e comunicação têm revolucionado cada vez mais as relações sociais, políticas, comerciais, consumeristas, culturais, dentre outras. A revolução tecnológica modificou substancialmente a forma como as pessoas se comunicam entre si e com instituições, no modo como consomem no mercado de produtos e serviços e até mesmo na forma como se relacionam com o Estado na prestação de serviços públicos. São inúmeras as possibilidades.

O avanço contínuo das tecnologias sem dúvidas representa muitas vantagens, pois permite o desenvolvimento da sociedade em vários aspectos, com a otimização de tempo para a execução de atividades simples, além da redução de custos, a exemplo da educação à distância, das compras *on-line* e do pagamento de um boleto bancário por meio de aplicativos. As relações de trabalho também foram objeto de diversas mudanças por meio da implementação de novos recursos tecnológicos. Esses são apenas alguns exemplos de inovações que integram a nova realidade, uma mudança acelerada, principalmente, em decorrência da pandemia do Covid-19.

O ponto em comum entre todas as relações mencionadas, assim como em muitas outras, é que, para a realização dessas atividades, o indivíduo deve compartilhar seus dados pessoais, sejam eles sensíveis ou não, tanto em formato informatizado quanto em formato físico, embora este último esteja se tornando progressivamente obsoleto. Ao se cadastrar em sites ou aplicativos de diversas finalidades, o usuário frequentemente precisa fornecer informações como nome completo, CPF, endereço de e-mail e endereço residencial. Em outros casos, são solicitados dados mais específicos, destinados a traçar um perfil detalhado do indivíduo, abrangendo sua origem étnica, religião, preferências políticas, informações relacionadas à saúde, entre outros aspectos.

A princípio, o fornecimento desses dados pode parecer inofensivo, afinal, ele se mostra imprescindível para o alcance do serviço ou produto de interesse do indivíduo. Assim, ainda que aqueles dados pessoais estejam atrelados a determinada finalidade, há o risco de que eles possam ser utilizados para fins indevidos e até ilícitos. Não faltam exemplos de crimes de estelionatos ou outras infrações cometidas a partir do acesso não autorizado a informações capazes de identificar potenciais

vítimas e suas vulnerabilidades. Os danos gerados podem ser de diversas naturezas, como a patrimonial, a moral, à imagem, à honra, à dignidade sexual.

A partir da constatação desse novo cenário, o Direito precisou acompanhar essa evolução para que pudesse cumprir a sua finalidade de regulação da vida em sociedade. Diversos países iniciaram um movimento de criação de legislações específicas sobre a proteção de dados pessoais. Ressalte-se que, antes da existência de normas representativas deste sistema, como o Regulamento Geral de Proteção de Dados da União Europeia e a Lei Geral de Proteção de Dados no Brasil, ainda que não houvesse a menção expressa ao direito à proteção de dados, este já recebia certa atenção por meio da previsão de outros direitos fundamentais, como o desenvolvimento da personalidade, privacidade, dignidade humana, entre outros.

Inicialmente, a proteção dos dados pessoais não possuía uma estrutura normativa própria, sendo que era considerado apenas como uma das formas de manifestação do direito à intimidade e da personalidade. Ocorre que houve a necessidade de avançar e explicitar tal direito para torná-lo autônomo em relação aos demais direitos de nível constitucional, até que alcançasse o *status* de direito fundamental e humano. Esta elevação do direito à proteção de dados pessoais representa a magnitude da modificação sofrida pelas relações jurídicas propiciada pela revolução tecnológica. Como sabido, o direito acompanha as mudanças da sociedade e não o contrário.

Graças a esta revolução, atualmente o ordenamento jurídico brasileiro conta com um sistema próprio de proteção de dados pessoais, que estabelece princípios norteadores da prática de tratamento de dados pessoais e os mecanismos de fiscalização e responsabilização administrativa pelo tratamento indevido ou ilícito dessas informações.

Atualmente, as instituições públicas e privadas devem cumprir diversas diretrizes externas e internas com o fim de respeitar os princípios basilares estabelecidos pela LGPD, como o da segurança, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, prevenção, não discriminação, boa-fé que, reunidos, direcionam o correto tratamento de dados pelas organizações.

A LGPD, inspirada principalmente pelo RGPD, trouxe ainda em seu bojo a previsão da criação da Autoridade Nacional de Proteção de Dados, que possui funções de promover a educação da sociedade para cumprimento das normas

relativas à proteção dos dados pessoais, bem como a competência de fiscalizar e aplicar as sanções administrativas previstas na lei.

No Brasil, a Autoridade Nacional de Proteção de Dados - ANPD experimentou um retardamento no início de suas atividades e ainda enfrenta algumas limitações em sua estrutura, o que impede o cumprimento pleno de todas as suas atribuições de forma potencialmente eficaz, especialmente no que se refere aos processos sancionadores. Diversas causas foram apontadas pela própria autarquia, entre elas a insuficiência de um quadro de pessoal próprio necessário para a execução adequada de suas funções. Adicionalmente, destaca-se a necessidade de regulamentação de dispositivos da Lei Geral de Proteção de Dados (LGPD) para viabilizar sua implementação plena.

Ainda assim, mesmo diante das dificuldades enfrentadas desde a sua criação, a autarquia tem exercido um importante e imprescindível papel no tocante à educação sobre os direitos dos titulares de dados pessoais e dos deveres das organizações quanto ao tratamento de dados pessoais. No site do órgão, são encontrados diversos materiais orientativos, como guias, cartilhas e outros documentos de grande relevância, os quais contribuem para a prevenção de infrações.

Acontece que, no que tange às suas atribuições de fiscalização e instauração de procedimentos penalizadores, verificou-se um fluxo muito pequeno no volume de processos concluídos. Ressalte-se que o estudo apresentado levou em consideração os dois relatórios de Monitoramento referentes ao ano de 2022 e primeiro semestre de 2023. Até o encerramento da pesquisa não havia sido disponibilizados dados relacionados ao período de 2024. No entanto, como ressalvado, uma eventual conclusão sobre a atuação da ANPD nessas atribuições de fiscalização e responsabilização dos infratores não pode ser realizada sem analisar o contexto de seu nascimento e dos obstáculos enfrentados pelo órgão desde então.

