UNIVERSIDADE DE SANTA CRUZ DO SUL
CURSO DE DIREITO

Gabriel Iaromicz Dummer

INTEROPERABILIDADE E COMPARTILHAMENTO DE DADOS A PARTIR DA LEI DE PROTEÇÃO DE DADOS

Santa Cruz do Sul
2024

Gabriel Iaromicz Dummer

INTEROPERABILIDADE E COMPARTILHAMENTO DE DADOS A PARTIR DA LEI DE PROTEÇÃO DE DADOS

Trabalho de Conclusão apresentado ao Curso de Direito da Universidade de Santa Cruz do Sul para obtenção do título de Bacharel em Direito.

Orientadora: Profa. Dra. Caroline Müller Bitencourt

Santa Cruz do Sul
2024

RESUMO

O presente trabalho monográfico possui como tema a interoperabilidade e compartilhamento de dados a partir da Lei de proteção de dados e tem como objetivo investigar e apontar os limites e as possibilidades de compartilhamento e interoperabilidade de dados pelos sujeitos públicos e privados, a partir da Lei de Proteção Geral de Dados no Brasil. Nesse contexto, a problemática a ser enfrentada consiste em quais os limites e as possibilidades da interoperabilidade e compartilhamento de dados pela administração pública e por sujeitos privados, em consonância com a Lei Geral de Proteção de Dados no Brasil. Para dar conta dessa tarefa, utiliza-se o método hipotético dedutivo. No primeiro capítulo será abordado o significado do direito fundamental de dados e a consonância com a privacidade e intimidade, o ordenamento jurídico internacional e nacional com relação à Lei Geral de Proteção de Dados (LGPD) e dificuldades no tratamento de dados, bem como as consequências possíveis na democracia. Enquanto que no segundo capítulo será tratado sobre o que a LGPD regula, as obrigações de proteção e tratamento de dados que o Estado e o âmbito privado devem acatar para estarem em consonância com a norma, da competência para legislar sobre proteção dos dados e acerca da compreensão quanto a Autoridade Nacional de Proteção de Dados (ANPD), além das dificuldades do sopesamento da Lei de Acesso à Informação (LAI) e a Lei Geral de Proteção de Dados (LGPD). Afinal, no terceiro capítulo será vista a Governança Pública Digital com os óbices para o tratamento de dados na modernidade, a importância dos sistemas de informações estatais e dos compartilhamentos de dados nas políticas públicas, serviços públicos e o controle social, os pontos positivos para a interoperabilidade na administração pública pátria e não menos importante, as divisas e viabilidades de compartilhamento e interoperabilidade por meio das leis, dos estudos de Direito difundidos e decisões judiciais. Assim, quanto a conclusão, pode-se afirmar que a interoperabilidade tem possibilidade de ocorrer para a efetivação da democracia por meio de ferramentas que proporcionem o controle social, evita a duplicidade de informações e perda dos serviços fornecidos no formato digital com uma proposição de um governo mais efetivo nas suas ações, evita a exibição tanto de informações como documental no que se refere ao indivíduo interessado na busca de elementos informacionais, políticas públicas mais

bem aproveitadas devido a possível troca de cadastros com aproveitamento de matérias necessárias, entretanto possui como limitação a informação pública submetida a sigilo por motivo de segurança para a sociedade e ao Estado, bem como dados pessoais em âmbito privado, requisitos, segurança da informação e comunicação, capacidade tecnológica, rentabilidade, custos em acesso de dados, reaproveitamento da infraestrutura investida, proteção de dados pessoais, dados em formato físico e das regulamentações que exigem determinados requisitos para sua implementação. Ainda, o compartilhamento deve respeitar a anuência do titular dos dados e interesse público, não sendo o consentimento necessário para políticas públicas, além disso dados da categoria ampla não precisam de anuência para compartilhamento, da restrita precisam de permissão da autoridade competente e não podem ter nova transmissão como regra, valendo o mesmo para a específica. Ainda, quem pediu os dados tem de arcar com os custos e pactos, bem como outros instrumentos não são requisitos para o procedimento.

Palavras-chave: Compartilhamento. Dados. Interoperabilidade. Limites. Possibilidades.

ABSTRACT

The present work monographic has as theme the interoperability and sharing of data from the data protection law and has as objective to investigate and to point the limits and the possibilities of sharing and the interoperability of data by the public and private subjects from the general data protection law in Brazil. In this context, the problem to be faced consists in which the limits and the possibilities of the interoperability and sharing of data by the government and by private subjects in accord with the general data protection law in Brazil. To handle this task, it is used the deductive hypothetical method. In the first chapter will be addressed the meaning of the fundamental data right and the consonance with the privacy and intimacy, the international legal ordem and national concerning to General Data Protection Law (GDPL) and difficulties in as well as the possible consequences in democracy. While in the second chapter will be treated about the GDPL regulates, the protection and data that the State private sphere must comply to be in line with the standard, of competence to legislate about data protection and about understanding regarding the National Data Protection Authority, beyond the difficulties of weighing of Acess to Information Law and the General Data Protection Law. In the end, in the third chapter will be seen the Digital Public Governance with the obstacles for the data processing in modernity, the importance of government information systems and shares data public policies, public services and social control, the positive points for interoperability in national public administration and not less important the currencies and infeasibility sharing and interoperability through laws of widespread law studies and court decisions. Thus, in terms of conclusion, it can be stated that interoperability has the possibility of occuring for the implementation of democracy through tools that can provide social control, avoiding duplication of information and loss services provided in digital format with a proposition of a government more effective in its actions, avoids the display of both information and documents with regard to the individual interested in the search for informational elements, public policies better utilized due to the possible exchange of records with the use of necessary materials, however it has the limitation of public information subject to secrecy for reasons of security for society and the State, as well as personal data in the private sphere, requirements, information and communication security, technological capacity, profitability, data access costs, reuse of invested infraestructure, protection of

personal data, data in physical format and regulations that require certain requirements for its implementation. Furthermore, sharing must respect the consent of the data holder and the public interest, with consent not being necessary for public policies. In addition, data from the broad category does not require consent for sharing, from the restricted category it requires permission from the competent authority and cannot have new transmission as a rule, the same being true for the specific one. Furthermore, whoever requested the data must bear the costs and agreements, as well as other instruments, wich are not requirements for the procedure.

Keywords: Sharing. Data. Interoperability. Limits. Possibilities.

SUMÁRIO

1 INTRODUÇÃO

O presente trabalho aborda o tema da interoperabilidade e compartilhamento de dados a partir da Lei de proteção de dados no Brasil. Em que busca responder ao problema de quais os limites e as possibilidades da interoperabilidade e compartilhamentos de dados pela administração pública e por sujeitos privados, em consonância com a Lei Geral de Proteção de Dados no Brasil?. Tendo como marco investigar e apontar os limites e as possibilidades de compartilhamento e interoperabilidade de dados pelos sujeitos públicos e privados, a partir da Lei Geral de Proteção de Dados no país. Enquanto que como objetivos específicos, se propõe a investigar o direito fundamental da proteção de dados no Brasil e sua relação com o direito fundamental da proteção à intimidade e vida privada, também para analisar o tratamento de dados pessoais em conformidade com a Lei Geral de Proteção de Dados no país e os deveres de proteção dos sujeitos públicos e privados, bem como os desafios de compatibilizar a proteção de dados com o dever de prestar as informações pela administração pública em consonância com a Lei 12.527/2011, por fim identificar os limites e as possibilidades de compartilhamento e interoperabilidade dos dados na Lei Geral de Proteção de Dados no Brasil.