Por outro lado, não pode ser deixada de lado a necessidade de efetivação das normas de proteção de dados, principalmente no que tange à responsabilidade pelas violações decorrentes de tratamento indevido ou ilícito, tendo em vista se tratar de uma competência do Estado, conforme determina a LGPD. Nesse sentido, o primeiro passo para o aprimoramento dos mecanismos existentes consiste em fomentar a ANPD com os recursos técnicos e humanos necessários para o seu adequado funcionamento. Afinal, o seu papel como agente orientador da sociedade contribui para a prevenção de violações ao direito de proteção de dados pessoais.

Apresentadas as ressalvas necessárias para uma compreensão sistemática e ponderada da questão e, diante da complexidade da sociedade tecnológica atual, acrescida da crescente relevância que o direito fundamental à proteção de dados tem adquirido, constatou-se a necessidade de analisar a interação desse novo sistema de proteção de dados com outros ramos do Direito.

Como visto, o sistema de proteção de dados pessoais possui uma imbricada relação com outras áreas jurídicas, a exemplo do direito do consumidor, direito civil, administrativo e até mesmo o direito penal. Sua intersecção com este último decorre da importância que o direito à proteção de dados pessoais apresenta e os riscos e danos graves decorrentes de sua violação, o que reclama uma intervenção estatal mais drástica e efetiva. Ao considerar o sistema principiológico que fundamenta o Direito Penal, principalmente a intervenção mínima e reserva legal, sua atuação somente será possível quando outros ramos do direito não se fizerem suficientes para alcançar a efetiva proteção ao bem jurídico.

Diante dos fatos recorrentes noticiados sobre violação de dados pessoais, as penalizações, que frequentemente constituem em multas milionárias, têm demonstrado serem insuficientes para promover a adequação das condutas das empresas. Um exemplo emblemático é o grupo Meta, proprietário de plataformas amplamente utilizadas, como Instagram, Facebook e WhatsApp. Essa empresa frequentemente figura nos noticiários do Brasil e do mundo devido ao tratamento inadequado de dados pessoais, que contraria as legislações vigentes, como LGPD e o RGPD.

Recentemente, a Meta foi multada em valores significativos por sua falha no tratamento de dados dos seus usuários. Essas penalizações, embora elevadas, parecem não ser um desincentivo suficiente, à medida que a empresa continua a ser alvo de investigações e processos relacionados à privacidade. As consequências desses incidentes não se limitam apenas a multas; afetam também a confiança do consumidor e geram um crescente clamor público por regulamentações mais rigorosas e um controle maior sobre o uso de dados pessoais.

Essas situações evidenciam a necessidade urgente de adoção e aprimoramento de uma cultura organizacional que priorize a proteção de dados e a transparência, em vez de uma abordagem reativa apenas em resposta a penalizações. A autonomia na gestão de dados pessoais é uma questão que demanda atenção constante, não apenas para cumprir a legislação, mas para garantir a

segurança da sociedade em relação às instituições que tratam suas informações mais sensíveis.

Diante do contexto que evidencia a vulnerabilidade deste novo direito e sua crescente relevância na sociedade contemporânea, constata-se que o direito à proteção de dados pessoais pode ser considerado um bem jurídico-penal. Como mencionado anteriormente, segundo a teoria do bem jurídico, a função do direito penal, enquanto *última ratio*, consiste em proteger os bens mais preciosos ao indivíduo, aqueles que possuem dignidade suficiente para justificar a aplicação de medidas mais rigorosas de responsabilização.

A proteção de dados pessoais, por sua vez, não se limita apenas à privacidade do indivíduo, mas abrange aspectos fundamentais como a autodeterminação informativa e o respeito à dignidade humana. A violação desse direito pode resultar em consequências significativas, incluindo danos à reputação, impactos emocionais e abusos de identidade, o que justifica a intervenção do Estado por meio de sanções penais.

Além disso, observa-se que a crescente digitalização da vida cotidiana e a interconexão entre diferentes plataformas acentuam a necessidade de uma resposta mais eficaz do sistema jurídico para lidar com esses novos desafios. A aplicação de penas e sanções para aqueles que desrespeitam as normas de proteção de dados não é apenas uma questão de justiça, mas uma exigência para garantir que os direitos fundamentais dos cidadãos sejam respeitados em um ambiente cada vez mais permeado por tecnologias que coletam e processam informações pessoais.

Portanto, a inclusão do direito à proteção de dados como um bem jurídico-penal não apenas reforça sua importância, mas também destaca a necessidade de implementação de mecanismos legais adequados que possam desencorajar práticas inadequadas e promover uma cultura de responsabilidade nas empresas e organizações que operam nesse espaço.

A partir da avaliação sistemática do tema, pode-se dividir a análise do problema sob dois aspectos: a) considerando a aplicação dos institutos penais vigentes da teoria do crime, há possibilidade de responsabilização penal pela violação a direito fundamental à proteção de dados em situações específicas; b) em segundo lugar, não se ignora a conclusão de que o direito à proteção dos dados pessoais exige atualmente uma regulamentação criminal própria, com a previsão de crimes específicos para a proteção deste bem jurídico a exemplo da Espanha.

Quanto à primeira assertiva, considerando o sistema de tipicidade adotado pelo Código Penal, há uma espécie de imputação que pode permitir a responsabilização criminal do controlador de dados em razão da prática de crimes por terceiros. Explique-se.

O referido diploma estabelece que o crime pode ser comissivo ou omissivo. Ou seja, a infração pode ser configurada em razão do cometimento de uma ação ou de uma omissão. Por sua vez, os crimes omissivos são classificados em próprios ou comissivos por omissão, também denominados de omissivos impróprios. A primeira espécie exige a existência de um tipo penal no qual faz a previsão de uma conduta negativa, como por exemplo o crime de omissão de socorro previsto no artigo 135 do Código Penal. Por outro lado, o crime omissivo impróprio não decorre de tipos penais específicos. A causalidade necessária para a configuração do crime reside na relação jurídica especial que o agente possui com o objeto juridicamente tutelado.

Nesse sentido, determinadas pessoas possuem deveres de atuação efetiva para proteção do objeto tutelado a fim de evitar a ocorrência do resultado danoso. Assim, em crimes comuns, é possível atribuir a responsabilidade daquele que deixou o bem desprotegido e vulnerável, permitindo, assim, que alguma infração penal fosse praticada em seu detrimento. Este indivíduo é denominado pela doutrina como garante, tendo em vista que possui a obrigação de garantir a proteção do bem jurídico. Com efeito, a posição de garante pode decorrer da constatação de três hipóteses, conforme previsão do art. 13, §2º do Código Penal: a) quando há uma obrigação legal de cuidado, proteção ou vigilância; b) quando o agente assume a responsabilidade de impedir o resultado em situações não abarcadas na hipótese anterior ou c) nos casos de ingerência, ou seja, quando o agente criou o risco da ocorrência do dano em razão de um comportamento seu anterior.

A problemática que reside na busca pelo fundamento ideal de equiparação entre ação e omissão ainda não encontrou um entendimento pacificado na dogmática jurídico-penal. As teorias mais relevantes apontadas pela doutrina podem ser divididas em duas grandes vertentes: as decorrentes de um fundamento formal e as que defendem a necessidade de existência de um substrato material que ensejará a exigência de ação do garante em direção à proteção do bem jurídico.

A teoria material mais defendida pela doutrina consiste na formulada por Shünemann, segundo a qual a responsabilidade criminal do garante dependerá de um requisito material: o domínio sobre o fundamento do resultado. Nesse sentido, não

somente o dever formal, por exemplo, a lei, ensejará na imputação do crime ao garante, mas em razão também da comprovação de que ele possuía plena capacidade de agir para evitar o resultado danoso. Em outras palavras, o garante poderá responder pelo crime quando, consciente do seu dever de proteção e vigilância sobre o bem, deixar de cumprir seus deveres mesmo tendo a plena capacidade e domínio sobre a situação fática que ensejou o resultado. Trata-se, portanto, de um nexo de causalidade normativo, diferente da causalidade necessária como requisito para a tipicidade em crimes comissivos.

Considerando que o controlador de dados pessoais possui deveres legais de proteção e vigilância sobre o tratamento de dados, chegou-se à constatação de que ele poderá se encaixar na posição de garantidor, nos termos previstos no Código Penal em seu artigo 13, § 2º. Assim, a eventual omissão dolosa (presentes todos os demais requisitos para a tipicidade da conduta omissiva) por parte dessa figura será relevante para o Direito Penal e, por consequência, possibilitará a responsabilização pelo resultado criminoso decorrente do tratamento irregular de dados. Ressalta-se que ao operador poderá ser aplicado o mesmo raciocínio nas hipóteses destacadas no artigo 42, § 1º, inciso I da LGPD.

Em retomada ao exame da relação existente entre a proteção de dados pessoais e o Direito Penal, denota-se que a LGPD atribuiu aos agentes de tratamento, em especial o controlador, o dever de adoção dos mecanismos de segurança técnicos e administrativos aptos a garantir a proteção dos dados pessoais em face de acessos não autorizados e de situações acidentais ou ilícitas que possam gerar danos aos titulares. Ressalte-se que tais medidas devem ser cumpridas desde a concepção do produto ou serviço, durante a sua execução e após finalizado o tratamento.

Por meio da imposição de deveres de proteção e vigilância, foi possível concluir que o controlador e, eventualmente o operador, podem figurar como garante para fins de responsabilização criminal por omissão imprópria. Contudo, tal imputação não deve ser realizada com base estritamente em razão dos deveres formais previstos na legislação, mas a partir da comprovação, no caso concreto de que o controlador detinha o domínio real sobre a causa do resultado.

Ainda, somente estará configurado o crime omissivo impróprio se restarem presentes os demais elementos necessários à configuração da tipicidade exigido para essa espécie de crime, quais sejam: 1) situação típica e a ausência da ação devida;

2) a capacidade de ação do garantidor; 3) o nexo de causalidade normativo ou de evitabilidade; 4) a produção de um resultado e 5) a análise do elemento subjetivo.

Com efeito, considerando a hipótese de enquadramento em todos esses requisitos, o controlador poderá ser responsabilizado pela prática de crime contra os dados pessoais em razão de conduta praticada por terceiro. Como dito, o raciocínio encontra-se respaldado a partir da adoção da teoria material defendida por Shünemann.

Convém destacar que a afirmação direcionada à responsabilidade criminal do controlador de dados pessoais na hipótese acima mencionada não viola os princípios gerais do Direito Penal, ao passo que constitui produto da interpretação de critérios legais e doutrinários adotados pela dogmática jurídico-penal.

Como ressalta Figueiredo Dias, atualmente no Direito Penal há uma quantidade maior de crimes por ações do que por omissões. Contudo, este cenário tende a ser alterar com o aumento da previsão de delitos omissivos em razão das novas características da Sociedade do Risco. No entanto, o autor ressalta a importância de evitar punições generalizadas ou alargadas.

Ao lado da conclusão mencionada, a pesquisa também se deparou com o questionamento sobre a necessidade de criação de uma política criminal voltada à proteção dos dados pessoais. É importante destacar que diante do avanço do uso de diversas tecnologias no cotidiano dos indivíduos, a proteção de dados pessoais deve estar abarcada em duas áreas distintas: a) no âmbito processual e segurança pública, para dispor sobre o tratamento de dados nas investigações e compartilhamento de informações pelas instituições e b) no âmbito penal com a disposição de infrações penais em razão da violação do direito fundamental à proteção de dados pessoais.

Em relação à primeira área, tramita na Câmara dos Deputados o Projeto de Lei 1.515/2022, chamada Lei de Proteção de Dados Penal, que tem como reger o tratamento de dados pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais.

Por outro lado, não há no atual sistema jurídico penal brasileiro um conjunto de disposições legais incriminadoras voltado à proteção de dados pessoais e autodeterminação informativa, como é possível encontrar na Espanha e em outros países integrantes da União Europeia. O saneamento desta situação deve ser realizado por meio de atuação do Congresso Nacional, com a criação de tipos penais específicos.