Ainda, a metodologia da pesquisa quanto aos objetivos, será a exploratória com um maior conhecimento do problema ou no auxílio pra construção de hipóteses, aprimorando a construção de ideias, envolvendo o uso de pesquisa bibliográfica com livros e Artigos Científicos, os quais serão as principais fontes de dados no trabalho. Ademais, em relação ao método, é o hipotético dedutivo, a fim de permitir uma análise baseada em evidências. Por fim, sobre as técnicas, são realizadas pesquisas bibliográficas e artigos científicos, resultando em uma abrangência maior de números de dados para a pesquisa.

Portanto, a pesquisa se faz relevante, tendo em vista que com a evolução tecnológica a sociedade adquiriu acesso a uma grande quantidade de dados disponíveis e eles ganharam uma valorização importante. Até porque atualmente é mais acessível adquirir ferramentas como telefone celular e computador que o uso causa a exposição, bem como empresas armazenam dados das pessoas e transformam em informação, ou seja, compreendem como devem atuar no mercado, o que modificou as relações comerciais. Para seduzir os usuários vários serviços

oferecidos são gratuitos, mas em troca devem ser fornecidas informações para cadastro. Entretanto, as suas intimidades e privacidades expostas, bem como o livre desenvolvimento da personalidade, visto que seus dados são difundidos sem a real consciência dele e para influenciá-lo nas suas escolhas de vida.

Além disso, a divisão do trabalho foi feita em três capítulos, sendo que no primeiro será abordada a proteção de dados no Brasil, pois na presente pesquisa é imprescindível compreender acerca da Lei Geral de Proteção de Dados (LGPD) que rege as circunstâncias de quando o tratamento é possível ou não como meio de proteção aos indivíduos. Assim, há de ser falado do seu funcionamento, da relação com os direitos fundamentais à intimidade e privacidade reguladas na Constituição Federal, dos casos da jurisprudência sobre tratamento inadequado desses dados e legislação internacional, tratados, bem como convenções relevantes que regulam o assunto.

Por sua vez, o segundo capítulo mencionará das alterações que a LGPD provocou no ordenamento jurídico, bem como das eventuais dificuldades para que a presente legislação se comunique com a Lei de Acesso à Informação (LAI). Porque, ambas tratam de direitos fundamentais diferentes que aparentam contrariedade e por vezes podem ter conflitos a serem solucionados. Além disso, será falado tanto do Estado como da iniciativa privada perante o tratamento de dados e proteção deles, bem como a quem cabe a competência para legislar sobre a proteção de dados e a Autoridade Nacional de Proteção de Dados quanto ao seu papel importante de fiscalização para fazer cumprir a lei e demais funções.

O terceiro e último capítulo trará sobre a interoperabilidade e compartilhamento de dados que em decorrência da evolução tecnológica proporciona que eles sejam difundidos com mais rapidez e com uso de finalidade pública, mas que tem suas oportunidades de uso e impossibilidades, em decorrência também da realidade da gestão pública no país. Ainda, há a governança pública digital e seus óbices para a implementação, o compartilhamento de dados com sua importância para diferentes áreas da administração estatal como políticas públicas, serviço público e controle da máquina pública, pontos positivos da interoperabilidade como a efetivação da democracia, por fim possibilidades e limites tanto para o uso da interoperabilidade como do compartilhamento dos dados.

2 O TRATAMENTO DOS DADOS PESSOAIS NO BRASIL

Será abordado no presente capítulo quanto aos dados pessoais no Brasil serem considerados Direitos Fundamentais que satisfazem a dignidade humana dos indivíduos, bem como dentro do conceito dessas informações personalizadas estarem a intimidade e vida privada sob proteção legal que possuem relação. Em um segundo momento serão trazidos casos de jurisprudência pátrios demonstrando os impactos para a democracia do não cumprimento do Direito Fundamental aos dados pessoais. Por fim, legislação internacional, tratados e convenções relevantes serão adicionados à discussão na medida em que será possível ser realizado um estudo comparativo com o regulamento brasileiro pertinente ao tema.

2.1 Conceito de dados como direitos fundamentais e sua relação com a intimidade e vida privada

Em decorrência da evolução tecnológica que ocorreu, a rotina das pessoas depende do fornecimento dos seus dados e a coleta deles por parte de terceiros, envolvendo diferentes informações desde as mais básicas e as mais sensíveis que caindo em mãos erradas poderão existir prejuízos de grande monta.

Primeiramente, Doneda (2020) ilustra que a privacidade foi sendo desenvolvida em várias épocas em diferentes comunidades, entrando em discussão no Direito durante o término do século XIX com uma transição para a proteção dos direitos individuais, sendo resguardada acima de tudo a liberdade. Assim, a privacidade costumava ser entendida como uma ideia de esconderijo, ou seja, tendo um conceito mais individualista. Todavia, a percepção foi mudando ao longo do tempo e condiz com várias exigências dos indivíduos, bem como com o caráter e sua evolução, contendo ainda um valor a mais, como um requisito para que a pessoa em si possa se satisfazer completamente.

Ademais, Arendt (2007), ressalta que a propriedade privada tinha significado divino no passado, sendo condizente com a família que ali estivesse. Entretanto, caso fosse hipoteticamente inexistente, o indivíduo deixava de ter sua condição de cidadão daquela sociedade, bem como o resguardo legal por parte das normas. Enquanto que na atualidade, não é considerada como requisito pré-existente, mas

sim adquirida com muito esforço e que é tido como o único local o qual possibilita estar invisível para o público.

Não obstante, Garcia (2018) explica que a privacidade surgiu com a proteção da propriedade para a salvaguarda da ideia de liberdade proveniente de revoluções burguesas, entendendo como o local em que os indivíduos estariam resguardados da administração pública e inclusive de outras pessoas, existindo também o óbice da possibilidade de perda ou alienação desse bem para outrem. Entretanto, com o passar do tempo e a evolução coletiva, houve a melhoria das máquinas e junto disso a exibição do titular dos dados, sendo necessária uma reflexão maior sobre o assunto, passando a existir como transcendente em relação ao conceito anterior e se tornando direito de personalidade. Ainda, também fala da intimidade, sendo originada com a criação dos direitos fundamentais de segunda geração, ou seja, os chamados direitos sociais, visto que houve a atenção à proteção da compleição física do ser humano, nascendo o conceito a partir de então. Portanto, pode ser tido como a alternativa que possui para a disposição do próprio corpo de estar submisso ou não sob a direção de um terceiro, envolvendo a maneira como é visto pelos outros e seus afazeres mais particulares.

Outrossim, Neta (2010) define que a ideia de privacidade está muito próxima da personalidade, haja vista que vários desejos estão presentes por parte dos demais indivíduos da sociedade e da própria pessoa, em que todos eles almejam a chance de optar por possibilidades e em decorrência disso, a evolução do seu caráter.

Aliás, Jaborandy e Porto (2021) mencionam um exemplo que elucida melhor as diferenças entre os conceitos, utilizando a obra literária de George Orwell, chamada de 1984 em que o enredo demonstra a falta de respeito no que tange a privacidade e intimidade. Diante disso, Winston, o personagem principal, é controlado de forma massiva pelo governo, bem como os demais cidadãos da sociedade distópica. Ademais, não tinham a possibilidade de exercer pensamento crítico, receber notícias verídicas mesmo que contrárias ao partido político vigente, ter uma educação e cultura diferente da imposta pelo Estado, enfim de viver diversamente ao que era imposto. Logo, o direito de privacidade e intimidade é violável pela administração pública por meio de uma fiscalização absoluta, não

sendo respeitada a opção por escolhas próprias que desenvolvem a personalidade de cada um e inclusive fornecendo individualidade.