A exemplo da Espanha, há previsão de responsabilidade criminal das pessoas encarregadas ou responsáveis pelos ficheiros e suportes informáticos utilizados no tratamento dos dados. Tais reflexões não constituíram objetivo específico do trabalho, mas demonstrou a necessidade de evolução do ordenamento jurídico brasileiro na mesma direção.

Com efeito, a necessidade de intervenção do direito penal na seara da proteção de dados se justifica pela relevância deste direito fundamental para o indivíduo e pela análise do sistema de responsabilização administrativa atual, que ainda se mostra insuficiente para alcançar a tutela necessária deste bem jurídico.

Da análise dos Relatórios emitidos pela Autoridade Nacional de Proteção de Dados de 2022 e primeiro semestre de 2023 (os únicos publicados até a finalização deste trabalho), foi possível constatar que ainda há um longo caminho pela frente para que seja alcançada uma efetividade no processamento dos requerimentos e denúncias de irregularidades e incidentes de segurança, bem como na aplicação das penalidades administrativas. A falta de recursos humanos, sistemas informatizados próprios e regulamentações especiais têm sido causa de obstáculos e até mesmo da impossibilidade de efetividade dos direitos previstos na LGPD.

Para além dessas questões, a partir da inserção do direto à proteção de dados como um direito fundamental na Constituição Federal (apesar de antes da publicação da Emenda Constitucional 115 de 2022 ser possível encontrar diversos autores que já defendiam essa natureza) e, por meio das inovações tecnológicas que invadiram as economias, relações sociais, políticas e culturais de quase todas as comunidades, abre-se um espaço cada vez maior de discussão sobre o aperfeiçoamento e implementação de novos mecanismos de defesa dos direitos.

Por outro lado, não se ignora a existência de independência dos ramos de direito, de forma que a previsão de sanções administrativas não impede a aplicação de outros tipos de responsabilização. De igual modo, não se pretende com esse trabalho defender um posicionamento que possa eventualmente contrariar os princípios penais basilares da reserva legal, fragmentariedade e subsidiariedade do Direito Penal.

Ao contrário, o Direito deve evoluir conforme as mudanças da sociedade. Esta tem sido modificada contínua e substancialmente desde o último quartel do século XX com a inserção de tecnologias da informação, que alteraram as mais diversas atividades dos indivíduos, como aquisição de bens, acesso a serviços governamentais

e de natureza privada e sem dúvida nas relações sociais. Diante desse cenário, como consequência, a quantidade de dados pessoais que alimenta a internet se tornou praticamente incalculável.

O vazamento de dados pessoais, principalmente os de natureza sensível, o tratamento irregular dessas informações e outros incidentes de segurança possuem o potencial de causar diversos prejuízos materiais e morais aos seus titulares, além da ofensa a outros direitos como a privacidade, personalidade, honra, imagem e outros. Tais danos são difíceis ou até mesmo impossíveis de serem reparados.

O avanço nos estudos do tema demonstra, antes de tudo, a necessidade de um aprimoramento no processo de conscientização e adoção de boas práticas e governança por parte das instituições. O objetivo principal do cumprimento das normas de proteção de dados não pode ser o de apenas evitar as sanções previstas na legislação, mas de nortear as atividades atendendo ao princípio da boa-fé, tendo sempre como bússola orientadora a preocupação que o impacto que o tratamento indevido de dados pode acarretar aos seus usuários.

Por derradeiro, pelas análises alcançadas por este trabalho, foi possível concluir afirmativamente sobre a possibilidade de considerar a aplicação do Direito Penal em razão da violação do direito à proteção dos dados sem desrespeito às regras e princípios sedimentados no ordenamento jurídico atual.

Após a exposição das principais reflexões dogmáticas necessárias para a compreensão da proteção de dados pessoais e a responsabilidade pelo tratamento indevido (sem, contudo, ousar atingir o esgotamento de todos os fundamentos existentes), chegou-se à conclusão de que o Brasil ainda necessita evoluir significativamente no tocante ao conteúdo normativo que envolve os crimes que podem ser praticados por meio de Tecnologias da Informação e Comunicação.

Tal dedução pode ser explicada por meio diversos fatores, a começar pelo tempo excessivo gasto para a aprovação do PL 4060/12, o qual deu origem à LGPD, que entrou em vigor parcialmente somente em 2018. Além disso, pode ser adicionada ainda toda a celeuma enfrentada para a criação da ANDP, alteração de sua natureza jurídica, bem como o início das suas atividades. As dificuldades ainda permaneceram em razão da insuficiência de recursos humanos e de sistemas para uma adequada execução de suas atribuições.

O presente estudo não pretende discordar ou eliminar a necessidade de construção de um corpo normativo próprio para prever condutas típicas com o objetivo

de proteger os dados pessoais de forma mais efetiva. Contudo, o recorte do trabalho consistiu na análise da responsabilização no contexto atual a partir da omissão penalmente relevante dos agentes de tratamento de dados pessoais.

Dessa forma, após o estudodoutrinário e jurisprudencial sobre o tema proposto, constatou-se que as indagações inicialmente levantas podem ser respondidas afirmativamente por meio de uma intermediação entre os sistemas jurídicos de proteção de dados e de Direito Penal.

REFERÊNCIAS

AGENCIA ESPANHOLA DE PROTECCIÓN DE DATOS (AEPD). **Innovación y tecnología**. Disponível em https://www.aepd.es/areas-de-actuacion/innovacion-y-tecnologia. Acesso em 24. out 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Balanço 3 anos**. Brasília, DF, 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/anpd_balanco_tres_anos.pdf. Acesso em 23 de jul 2024. p 11.

____.**Comunicação de incidente de segurança**. Brasília, DF, 2022.Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acesso em 23 de jul 2024.

____. **Processo administrativo 00261.001888/2023-21**. Brasília, DF, 2023. Disponível em https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao/PAS_INSS_principal_publica.pdf. Acesso em 24 set 2024.

____. **Relatório de instrução n.º 01/2024/CGF/ANDP**. Brasília, DF, 2024. Disponível em: https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao/PAS_INSS_principal_publica.pdf. Acesso em 24 set 2024

____. **Resolução CD/ANDP n.º 4, de 24 de fevereiro de 2023.** Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077. Acesso em 23 de jul 2024.