Ademais, Barbosa e Valle (2023), abordam o respaldo jurídico do direito fundamental à intimidade e privacidade com a menção ao Artigo 5°, inciso X, da Constituição Federal de 1988 (BRASIL, 1988) e por meio da origem do liberalismo nos séculos XVII e XVIII, onde as liberdades individuais eram garantidas visando um desenvolvimento próprio do indivíduo sem a intervenção estatal, em que a proteção restava somente sobre a propriedade, visto que não existiam outras exposições que justificassem uma maior proteção. Não obstante, a evolução tecnológica no decorrer dos séculos trouxe a necessidade de uma segurança maior ao resguardo da pessoa, pois a privacidade já não estava resguardada somente pela propriedade, mas sim tornou-se direito à personalidade. Além disso, insta salientar que eles são regulados por várias normas de instâncias nacionais e internacionais, inclusive os Estados-membros podem decidir como serão realizadas as defesas desses direitos de acordo com a competência de cada um deles. Logo, a própria Constituição abrange um bifurcamento da privacidade e intimidade, devendo haver uma análise de forma especificada.

Outrossim, Sarlet (2020) exemplifica que existem diversos regulamentos nacionais para o assunto, no que tange a Lei n.° 13.709/2018 (BRASIL, 2018) ou Lei Geral de Proteção de Dados que será tratada de forma específica mais adiante no presente trabalho, a Lei n.° 8.078/90 que é conhecida como Código de Defesa do Consumidor (BRASIL, 1990), a Lei n.° 12.965/2014 (BRASIL, 2014) também chamada por Marco Civil da Internet, a Lei n.° 12.527/2011 (BRASIL, 2011) nomeada como Lei de Acesso à Informação e o Habeas Data com a Lei 9.507/97 (BRASIL, 1997) e o Artigo 5°, Inciso LXXII, da Constituição Federal (BRASIL, 1988).

Todavia, a norma a qual deverá ser fornecida especial atenção é o Código Civil, o qual, de acordo com Vieira (2007), estabeleceu certas possibilidades para o resguardo da personalidade dos Artigos 11 ao 21 (BRASIL, 2002).

Enquanto que na doutrina dos Estados Unidos da América, Allen (2013) e Brandeis e Warren (1890), dispõem que não há diferença entre a intimidade e a privacidade, deixando de ser conceituado na legislação e sendo definido somente nos casos jurisprudenciais americanos com um significado não tão exato, como é o caso da Quarta Emenda à Constituição dos Estados Unidos. Portanto, os

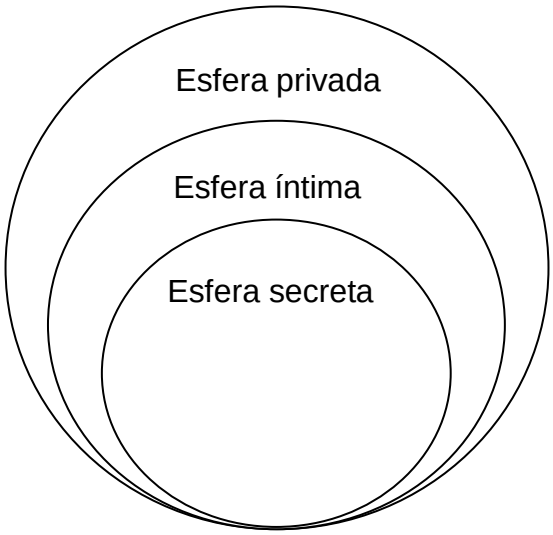
americanos compreendem a privacidade como conceito que ocorre a partir da propriedade, impondo restrições ao poder público quanto a transgredir, gerenciar e de poder fazer disposição dela. Não obstante, para os estadunidenses, a ideia foi oriunda de um artigo feito por dois procuradores em que debateram a capacidade de usurpação e sua evolução cada vez maior por parte do Estado e da imprensa na vivência das pessoas. Todavia, as decisões judiciais se desenvolveram e o significado inicial foi deixado para trás, dando lugar para um bem mais dificultoso.

No entanto, a diferenciação não é uníssona na doutrina brasileira, por um lado sendo semelhante ao Direito Estadunidense no sentido de não diferenciar ambos os conceitos e por outro, existem doutrinadores brasileiros que os separam, dentre eles Pereira (2006), o qual na comparação entre os significados, ele compreende a intimidade como o resguardo de um âmbito mais intrínseco do indivíduo.

Ademais, Sampaio (1993) comenta de maneira mais específica sobre ambos os conceitos, sendo para ele a privacidade como o direito que o indivíduo tem de estar sozinho, ter informações em relação a ele que não são sujeitas a compartilhamento com outras pessoas e a possibilidade de dispor de seus dados como pessoa física autônoma que é. Enquanto que a intimidade seria um complemento da privacidade, garantindo que possa estar sozinho, caso for de sua vontade.

Ainda, Hirata (2017), aborda a teoria das esferas do direito da Alemanha, onde os conceitos examinados seriam provenientes de uma crescente salvaguarda da opção de estar só. Assim, a privacidade é partida em três camadas, a privada, íntima e a secreta. A primeira é a mais geral em relação às restantes por englobar as demais e diz respeito ao campo privado, em que são incluídas atitudes que o titular dos dados não detém vontade que se tornem de conhecimento público. Enquanto que a segunda está dentro da anterior e é a intimidade, uma intermediária das outras, sendo acessível somente para indivíduos de confiança e que sejam próximas. Por fim, a terceira e de menor tamanho pode ser definida como sigilosa. Diante do exposto, será retratada abaixo a ilustração do explanado supra.

Figura 1: Teoria das Esferas.



Fonte: Linkedin, 2020.

Logo, possível dizer que quanto mais secreto for o componente, haverá uma proteção jurídica cada vez maior quanto aos direitos ali envolvidos dos titulares e que as divergências das ideias aqui discutidas seriam em decorrência disso, de acordo com a teoria das esferas.

Portanto, de acordo com Sarlet (2020), o direito fundamental da proteção de dados pessoais ainda não era positivado de forma clara na Carta Magna brasileira, em que restava somente o resguardo das comunicações de dados, cartas, telefonemas e telégrafos, no Artigo 5°, Inciso XII, da CF (BRASIL, 1988) e o remédio constitucional do Habeas Data, pela Lei 9.507/97 (BRASIL, 1997) e o Artigo 5°, Inciso LXXII, da Constituição Federal (BRASIL, 1988). Ainda, em nível abaixo da Constituição, existem a Lei Geral de Proteção de Dados com o n° 13.709/2018 (BRASIL, 2018), o Marco Civil da Internet n° 12.965/2014 (BRASIL, 2014) e a Lei de Acesso à Informação n° 12.527/2011. Assim, pode-se dizer que os dados em questão eram ao menos considerados parcialmente presentes no ordenamento jurídico pátrio para proteção e por causa das regulamentações constitucionais, desde já subentendida.

Porém, segundo Fachin (2022), após a Emenda Constitucional n.° 115/2022 (BRASIL, 2022), a proteção de dados pessoais foi finalmente prevista e considerada como direito fundamental de forma expressa no Artigo 5°, inciso LXXIX, da Constituição Federal brasileira (BRASIL, 1988), o qual possui a incidência sobre qualquer elemento que se refira à determinada pessoa, não delimitando somente

àqueles de formato tecnológico, ou seja, não há importância quanto ao local em que está.

Contudo, os dados são direitos fundamentais respaldados pela Carta Magna brasileira, onde existem o direito a intimidade e privacidade. Elas por sua vez garantem que os titulares possam estar sós, sem interferências por parte de terceiros, tendo a proteção da sua personalidade e não tendo seus dados difundidos, não sendo exposto perante estranhos com o uso errôneo dessas informações que poderão ser acarretados danos. Inclusive, o tratamento inadequado pode infringir direitos fundamentais muito caros para a Constituição, onde hão de ser demonstradas decisões judiciais sobre o assunto.

2.2 Legislação internacional e os tratados e convenções relevantes no tema da interpretação de dados

Diante de casos jurisprudenciais universais e nacionais, serão abordadas leis, tratados e convenções importantes para a interpretação de dados. Não obstante, o Brasil se inspirou em alguns e como não é líder no tema, será feita a comparação em virtude dos demais ordenamentos jurídicos, sendo feita também uma análise do patamar em que o país está em relação à matéria.