____. **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado.** Brasília, DF, 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf. Acesso em 20/07/2023.

____. **Relatório de ciclo de monitoramento de 2022**. Brasília, DF, 2022. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.gov.br/anpd/pt-br/assuntos/noticias/2023-08-17-relatorio-do-ciclo-de-monitoramento-2022.pdf . Acesso em 14.05.2023.

____. **Relatório de ciclo de monitoramento. 1º semestre de 2023**. Brasília, DF, 2023. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/2023-11-07-relatorio-do-ciclo-de-monitoramento-2023-versao-final.pdf. Acesso em 14.05.2023.

____ **Voto Nº 23/2024/DIR-JR/CD.** Processo nº 00216.004529/2024-36. Brasília, DF, 2024. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/deliberacoes-do-conselho-diretor-1/circuitos-deliberativos-2024/cd-18-2024-votos.pdf. Acesso em 31 out. 2024.

ASSOCIAÇÃO BRASILEIRA DE INTERNET. (ABRANET) . **Banco Central**: vazaram dados de 39 mil chaves Pix do 99Pay. São Paulo, SP, 2024. Disponível em: https://www.abranet.org.br/Noticias/Banco-Central%3A-vazaram-dados-de-39-mil-chaves-Pix-do-99Pay-5022.html. Acesso de 29 de jul. 2024.

____. **Vinte e cinco contas sofrem violação de dados por minuto no Brasil**. São Paulo, 2022. Disponível em: https://www.abranet.org.br/Noticias/Vinte-e-cinco-contas-sofrem-violacao-de-dados-por-minuto-no-Brasil-3966.html?UserActiveTemplate=mobile%2Csite. Acesso em 03 mai.2024.

BAUMAN, Zygmunt. **Modernidade líquida**. Tradução de Plinio Dentzien. Rio de Janeiro: Zahar, 2021.

BBC News Brasil. **Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira das autoridades.** São Paulo, SP, 2018. Disponível em: < https://www.bbc.com/portuguese/internacional-43461751>. Acesso em 23 set de 2024.

BECK, Ulrich. **Sociedade de risco.** Rumo a uma outra modernidade. São Paulo: 34, 2010.

BIONI, Bruno R. **Proteção de dados pessoais -** A Função e os Limites do Consentimento. Rio de Janeiro: Grupo GEN, 2021. E-book. ISBN 9788530994105. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994105/. Acesso em: 21 mai. 2024.

BITENCOURT, Cezar Roberto. **Tratado de direito penal**. Parte Geral. Vol. 1. 22.ed. rev. e atual. São Paulo: Saraiva, 2016.

BORRALLO, Enrique Anarte *et al*. **Sobre los limites de la protección penal de datos personales**. Revista Derecho y conocimiento, v. 02. 2002. Huelva, Espanha: Universidade de Huelve, 2002. Disponível em https://rabida.uhu.es/dspace/handle/10272/2554?show=full. Acesso em 29 out. 2024.

BOTELHO. Marcos César. **A LGPD e a proteção ao tratamento de dados pessoais de crianças e adolescentes.** Revista de Direitos Sociais e Políticas Públicas (UNIFAFIBE). v. 8, n. 2. São Paulo, 2020. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_informativo/bibli_inf_2006/Rev-Dir-Soc-Pol-Publicas_v.8_n.2.08.pdf. Acesso em 01 fev. 2021.

BRASIL. [Constituição (1988)] **Constituição Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/ constituicao.htm. Acesso em: 21/01/2021.

_____ [Constituição (1988)]. **Emenda constitucional n° 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Presidência da República, 2022. Disponível em:

https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#art1. Acesso em: 21 jul. 2023.

____. **Decreto n.º 592, de 06 de julho de 1992**. Disponível em: https://legislacao.presidencia.gov.br/atos/?tipo=DEC&numero=592&ano=1992&ato=2dco3YE10MFpWTf3e. Acesso em 11 jun. 2024

____. **Decreto 2.848, de 07 de dezembro de 1940**. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 25 de jul. 2024.

____. **Decreto 9.936 de 24 de abril de 2019**. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d9936.htm#:~:text=DECRETO%20N%C2%BA%209.936%2C%20DE%2024,forma%C3%A7%C3%A3o%20de%20hist%C3%B3rico%20de%20cr%C3%A9dito. Acesso em 21. mai 2024.

____. **Decreto nº 8.771, de 11 de maio de 2016.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm. Acesso em 24 mai 2024.

____. **Lei complementar 166 de 08 de abril de 2019**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp166.htm. Acesso em 21. maio 2024.

____. **Lei federal 10.406, de 10 de janeiro de 2002**. Disponível em https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em 22.05.2024

____. **Lei federal 12.737 de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Acesso em 31 mai. 2024.

____. **Lei federal 12.414, de 09 de junho de 2011**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm#:~:text=LEI%20N%C2%BA%2012.414%2C%20DE%209%20DE%20JUNHO%20DE%202011.&text=Convers%C3%A3o%20da%20Medida%20Provis%C3%B3ria%20n%C2%BA%20518%2C%20de%202010.&text=Disciplina%20a%20forma%C3%A7%C3%A3o%20e%20consulta,forma%C3%A7%C3%A3o%20de%20hist%C3%B3rico%20de%20cr%C3%A9dito.Acesso em 21.05.2024.

____. **Lei federal 12.737 de 30 de novembro de 2012**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 31 mai. 2024.

____. **Lei federal 12.965, de 23 de abril de 2014**. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 21 jul. 2023.

____. **Lei federal n. 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados. Disponível em http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 21 de jul. 2023.

____. **Lei federal n. 13.853, de 08 de julho de 2019**. Disponível em: 1 BRASIL.Decreto n.º 10.474, de 26 de agosto de 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10474.htm. Acesso em: 23 de jul 2024.

____. **Lei federal n. 8.078**, de 11 de setembro de 1990. Disponível em https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 21 de maio. 2024

____. **Lei federal n.º 11.343 de 23 de agosto de 2006**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11343.htm. Acesso em 26 de jul. 2024.

____. **Lei Federal n.º 12.850, de 02 de agosto de 2013**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em 26 de jul. 2024.

____. **Lei federal n.º 9.296 de 24 de julho de 1996**. Disponível em https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em 26 de jul. 2024.

____. **Lei federal nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Disponível em: www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 15 de out 2024.

____. **Decreto n.º 11.348 de 01º de janeiro de 2023**. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11348.htm. Acesso em 23 de jul 2024.

____. **Lei federal n.º 14.460, de 25 de outubro de 2022**. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Lei/L14460.htm. Acesso em 23 de jul. 2024.

____. **Lei federal n.º 14.600, de 19 de junho de 2023**. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Lei/L14460.htm. Acesso em 23 de jul 2024.

____. **Medida provisória n.º 869, de 27 de dezembro de 2018**. Disponível em: https://www12.senado.leg.br/publicacoes/estudos-legislativos/tipos-de-estudos/sumarios-de-proposicoes/mpv869. Acesso em 25 de out. 2024.

____. **Medida provisória nº 954, de 17 de abril de 2020**. Dispõe sobre compartilhamento de dados por empresas de telecomunicações durante a emergência de saúde pública. Brasília, DF: Presidência da República, 2020. Disponível em: https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/141619. Acesso em 27 out. 2024.

____. **Projeto de lei 1515/2022.** Câmara dos Deputados. Brasília, DF, 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2326300#tramitacoes. Acesso em 02/08/2023.

____. Superior Tribunal de Justiça (3. Turma). **Recurso especial 1.794.971/SP**. Recorrente: TIM Celular AS. Recorrido: Ministério Público do Distrito Federal e Territórios. Relator: Ministro Herman Benjamin, 20 de maio de 2021. Disponível em: https://processo.stj.jus.br/processo/pesquisa/?num_registro=201902426992. Acesso em 29 jul. 2024.

____. Superior Tribunal de Justiça. (2. Seção). **Súmula 479.** 01 de agosto de 2012. Disponível em: https://processo.stj.jus.br/SCON/sumstj/toc.jsp?sumula=479.num. Acesso em 27 out 2024.

____. Superior Tribunal de Justiça. (2. Seção). **Tema repetitivo 466.** 12 de setembro de 2011. Disponível em: https://processo.stj.jus.br/repetitivos/temas_repetitivos/pesquisa.jsp?novaConsulta=true&tipo_pesquisa=T&sg_classe=REsp&num_processo_classe=1197929. Acesso em 27 out 2024.

____. Superior Tribunal de Justiça. (2. Turma). **Agravo em recurso especial n.º 2130619**. Processual civil e administrativo. Indenização por dano moral. Vazamento de dados pessoais. Dados comuns e sensíveis. Dano moral presumido. Impossibilidade. Necessidade de comprovação do dano. I - Trata-se, na origem, de ação de indenização ajuizada por particular contra concessionária de energia elétrica pleiteando indenização por danos morais decorrentes do vazamento e acesso, por terceiros, de dados pessoais.[...]. Agravante: Eletropaulo Metropolitana Eletricidade de São Paulo S.A. Agravado: Maria Edite de Souza. Relator: Ministro Francisco Falcão, 10 de mar de 2023. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202201522622&dt_publicacao=10/03/2023. Acesso em 27 out 2024.

____. Superior Tribunal de Justiça. (3. Turma). **Recurso especial n.º 2077278.** Consumidor. Recurso especial. Ação declaratória de inexigibilidade de débito por vazamento de dados bancários cumulada com indenização por danos morais e repetição de indébito. Golpe do boleto. Tratamento de dados pessoais sigilosos de maneira inadequada. Facilitação da atividade criminosa. Fato do serviço. Dever de indenizar pelos prejuízos. Súmula 479/stj. Recurso especial provido. 1. Ação declaratória de inexigibilidade de débito por vazamento de dados bancários cumulada com indenização por danos morais e repetição de indébito, ajuizada em 13/2/2020, da qual foi extraído o presente recurso especial, interposto em 15/2/2022 e concluso ao gabinete em 19/6/2023. [...] Recorrente: Daniela Ferreira Ramos. Recorrido: BV Financeira SA. Relatora: Ministra Nancy Andrigui, 09 de outubro de 2023. Disponível em: https://scon.stj.jus.br/SCON/pesquisar.jsp?preConsultaPP=&pesquisaAmigavel=+%3Cb%3E2.077.278%3C%2Fb%3E&acao=pesquisar&novaConsulta=true&i=1&b=ACOR&livre=2.077.278&filtroPorOrgao=&filtroPorMinistro=&filtroPorNota=&data=&operador=e&thesaurus=JURIDICO&p=true&tp=P&processo=&classe=&uf=&relator=&dtpb=

&dtpb1=&dtpb2=&dtde=&dtde1=&dtde2=&orgao=&ementa=&nota=&ref=.. Acesso em 27 out 2024.

____. Supremo Tribunal Federal. (Plenário). **Ação direta de inconstitucionalidade n.º 6387**. Relatora: Ministra Rosa Weber, 07 de maio de 2020. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur436273/false. Acesso em: 27 out 2024.

____. Supremo Tribunal Federal. (Plenário). **Recurso extraordinário n.º 673707/MG.** Relator: Ministro Luiz Fux, 17 de junho de 2015. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=9487405. Acesso em 27 out. 2024.

____.CÂMARA DOS DEPUTADOS. **Projeto de lei n.º 4060 de 13 de junho de 2012**. Disponível em https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1001750&filename=Tramitacao-PL%204060/2012. Acesso em 25 de out. 2024.

CASTELLS, Manuel. **A sociedade em rede**. v. 1. 8.ed. São Paulo: Paz e Terra, 2005.

CNN BRASIL. **PF prende hacker que vazou dados de 223 milhões de brasileiros**. São Paulo, SP, 2024. Disponível em: https://www.cnnbrasil.com.br/nacional/pf-prende-hacker-que-vazou-dados-de-223-milhoes-de-brasileiros/#:~:text=PF%20prende%20hacker%20que%20vazou%20dados%20de%20223%20milh%C3%B5es%20de%20brasileiros,-Investiga%C3%A7%C3%A3o%20aponta%20que&text=A%20Pol%C3%ADcia%20Federal%20prendeu%2C%20nesta,entre%20vivos%20e%20j%C3%A1%20falecidos. Acesso em 29 de jul. 2024.