Os países nórdicos foram os líderes em relação ao regramento de informações públicas, como afirma Júnior (2018), tendo a Suíça em 1766 inventado um comitê, a fim de tratar das manifestações da mídia, tanto na forma escrita como de opinião, sem que precisassem passar pelo crivo da censura. Assim, é a primeira norma que tratou do acesso às informações de perfil público na instância mundial.

Posteriormente, em 1789 aconteceu a Revolução Francesa que criou a Declaração de Direito do Homem e do Cidadão, sendo que no seu artigo 15 restou assegurado o direito do cidadão a pedir a prestação de contas para quem estivesse encarregado da administração estatal, de acordo com Novo (2021).

Ainda, em 1951 surgiu a segunda lei que rege o acesso das informações públicas na Finlândia. Após, em 1970 foram as vezes da Noruega e Dinamarca, a criação dos seus ordenamentos jurídicos, conforme Limberger (2022).

Enquanto que, Spiecker Genannt Döhmann (2020) elucida acerca da proteção de dados pessoais, ela começou no ano de 1970, em Hesse, na Alemanha,

sendo a primeira regulação da matéria em todo o globo terrestre. Ainda, a sua legislação pátria fornece significado semelhante ao exposto na lei brasileira, na medida em que acrescenta que os dados pessoais ainda seriam informações especificadas acerca das situações pessoais ou de fato sobre determinado indivíduo identificado ou identificável, conforme Guidi (2021).

Posteriormente, no ano de 1978 a França, por meio de sua legislação, regulou a criação de Comissão Nacional para Proteção de Dados, de acordo com Doneda (2020). Enquanto que a lei francesa de proteção de dados é anterior a lei brasileira e define os dados pessoais no seu Artigo 2° como sendo aquilo que identifica determinada pessoa ou pode vir a identificá-la, inclusive significado ao qual a lei nacional de proteção de dados (LGPD) utiliza no seu ordenamento jurídico no Artigo 5°, inciso I, da Lei n.° 13.709 (BRASIL, 2018), conforme Guidi (2021).

Ademais, como mencionado supra, a França elaborou sua própria lei, sendo que, de acordo com Carvalho e Rosa (2023), se inspirou na da União Europeia. Ainda, a lei francesa influenciou a norma de Portugal referente ao assunto. Além disso, o Reino Unido também é um país que possui o próprio ordenamento jurídico.

Quanto à legislação europeia, Silva e Silva (2018), lembram que houve a Diretiva 95/46/CE (UNIÃO EUROPEIA, 1995) no ano de 1995, sendo tratada como a norma mais relevante no assunto, visto que as leis posteriores da mesma matéria e feitas por membros da União Europeia se inspiraram nela. Além disso, de acordo com as disposições e o Artigo 8°, da Carta de Direitos Fundamentais da União Europeia do ano 2000 (UNIÃO EUROPEIA, 2000), são criados os direitos fundamentais da União Europeia, envolvendo princípios pelos quais o ente precisará agir e como mais notável acontecimento, o estabelecimento da proteção de dados pessoais como direito fundamental. Não obstante, de acordo com Silveira e Froufe (2018), bem como com o Regulamento Geral de Proteção de Dados da União Europeia (UNIÃO EUROPEIA, 2016), o ente tinha a Diretiva n° 95/46/CE (UNIÃO EUROPEIA, 1995) em vigência, porém posteriormente em 2016 houve a publicação da sua nova lei de proteção de dados, também conhecida como General Data Protection Regulation (GDPR) (UNIÃO EUROPEIA, 2016) que está vigorando desde o ano de 2018.

Inclusive, conforme Barbosa e Valle (2023), o GDPR teve grande influência na legislação brasileira da matéria que é a LGPD, como é o caso do *ex-ante*, em que

no momento anterior da coleta e antes mesmo de usar os dados, quem estiver o tratando deve desde já motivá-lo em conformidade com as situações legais do Artigo 7°, Caput e incisos, da LGPD (BRASIL, 2018).

Não obstante, de acordo com Sarlet (2020), a Constituição brasileira (BRASIL, 1988), também trouxe regulação do conteúdo, primeiro de forma implícita antes do ano de 2022, por meio do Artigo 5°, inciso XII, da CF (BRASIL, 1988) com a confidência de interações dos elementos informáticos condizentes com os indivíduos, isso sem falar no direito da reserva dos telegramas, ligações e mensagens por telégrafo. Ainda, posteriormente, Sarlet (2022) acrescenta que com a vinda da Emenda Constitucional n.° 115/2022 (BRASIL, 2022), a proteção de dados pessoais foi finalmente incorporada como direito fundamental positivado no Artigo 5°, da Constituição Federal (BRASIL, 1988).

Enquanto que no Código Civil, conforme Doneda (2020), existem os Artigos 11 ao 21, (BRASIL, 2002) em que a privacidade é resguardada em total consonância com a personalidade e quanto a esses direitos que os indivíduos são titulares.

Por fim, o Regulamento europeu de n° 1049/2001 (UNIÃO EUROPEIA, 2001) abrange a possibilidade de acesso aos documentos estatais da União Europeia, referente a instituições, organismos, serviços e suas agências. Entretanto, no caso de possível prejuízo para o interesse comum e de afetar a vida privada, existem exceções ao direito estipulado, assim sendo relativo e não integral.

Assim, o Brasil não foi o pioneiro na elaboração de lei sobre proteção de dados, tendo se inspirado em outras legislações referentes à matéria que já estavam mais bem consolidadas, como é o caso mencionado supra acerca do GDPR. Diante disso, posteriormente o país elaborou sua própria legislação, sendo a Lei Geral de Proteção de Dados (LGPD), conforme Almeida e Soares (2023). Logo, em seguida será abordado das dificuldades para a realização do procedimento correto para a proteção de dados e, caso feito de maneira errônea, prejuízos que possam ser causados em face da democracia, também sendo exemplificado através de casos jurídicos reais.

2.3 Desafios ao tratamento adequado de dados e seus possíveis impactos na democracia

Após a verificação supra acerca do direito fundamental de intimidade e vida privada quanto aos dados das pessoas naturais e jurídicas, bem como das normas nacionais e internacionais acerca da interpretação da proteção de dados, deverão ser verificados casos jurisprudenciais das dificuldades para o tratamento correto dos dados e resultados que porventura possam afetar a democracia. Ademais, com isso há de ser verificada a importância quanto a proteção mencionada.

Em 2013, conforme Calsing (2019), foi feito no Brasil um acordo de cooperação entre o Tribunal Superior Eleitoral (TSE) e a Serasa, sendo que a empresa ainda poderia passar os dados aos seus clientes com a finalidade deles saberem como os devedores se encontravam no momento, bem como da correta identificação do indivíduo, sendo mais fáceis as ações de cobrança e evitando fraudes tanto na realização de negócios jurídicos como no fornecimento de crédito para pessoas falecidas. Assim, foram fornecidos os dados de cadastro das eleições no montante de 141 milhões de pessoas quanto aos nomes, número e status da inscrição eleitoral, mortes, nome da genitora e dia de nascimento. Enquanto que ao órgão jurisdicional seria dado em troca, uma assinatura eletrônica aplicável para documentos oficiais (certificação digital) que facilitaria o andamento dos processos digitais.

No entanto, o Supremo Tribunal Federal (STF) cancelou o pacto com base, inclusive, no direito fundamental da privacidade, tendo a presidente do STF naquela oportunidade, a Ministra Carmen Lúcia, fundamentado que as pessoas jurídicas de direito privado possuem finalidades privadas e não podem ter autorização pela Justiça Eleitoral para acessar os dados e utilizá-los com finalidade diversa ao qual foi atribuída de somente entregar aos cuidados da administração pública.