COSTA JÚNIOR, Paulo José. **O direito de estar só.** Tutela penal da intimidade. 2.ed. rev. e atual.. São Paulo: Revista dos Tribunais, 1995.

DIAS, Jorge de Figueiredo. **Direito penal: p**arte geral. Tomo I, 1.ed. São Paulo: Revista dos Tribunais, 2007.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental.** Espaço Jurídico Journal of Law [EJJL], v. 12, n. 2, p. 91-108, 2011. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315/658. Acesso em 18 jul. 2022.

____. **Panorama histórico da proteção de dados pessoais.** In: DONEDA. Danilo et al (coord). Tratado de Proteção de dados Pessoais. Rio de Janeiro: Forense, 2021.

EDPB. **1.2 billion euro fine for facebook as a result of EDPB binding decision. Bruchelas, Belgica, 2023.** Disponível em https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_pt. Acesso em 29 de jul. 2024.

EL PAÍS· **¿Puede facebook poner precio a mi privacidad?** Espanha**,** 2024. Disponível em: https://elpais.com/economia/negocios/2024-04-28/puede-facebook-poner-precio-a-mi-privacidad.html. Acesso em 31 out. 2024.

ESPANHA. **Lei orgânica 03, de 5 de dezembro de 2018**. Disponível: http://data.europa.eu/88u/dataset/https-opendata-euskadi-eus-catalogo-linguisticos-ley-organica-32018-de-5-de-diciembre-de-proteccion-de-datos -personales-y-garantia-de-los-derechos-digitales-. Acesso em 24 out. 2024.

ESPANHA**. Ley orgánica 10/1995, de 23 de noviembre**, del Código Penal. Disponível em https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444. Acesso em 24 out. 2024.

ESTELLITA, Heloisa. **Responsabilidade penal dos dirigentes de empresas por omissão:** estudo sobre a responsabilidade omissiva imprópria de dirigentes de sociedades anônimas, limitadas e encarregados de cumprimento por crimes praticados por membros de empresa. São Paulo: Marcial Pons, 2017.

EUA. **Digital 2024: 5 bilhões de usuários de mídia social**. Análise do relatório global de visão geral digital 2024. Londres, 2024. Disponível em: https://wearesocial-com.translate.goog/uk/blog/2024/01/digital-2024-5-billion-social-media-users/?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-br&_x_tr_pto=sc. Acesso em 18.jul.2024.

FERRAJOLI, Luigi. **Direito e razão**: teoria do garantismo penal. 3.ed. ver. São Paulo: Revista dos Tribunais, 2022.

GLOBO. **Documentos da NSA apontam Dilma Rousseff como alvo de espionagem**. São Paulo, 2024.. Disponível em: https://g1.globo.com/politica/noticia/2013/09/documentos-da-nsa-apontam-dilma-rousseff-como-alvo-de-espionagem.html. Acesso em 22.05.2024.

GLOBO. **Megavazamento de dados expõem informações de 223 milhões de números de CPF.** São Paulo, 2021. Disponível em: https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2021/01/25/vazamentos-de-dados-expoem-informacoes-de-223-milhoes-de-numeros-de-cpf.ghtml. Acesso em 23 set. 2024.

HABERMAS, Jürgen. **El concepto de dignidad humana y la utopia realista de los derechos humanos**. Diánoia, v. LV, n. 64, p. 3–25, maio 2010.

LIMBERGER, Têmis. Informação e Internet: **Apontamentos para um estudo comparado entre o regulamento geral de proteção de dados europeu e lei de proteção de dados brasileira**. Novos Estudos Jurídicos, v. 25, n. 2, p. 478-500, 2020. Santa Catarina, Brasil. Disponível em https://periodicos.univali.br/index.php/nej/article/view/16916. Acesso em 26.08.2023.

____ **O direito à Intimidade na era da informática**: A necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.

____. **Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso a Informação Pública (LAI):** um diálogo (im)possível? As influências do direito europeu. Revista de Direito Administrativo. Rio de Janeiro: FGV. Vol. 281, n. 1, p. 113-144, jan/abr. 2022. Disponível em: https://periodicos.fgv.br/rda/issue/view/4786. Acesso em 25 de out. 2024.

LODDER, George Neves. **Proteção de dados pessoais e investigação criminal**. Autoridade Nacional de Proteção de Dados: questões penais. Brasília: 2020.

LUZ, Ilana Martins. **A responsabilidade penal por omissão e os programas de compliance. 2017**. Tese (Doutorado) – Universidade de São Paulo, São Paulo, 2017. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2136/tde-15032021-232238/. Acesso em: 31 maio 2024.p. 202.

MAÑAS, José Luis Piñar. **El derecho fundamental a la protección de datos personales**. Algunos retos de presente y futuro. Asamblea. Revista parlamentaria de la Asamblea de Madrid, n. 13, p. 21-46, 2005.

____. **Seguridad, transparencia y protección de datos**: el futuro de um necessário e incierto equilíbrio. V. 147. Madrid: Documentos de trabaljo (Laboratorio de alternativas). Fundación Alternativas. 2009. Disponível em: https://fundacionalternativas.org/publicaciones/seguridad-transparencia-y-proteccion-de-datos-el-futuro-de-un-necesario-e-incierto-equilibrio/. Acesso em 11 jun. 2024. p. 12

MARQUES, Claudia Lima. **O "diálogo das fontes" como método da nova teoria do direito:** um tributo a Erik Jayme. In: Diálogo das fontes. Do conflito à coordenação de normas do direito brasileiro. MARQUES, Claudia Lima (coord). São Paulo: Revista dos Tribunais.

MARTINS-COSTA, Antônio Goya de Almeida. **Posição de garantia em direito penal**: a problemática da equiparação na omissão imprópria. Rio de Janeiro: Marcial Pons, 2023.