Além disso, de acordo com Fornasier e Beck (2020), houve outra ocorrência em 2016 nas eleições dos Estados Unidos da América (EUA) e no Brexit, onde a pessoa jurídica Cambridge Analytica foi acusada de por meio dos dados coletados no Facebook em testes de personalidade, ter utilizado para dar suporte aos candidatos, a fim de obterem uma melhor comunicação perante os eleitores. Aliás, cabe salientar que foram divulgadas notícias falsas e que os usuários foram comunicados de outra finalidade no momento da concessão dos dados, diferente do que ocorreu na prática.

Ainda, deve ser mencionada as eleições de 2018 no Brasil, sendo o caso de maior repercussão no país devido ao Estado Democrático de Direito constituído. Ademais, Almeida (2021) elucida que as redes sociais foram utilizadas como principal instrumento na decisão do processo eleitoral, em que houve um grande investimento financeiro e por sua vez promovendo compartilhamento de notícias falsas sem possibilidade de verificação da veracidade, bem como para indivíduos que sequer consentiram no recebimento.

Por fim, em maio de 2020 foi julgado nas Ações Diretas de Inconstitucionalidade (ADIs) de n.° 6.387, 6.388, 6.389, 6.390 e 6.393, liminarmente pela ministra Rosa Weber do Supremo Tribunal Federal (STF), a suspensão da Medida Provisória (MP) n.° 954/2020. Além disso, o fato ocorreu porque ela continha como conteúdo o compartilhamento de informações pessoais em relação aos clientes de linhas telefônicas tanto fixas como móveis, que as empresas do ramo possuíam o controle. Assim, foi definido na decisão que nomes, números de telefone e endereços que identificam determinada pessoa ou podem identificá-las, são dados pertencentes a esses usuários que merecem resguardo legal do direito fundamental no Artigo 5°, Caput, da Constituição Federal (BRASIL, 1988) em relação às liberdades, bem como da privacidade e livre desenvolvimento da personalidades, esses por sua vez no Artigo 5°, incisos X e XII, da Constituição Federal (BRASIL, 1988), conforme Pinheiro e Cotta (2022). Por fim, a decisão foi confirmada posteriormente pelo tribunal.

Assim, os presentes casos narrados demonstram que os vazamentos de dados ou o mero tratamento inadequado, tornam a causar ofensa aos direitos de privacidade e intimidade dos cidadãos envolvidos, pois são extensões das suas personalidades para outras pessoas jurídicas utilizarem com fim diverso ao combinado, sem falar dos indivíduos não terem autorizado a transferência. Há de se falar o mesmo para o caso apresentado por Fornasier e Beck (2020), bem como Almeida (2021), a primeira sobre as eleições e o Brexit com o plebiscito, tendo em vista que por meio da coleta errônea de dados sem a concordância e da divulgação, existiram transgressões de decisões livres asseguradas pelos direitos de personalidade dos indivíduos, sem falar da veiculação de fatos inverídicos, já o segundo menciona os compartilhamentos de notícias falsas sem averiguação de veracidade para as pessoas sem autorização e que também comprometem a livre

gerência sobre suas próprias vidas, devido à manipulação da manifestação de vontade nas eleições.

Ademais, em seguida será abordado da regulação da proteção de dados no país como um todo, sendo explanadas suas nuances. Além disso, também serão tratados dos óbices para a Lei Geral de Proteção de Dados e a Lei de Acesso à Informação conviverem de forma harmônica no ordenamento jurídico, considerando que uma trata do resguardo e a outra da divulgação dos elementos pertencentes aos titulares.

3 MARCO REGULATÓRIO DE PROTEÇÃO DE DADOS NO BRASIL E O DESAFIO DA COMPATIBILIDADE COM O ACESSO À INFORMAÇÃO COMO DEVER DA ADMINISTRAÇÃO PÚBLICA

Ao longo do presente capítulo será abordado sobre o surgimento da Lei Geral de Proteção de Dados (LGPD) no Brasil com tudo que ela abrange na sua regulação. Ainda, dos deveres atribuídos para sujeitos públicos e privados devido à LGPD, bem como da Lei de Acesso à Informação (LAI) que estipula fornecimento de informações públicas. Além disso, quem teria a competência legislativa para legislar sobre proteção de dados e a autoridade nacional de proteção de dados (ANPD). Por fim, os óbices a serem superados para a LAI e a LGPD convergirem em prol das regulações que trazem consigo.

3.1 Lei Geral de Proteção de Dados (LGPD)

A legislação de proteção de dados pessoais surge no Brasil em 2018, mesmo ano em que o General Data Protection Regulation (GDPR) (UNIÃO EUROPEIA, 2016), regulamento acerca da matéria entrou em vigor na União Europeia, tendo sido uma inspiração para a nova integrante do ordenamento jurídico brasileiro, conforme Queiroz (2021).

Como diz Siderly e Tania (2022), é lei de abrangência nacional aplicável para todos os entes federativos do país, conforme Artigo 1°, Parágrafo Único, da LGPD (BRASIL, 2018), ou seja, União, Estados, Distrito Federal e Municípios. Além disso, de acordo com o Artigo 1°, Caput, da LGPD (BRASIL, 2018) tanto as pessoas físicas como as jurídicas de direito privado e público estão sujeitas ao ordenamento, a fim de protegerem os dados físicos e digitais, bem como à pessoa natural em relação aos direitos fundamentais estipulados na Constituição Federal, tais como a liberdade, privacidade e livre desenvolvimento de personalidade.

Inclusive, a norma da matéria possui incidência sempre que existirem dados sendo modificados por parte de pessoas físicas, não importando o meio do procedimento, bem como a nação em que estão sediados ou presentes naquele momento, sendo de caráter imprescindível que o tratamento de dados ocorra no Brasil com o intuito de oferta ou providenciar bens, além do tratamento de dados em

circunscrição brasileira. Portanto, para aqueles dados a serem tratados com objetivo individual, sem motivo financeiro, na defesa nacional do país, segurança, investigação, penalização dos delitos de instância penal, jornalismo, arte e de ensino na academia, não existe subordinação diante da norma, de acordo com Cartolari e Silva (2019) juntamente com os Artigos 3° e 4°, da LGPD (BRASIL, 2018).

Ademais, a lei fornece os significados dos dados classificados em pessoais, sensíveis e anonimizados no Artigo 5°, incisos I, II e III, da LGPD (BRASIL, 2018), conforme Santos (2020). Assim, o primeiro conceito é considerado como sendo uma informação de determinado indivíduo que o identifique ou tenha potencial de identificá-lo. Enquanto que o segundo tipo de dado é o pessoal sensível, acerca da raça, etnia, crença religiosa, ideologia política, se faz parte de sindicato quanto a filiação ou ainda em organizações de caráter tanto religioso, como filosófico ou de política, dados que caracterizem a saúde, inclusive o aspecto de atração sexual, por fim dados de genes ou biométricos, contanto que estejam associados a uma determinada pessoa física. Enfim, o último é o dado anonimizado, quando a pessoa não é passível de ser identificada como titular daquele dado, visto que determinados procedimentos foram utilizados durante o tratamento necessitado.

A proteção dos dados pessoais cabe tanto para as pessoas físicas como jurídicas, sendo para os formatos em geral e até mesmo de âmbito digital, de acordo com Artigo 5°, inciso LXXIX, da Constituição Federal (BRASIL, 1988). Assim, o formato do dado é irrelevante para que mereça proteção ou não, sendo físico ou digital, porque o tamanho do dano que possa provocar depende da situação como a abrangência do público que virá a ter conhecimento daquilo, de acordo com Guidi (2021).

Ademais, de acordo com Barbosa e Valle (2023), a LGPD adota o modelo ex-ante, realizando uma proteção prévia dos dados pessoais que identifiquem o indivíduo ou sejam capaz de nomeá-lo, visto que antes mesmo de coletados ou de utilizados para determinado fim, o responsável pelo tratamento de dados deve motivar o processo por pelo menos alguma das hipóteses elencadas no Artigo 7°, Caput e incisos, da LGPD (BRASIL, 2018). Ainda, a ideia da norma é a presunção de importância aos dados e informações pessoais, haja vista que eles são costumeiramente utilizados em grande quantidade na modernidade, exigindo a devida normatização do processamento para a proteção dos direitos dos titulares.

Assim, a norma visa proteger os direitos fundamentais da privacidade e liberdade, por meio dos fundamentos elencados no Artigo 2°, Caput e incisos, da LGPD (BRASIL, 2018), de acordo com Almeida e Soares (2023). Dentre os quais, possível citar, a privacidade, autodeterminação informativa que é o direito do próprio titular dos dados ter consciência da finalidade do uso e de poder interferir também, liberdades de expressão, informação, comunicação e opinião, a não violabilidade da intimidade, honra e imagem referente aos titulares de dados; o desenvolvimento econômico e tecnológico, bem como da inovação, uma vez que os dados são essenciais para que as empresas exerçam as suas atividades; a livre iniciativa, a livre concorrência e a defesa do consumidor, já que as disputas entre negócios são respaldadas pelo Direito, desde que haja legalidade; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Ainda, devem ser distinguidos os conceitos de dados e informações, haja vista que comumente confundidos e possuem significados diferentes. Assim, conforme Bitencourt, Cristóvam e Tavares (2022) e Artigo 2°, I, da Instrução Normativa n.° 4, de 2012 (BRASIL, 2012), dados são tanto símbolos como valores que são representados em determinadas formas e por meio de procedimentos naturais ou artificiais, não sendo possível obter uma conclusão através da junção entre eles. Enquanto que as informações, conforme Bitencourt, Cristóvam e Tavares (2022) e Artigo 2°, II, da Instrução Normativa n.° 4, de 2012), ao contrário dos dados, ao serem juntados demonstram uma situação específica que passa a ser compreensível.

Além disso, para Bioni (2019), os conceitos de dado e informação se diferem, por mais que sejam taxados como sinônimos no dia a dia. Enquanto que o primeiro termo, de acordo com Cristóvam e Hahn (2020), é considerado como um estágio inicial da informação, visto que não o é, mas que potencialmente poderia ser diante de processamento ou organização. Agora, quanto ao segundo conceito, Vieira (2007) elucida que é a informação, define-se como sendo dado, um deles ou uma soma, após ter passado por procedimento de processo ou não necessariamente, no caso em que já estaria em plataforma que pudesse informar, portanto exemplifica-se com foto, volume, documentos em mídia física ou digitalizado, por fim podendo ser também determinado dado a sós.

Portanto, para Tepedino e Doneda (2018), as informações são tidas de enorme importância, haja vista que as informações possibilitam a compreensão dos consumidores em potencial, suas atitudes usuais, bem como outras, em suma podendo servir de subsídio para as decisões a serem feitas nas instâncias táticas e estratégicas de como agir no mercado. Não obstante, são muito utilizadas no cotidiano como na internet e em serviços, sendo concedidas com muita frequência para outrem. Ademais, após o fornecimento, o titular perde a administração da utilização deles, ficando sujeito aos atos de quem os detiver. Assim, a vontade da pessoa também resta prejudicada, não somente pela manipulação em virtude das suas informações, mas também pelos prejuízos possíveis em caso de tratamento indevido de dados pessoais sensíveis que por ventura possam provocar discriminação e danos ao titular.

Quanto a sua aplicação em temas mais específicos, Cotta e Pinheiro (2022) elucidam que a lei regula a investigação de delitos administrativos. No entanto, não se aplica para apuração de irregularidades criminais e de sua punição, de acordo também com a exclusão contida no Artigo 4°, III, d, da LGPD (BRASIL, 2018).

Em decorrência da necessária proteção inovadora aos dados digitais, foram estabelecidos no Artigo 7°, Caput e incisos, da LGPD (BRASIL, 2018), os procedimentos de tratamento dessas informações pessoais no que tange a forma correta de ser feito e inclusive de acordo com (GUERREIRO e TEIXEIRA, 2022, P. 90 - 91), não há hierarquia entre as hipóteses legais apesar que o consentimento seja trazido por muitos como a principal opção.

Ademais, as hipóteses do Art. 7°, Caput e incisos, da LGPD (BRASIL, 2018) são de poder ocorrer através da anuência por parte da pessoa que os dados sejam pertencentes. Além disso, as situações a seguir não necessitam do consentimento, como quando o controlador é obrigado a fazer o procedimento em virtude de lei, bem como a administração pública em caso de utilizar as informações para cumprir políticas públicas legisladas ou regulamentadas, quando necessários para estudo por órgãos de pesquisa como o IBGE, também no caso de cumprir contrato como em entrega de uma mercadoria comprada ou fase preliminar no que tange a ser antes do contrato sequer ter sido celebrado, por exemplo, consulta do CEP para cálculo do custo de frete, exercício regular de um direito exemplificado no fornecimento dos dados de testemunhas para um processo judicial ou em litígios

tanto administrativos como arbitrais, com fins de proteção da vida ou incolumidade física em que pode ser citado algum acidente que seja necessário pegar os dados do indivíduo que foi vítima para protegê-lo, procedimentos por profissionais de saúde ou serviços ou entidades sanitárias para proteger a saúde de determinada pessoa ou da coletividade como na coleta de dados antes da realização de eventual exame, no envolvimento de legítimo interesse por quem está tratando como uma medida de segurança da empresa para não ter fraude, proteção ao crédito como nos cadastros de restrição ao crédito para que a economia possa se desenvolver.

Ainda, há de ser explicado que os dados pessoais sensíveis definidos pelo Artigo 5°, inciso II, da LGPD (BRASIL, 2018), por serem informações que são mais sujeitas a danos para a pessoa envolvida, como é o caso da discriminação, assim necessitam de proteção maior com procedimentos mais sérios estipulados no Artigo 11, Caput e incisos, da LGPD (BRASIL, 2018). Como nos casos de consentimento pelo estipulado no inciso I ou sem ela nas situações do inciso II, em cumprir obrigação legal ou regulatória, dados exigidos para que a administração pública cumpra políticas públicas, estudos por órgão de pesquisa, exercício regular de direitos, proteção da vida ou incolumidade física e tutela de saúde.

Assim, quanto aos dados sensíveis para estudos por órgãos de pesquisa, Almeida e Soares (2023) mencionam que há uma menção específica no Artigo 13, Caput e Parágrafos, da LGPD (BRASIL, 2018), em que o uso desses dados é permitido a esses entes, bem como o tratamento a ser realizado é somente no âmbito interno do local e deve ser realizado com o respeito ao objetivo para o qual foram concedidos. Ainda, o tratamento deve ocorrer de forma que, quando for cabível, os dados sejam anonimizados ou pseudoanonimizados e que a ética seja considerada no procedimento. Por fim, está proibido de os resultados serem mostrados divulgando os dados pessoais de pessoas envolvidas, inclusive perante terceiros.

No entanto, Almeida e Soares (2023) alertam que caso os controladores compartilharem os dados sensíveis em seu poder por troca de vantagem financeira, o Poder Público imporá sanções, uma vez ouvidos os órgãos setoriais que o integram. Além disso, se na área da saúde os controladores usarem ou fizerem o compartilhamento dos dados pessoais sensíveis para ganho de dinheiro, também arcarão com sanções, de acordo com o Art. 11, §4°, da LGPD (BRASIL, 2018).