MAYRINK, Renata Pereira. **Responsabilidade penal do compliance officer**: a omissão imprópria e os pressupostos para a tipicidade. São Paulo: D´Plácido, 2022.

MENKE, Fabiano; GOULART, Guilherne Damasio. **Segurança da informação e vazamento de dados**. In: DONEDA, Danilo et al (coord). Tratado de Proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p. 329 - 360.

PRADO, Luiz Regis. **Bem jurídico-penal e Constituição**. 8.ed. rev. atual. amp. Rio de Janeiro: Forense, 2019.

____. **Novo código penal espanhol (lei orgânica 5/2010) responsabilidade penal do ente coletivo** - impressões iniciais. Revista de Ciência Penais. Vol. 14, p. 431. Jan/2011. Espanha, 2011. Disponível em Agencia espanhola de protección de datos. Innovación y tecnología. Disponível em https://www.aepd.es/areas-de-actuacion/innovacion-y-tecnologia. Acesso em 24. out 2024.http://regisprado.com.br/resources/Artigos/Luiz_Regis_Prado/Novo%20C%C3

%B3digo%20Penal%20Espanhol%20(Lei%20Org%C3%A2nica%2052010)%20Responsabilidade%20Penal%20do%20ente%20coletivo%20-%20Impress%C3%B5es%20Iniciais.pdf. Acesso em 24 out. 2024.

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

ROXIN, Claus. **A proteção de bens jurídicos como função do Direito Penal**. Rio Grande do Sul: Livraria do Advogado, 2009.

SAMUEL D. Warren; LOUIS D. Brandeis. ***The right to privacy***. Harvard Law Review, v. 4, No. 5. (Dec. 15, 1890), p. 193-220. Havard, EUA, 2020. Disponível em: https://www.jstor.org/stable/i256795. Acesso em 23 de jul. 2024.

SARLET, Ingo Wolfgang. **Fundamentos constitucionais: o direito fundamental à proteção de dados.** In: DONEDA, Danilo et al (coord). Tratado de Proteção de dados pessoais. Rio de Janeiro: Forense, 2021.

____ *et all*. **Fundamentos jusfilosóficos e âmbito de proteção do direito fundamental à proteção de dados pessoais**. Revista Direito Público, 2020 .Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://meriva.pucrs.br/dspace/bitstream/10923/18861/2/Fundamentos_Jusfilosficos_e_mbito_de_Proteo_do_Direito_Fundamental_Proteo_de_Dados_Pessoais.pdf

____. **Proteção de dados como direito fundamental na Constituição Federal Brasileira de 1988**: contributo para a construção de uma dogmática constitucional adequada. Direitos Fundamentais & Justiça. ano 14, n. 42, p. 179-218, jan./jun. 2020. Belo Horizonte, MG, 2020. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/875. Acesso em 30.08.2023.

SCHÜNEMANN, Bernd. **Cuestiones básicas de dogmática jurídico-penal y de política criminal acerca de la criminalidad de empresa**. Anuario de derecho penal y ciencias penales. Madrid, v. 41, n. 2, p. 529-558, mai./ago.1988. Disponível em: https://scholar.google.com.br/scholar?hl=pt-BR&as_sdt=0%2C5&q=sch%C3%BCnemann+bernd+Cuestiones+basicas+de+dogmatica+juridico+penal+y+de+politica+criminal+acerca+de+la+criminalidad+de+empresa&btnG=. Acesso em 31 mai. 2024.

SENADO FEDERAL**. Dez anos de vigência da lei Carolina Dieckmann**: a primeira a punir crimes cibernéticos. Brasília, DF, 2023. Disponível em https://www12.senado.leg.br/radio/1/noticia/2023/03/29/dez-anos-de-vigencia-da-lei-carolina-dieckmann-a-primeira-a-punir-crimes-ciberneticos. Acesso em 31 mai. 2024.

SOUZA, Arthur de Brito Gueiros. **Programas de *compliance* e a atribuição de responsabilidade individual nos crimes empresariais**. In: VITORELLI, Edilson (coord.). Temas atuais do Ministério Público Federal**.** 4. ed. Salvador: JusPodivm, 2016.

STF. **Acórdão HC 107638/PE**. Relator(a): Min. CÁRMEN LÚCIA. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur199231/false. Acesso em 29 de jul. 2024.

TAVARES. Juarez Estevam Xavier. **Teoria dos crimes omissivos**. Tese (doutorado). Rio de Janeiro: Universidade do Estado do Rio de Janeiro, 2012.

TOLEDO. Francisco de Assis. **Princípios básicos do direito penal**. São Paulo: Saraiva, 1994. p. 82.

UNIÃO EUROPEIA. **Carta dos direitos fundamentais da União Europeia**. 2000/C 364/01. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em 24 de jul. 2024.

UNIÃO EUROPEIA. **Convenção n.º 108, de 28 de janeiro de 1981.** Disponível em: https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2. Acesso em 31 out. 2024.

UNIÃO EUROPEIA. **Convenção n.º 108+, de 18 de maio de 2018.** Disponível em: https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2. Acesso em 16 nov. 2024.

UNIÃO EUROPEIA. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:31995L0046. Acesso em 31 out. 2024.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT. Acesso em 21 jul. 2023.

VALENTE, Victor Augusto Estevam. **A proteção de dados pessoais no direito penal: uma análise crítica da criminalização nas perspectivas constitucional e de política criminal**. São Paulo: D'Plácido, 2022.

VIOLA, Mario; TEFFÉ, Chiara Spadaccini. **Tratamento de dados pessoais na LGPD**: estudo sobre as bases legais dos artigos 7º e 11. In: DONEDA, Danilo et al (Coord). Tratado de Proteção de dados pessoais: Rio de Janeiro: Forense, 2021.

WALDRON, Jeremy. **Es la dignidade el fundamento de los derechos humanos?** In_ Democratizar la dignidade: estudios sobre dignidad humana y derechos. Bogotá: Universidad Externado de Colômbia, 2019. p. 189-227.

WOLTER, Jürgen. **O inviolável e o intocável no direito processual penal**: reflexões sobre dignidade humana. São Paulo. Marcial Pons, 2018.