Ademais, de acordo com Barbosa e Valle (2023), em relação à Autoridade Nacional de Proteção de Dados (ANPD), as informações quanto a sua segurança devem ser cuidadas ainda após o seu tratamento, caso ocorra acidente com possibilidade de prejuízo ou que já tenha tido resultado adverso em termos de proteção, é imposta que a pessoa no cargo de operadora faça o célere aviso para a ANPD, devendo conter as explicações dos fatos ocorridos, informações de quem foi prejudicado como titular dos dados, males relacionados que podem provocar mais resultados ruins e, por fim, as atitudes a serem tomadas pra que o estado anterior ao dano seja reestabelecido.

Por fim, existem sanções administrativas previstas no Artigo 52, incisos I ao XII, da LGPD (BRASIL, 2018), em eventuais descumprimentos da norma entre os Artigos 1° ao 65, da LGPD (BRASIL, 2018) a serem aplicadas por meio da Autoridade Nacional de Proteção de Dados (ANPD), algumas delas a advertência com prazo para correção do que está irregular, dados pessoais bloqueados em relação à gravidade cometida até que seja consertada, atividades da empresa pertinente ao banco de dados não podem ser feitas de forma total ou parcial a depender se as atitudes tem relevância com as faltas cometidas.

Em suma, Garcel, Moro, Netto e Hippertt (2020), sintetizam que a LGPD (BRASIL, 2018) é uma lei que busca regularizar a utilização dos dados, bem como preservar os direitos fundamentais da liberdade e privacidade, não obstante busca respeitar a vontade do titular, apesar de que tenham situações como de interesse legítimo e de interesse público configuradas como exceções. Ainda, possui aplicação ampla, o que provoca o respeito às particularidades dos indivíduos que são normatizados no ordenamento jurídico, bem como propõe um rito a ser seguido e as medidas para preservação dos dados recolhidos, ainda assim proporcionando a evolução dos aparatos tecnológicos, posto que o regulamento possui uma parcela de liberdade e também de razoabilidade na sua finalidade.

Assim, serão especificados a seguir quanto aos deveres tanto da proteção como do tratamento de dados pelo Estado e no âmbito privado, bem como as devidas diferenças no que tange a cada uma delas.

3.2 Os deveres de proteção e tratamento dos dados pela administração pública e sujeitos privados

O conceito de tratamento de dados pode ser definido por meio do Artigo 5°, inciso X, da LGPD (BRASIL, 2018), sendo toda atividade com o uso de dados pessoais referente a determinada pessoa física ou jurídica que são atribuídos a ela diretamente ou que o titular dos dados possa ser descoberto.

Ainda, Sarlet (2022) menciona que o tratamento de dados surgiu com a Emenda Constitucional n° 115 na Constituição, a qual adicionou o Artigo 5°, inciso LXXIX, da CF, (BRASIL, 1988), que fala sobre a proteção dos dados pessoais ser assegurada por meio do que a lei disciplina e também nos meios virtuais, a fim de regular o conhecimento dos dados por parte da sociedade, tanto pela administração pública como por outrem, não proporcionando um acesso absoluto, e sim relativo com certas condições.

Enquanto que os dados pessoais, conforme Artigo 5°, inciso I, da LGPD (BRASIL, 2018) e definição de Barbosa e Valle (2023), podem ser conceituados como aqueles conhecimentos em forma de símbolos relativos a um determinado indivíduo que uma vez tratados resultam em uma informação daquela pessoa, como são os casos do cargo, identificação, endereço residencial, CEP, número de contato, quem são as pessoas integrantes da sua família, município de nascimento, numerais do cartão de crédito, informações de conta bancária, e-mail, quanto recebe no trabalho, conversas em aplicativos de mensagens, imagens, clipes, endereço IP, bem como outras situações.

Quanto aos sujeitos privados, Almeida e Soares (2023) mencionam as instituições de ensino superior, consideradas as de qualquer área onde atuam e até mesmo porte, visto que são constituídas de modo a terem amparo da empresa que as mantém, sendo consideradas como controladoras que possuem o encargo da transparência no tratamento de dados considerado de seu legítimo interesse, conforme o Art. 10, §2°, da LGPD (BRASIL, 2018). Ademais, os entes mencionados fazem a coleta constante de uma grande quantidade de dados de forma contínua, sendo determinado por via de lei uma maior transparência da sua parte com o tratamento dos dados pessoais coletados, de maneira que a portabilidade dos dados para outro fornecedor de serviço somente pode ocorrer mediante requisição expressa do interessado, em conformidade com a regulamentação da autoridade

pátria e com a defesa dos segredos industrial, bem como dos comerciais, de acordo com o Art. 18, Inciso V, da LGPD (BRASIL, 2018).

Não obstante, em se falando do poder público, houve uma nova filosofia quanto ao gerenciamento, aspecto financeiro e administração de tarefas tidas como públicas, visto que a evolução tecnológica e o uso mundial proporcionou uma difusão de ferramentas de tecnologia da informação (TICs), bem como de aparatos tecnológicos para manutenção e guarda dos dados, os quais vem apresentando mais capacidade. Assim, foi possível concluir que os dados das pessoas não são necessariamente sós, mas que podem ser transformados em informações de grande valia, logo o Estado possui a responsabilidade de agir com atitudes para defesa dos titulares e daqueles que detém a incumbência de realizarem o procedimento de tratamento.

Outrossim, Castro e Lovato (2020), exemplificam com o Tribunal de Contas, o qual detém funções que envolvem a necessidade de captar dados e por consequência, o dever de tratá-los. Ademais, é impositivo que o mesmo seja dito quanto à admissão de pessoas, visto que nos pactos firmados os dados também aparecem, bem como em registros de indivíduos que ingressam no local para conhecerem, exames probatórios para entrada no serviço público, fiscalização do lado de fora do órgão como menciona o Art. 71, da Constituição Federal (BRASIL, 1988), avaliação de cálculos prestados por parte daqueles submetidos ao procedimento.

Enquanto que, Monteiro (2020) ressalta que toda a administração pública, tanto direta como indireta, possui a incumbência do tratamento de dados, haja vista que o Artigo 3°, Caput, da LGPD (BRASIL, 2018), estabelece sua abrangência inclusive para ela.

Ademais, o Estado possui dever de tratamento dos dados por meio do Artigo 23, Caput, da LGPD (BRASIL, 2018), que por sua vez o faz visando satisfazer os direitos da sociedade e com interesse público por meio da realização de competências legais ou cumprir as funções encarregadas ao serviço público.

Além disso, o poder público na forma de seus órgãos devem realizar o tratamento de dados pessoais em conformidade com o Art. 6°, da LGPD (BRASIL, 2018), quanto aos princípios que estabelece.

Dentre as diretrizes mais relevantes estão a necessidade, finalidade e adequação, devendo ter relação entre a coleta de dados pessoais e a finalidade do procedimento de tratamento, bem como há de existir explicação ao titular de dados para que ocorra da maneira correta disposta pela lei, de acordo com Cotta e Pinheiro (2022). Inclusive, o tratamento de dados acerca de suas minúcias devem ser disponibilizados em sítios eletrônicos estatais, cumprindo com a transparência ativa.

Além disso, Têmis (2022) concorda que o tratamento deve se pautar pelo princípio da transparência que se encontra disposto no Artigo 6°, inciso VI, da LGPD (BRASIL, 2018). Inclusive, Limberger (2022) em concordância com Cotta e Pinheiro (2022), se manifesta da mesma maneira que o sítio eletrônico estatal deve demonstrar como foi realizado o tratamento de dados pessoais do seu cidadão.

Aliás, para Bitencourt e Tavares (2022), a transparência por parte do poder público é a disposição do acesso na informação, mas não só, como também ordenar os dados para que estejam organizados e por consequência haja, por exemplo a avaliação, acompanhamento e fiscalização das políticas que o Estado implemente, a fim de atender as necessidades de seus cidadãos na forma dos direitos fundamentais estampados na CF.

Ademais, pelo que foi visto supra acerca do princípio da transparência, a comunicação tem que ser passível de compreensão ao usuário para que tenha consciência de como estão sendo utilizados seus dados pelo ente governamental, inclusive, a fim de que os direitos das pessoas naturais e jurídicas sejam cumpridos com êxito, senão de nada adiantaria fornecer as informações pertinentes ao titular. Além disso, a conversa entre a administração pública e o cidadão ou pessoas jurídicas, ocorreria por meio do controlador e encarregado, sendo o último indicado pelo poder público, consoante Artigo 41, da LGPD (BRASIL, 2018) e Limberger (2022).

Insta salientar ainda que como a pessoa jurídica de direito público deve respeitar os princípios do Artigo 6° e incisos, da LGPD (BRASIL, 2018), de acordo com Cotta e Pinheiro (2022), o tratamento de dados nesse viés seria igual ao das pessoas físicas e pessoas jurídicas de direito privado.

Em conformidade com as diretrizes, de acordo com Guidi (2021) para o tratamento deve ter uma base legal, ou seja, algum motivo autorizado por lei para que possa acontecer, desde que com finalidade específica e com o procedimento

correto. A tamanha publicidade dos dados de determinada pessoa também não retira a necessidade da lisura procedimental, não deixando de ser dado pessoal.

Ainda, há de se falar que a administração pública possui a limitação de cessão e comunicação dos dados pessoais que detenha, pois somente pode fazê-lo contanto que respeite a finalidade para a qual existiu a coleta e o interesse da coletividade, sendo esta última atrelada nas funções comuns do Estado para satisfação das necessidades dos cidadãos que estão positivadas como direitos fundamentais na Constituição, de acordo com Limberger (2022). Ademais, a finalidade pública deve ser obedecida também pelos sujeitos privados, haja vista que por vezes integram o Estado, auxiliando em suas tarefas.

Logo, em seguida será tratado acerca da competência legislativa para regular a matéria de proteção de dados e sobre a Autoridade Nacional de Proteção de Dados (ANPD).

3.3 A competência legislativa em matéria de proteção de dados e a autoridade nacional de proteção de dados

A competência legislativa passou a ser privativa da União no caso da proteção e tratamento de dados pessoais, considerando o Artigo 22, inciso XXX, da Constituição Federal (BRASIL, 1988), enquanto que a competência administrativa quanto a Autoridade Nacional de Proteção de Dados (ANPD) também é da União, conforme Artigo 21, inciso XXVI, da Constituição Federal (BRASIL, 1988), em virtude do advento da Emenda Constitucional n.° 115 de 2022 (BRASIL, 1988), conforme esclarecem Tavares, Bitencourt e Cristóvam (2022).

Não obstante, cabe mencionar quanto a sua estrutura que o Conselho Diretor é o principal órgão dentro da ANPD, tendo 5 integrantes, dentre os quais o presidente é quem escolhe, dependendo da aprovação do Senado. Assim, a Autoridade Nacional de Proteção de Dados é denominada como órgão da administração pública de âmbito federal, fazendo parte também do poder executivo da União, podendo ser caracterizada de modo mais específico pelo Artigo 55-J, incisos, da LGPD (BRASIL, 2018).

Ademais, possível conceituá-lo também, conforme o Artigo 5°, Inciso XIX, da LGPD (BRASIL, 2018), como ramificação governamental, ou seja, um ente estatal e

com incumbências de garantir, executar e cuidar para que a norma seja devidamente obedecida.

Além disso, o Artigo 55-A, da LGPD (BRASIL, 2018), dispõe que a ANPD está em subordinação da pessoa que possui a incumbência como chefe de governo e de Estado no presidencialismo brasileiro, tendo a possibilidade de se tornar integrante da administração pública federal indireta, momento o qual estaria sob o regramento que as autarquias especiais devem cumprir.

Em relação às suas funções, segundo Calsing (2019), tem funções consultivas, como é o caso de fazer os princípios para a chamada Política Nacional de Proteção de Dados Pessoais e da Privacidade, estabelecer maneiras para divulgação dos tratamentos, confecção de normas e ritos, exposição dos possíveis resultados maléficos quanto aos tratamentos de dados com elevado grau de periculosidade, bem como regras, diretrizes e ritos simples e específicos para os diferentes tipos de estabelecimentos existentes com base em suas particularidades.

Não obstante, Monteiro (2020) explica as demais funções como a de supervisão, fiscalizando se a LGPD está sendo cumprida e até cabendo a ela aplicar sanções por eventuais descumprimentos, mediante processo administrativo que o acusado possui direito ao contraditório, ampla defesa e ao recurso da decisão que virá a surgir. No entanto, nas penalidades contra pessoas jurídicas de direito privado deve ser respeitada ideia da intervenção mínima, a qual será respeitada a livre iniciativa da atividade econômica com pouca intervenção estatal.

Diante disso, também cabe a ela receber avisos de acidentes de segurança por parte de quem tenha atribuição de operador, desde que envolva a possibilidade de resultado danoso ou de efetivo prejuízo a determinada pessoa titular de dados. Deve ser enfatizado ainda que a comunicação deve conter os acontecimentos ocorridos, conhecimentos daquelas pessoas titulares de dados que sofreram prejuízos, adversidades que ainda possam ocorrer e tudo o que será realizado para que o estado anterior ao dano seja reestabelecido.

Ainda, resta mencionar a função de promoção ou aperfeiçoamento, o qual a ANPD teria um papel de disseminador das informações pertinentes ao tratamento de dados para que todos soubessem como deve ser feito o procedimento correto, sendo mais preferível do que os poderes consultivos e punitivos que detém. Afinal,

trata-se de matéria inovadora que necessita da adaptação de todos e é esperada uma maior dificuldade para que a sociedade se inteire do assunto.

Outrossim, consoante Limberger (2022), há de se falar na responsabilidade para tratar acerca da publicidade de tratamentos de dados pessoais que o poder público por ventura faça na forma de suas pessoas jurídicas de direito público, exceto os segredos industrial e comercial, conforme Art. 55, J, X, da LGPD (BRASIL, 2018). No entanto, a exceção aos segredos industrial e comercial não podem ser subterfúgios para violarem os princípios da Constituição, no que tange a publicidade e transparência.

Em suma, Barbosa e Valle (2023) corroboram definindo a Autoridade Nacional de Proteção de Dados como integrante do poder executivo federal, sendo órgão junto da presidência da República, cabendo na prática da LGPD (BRASIL, 2018) realizar a execução do que consta na norma e fiscalização do cumprimento por quem está obrigado, bem como da conformidade perante a lei. Além disso, deve disciplinar e monitorar os tratamentos de dados que acontecerem, por fim, quando necessário realizar as sanções em virtude de desobediência da legislação.

Assim, será tratado em diante sobre óbices de compatibilidade da proteção de dados com a Lei de Acesso à Informação, visto que LGPD (BRASIL, 2018) e LAI (BRASIL, 2011) tratam de propostas diferentes, sendo uma, a privacidade e a última, o compartilhamento.

3.4 Os desafios da compatibilidade de proteção de dados com a Lei de Acesso à Informação

A Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2018) e a Lei de Acesso à Informação (BRASIL, 2011) tratam sobre dados de pessoas físicas e jurídicas, porém a primeira se refere ao tratamento dessas informações propriamente ditas no que tange a um resguardo e a outra se refere ao direito de obtê-las em caráter público, visando a informação. Assim, será tratado dos óbices para convergirem, tendo em vista a aparente contradição entre ambas, bem como a regra geral ser a publicidade e não o sigilo ou a restrição a determinados dados custodiados ou produzidos pelo Estado, a fim de manter um Estado Democrático de Direito, de acordo com Cotta e Pinheiro (2022).

Inicialmente, deve ser enfatizado que a LGPD (BRASIL, 2018) e a LAI (BRASIL, 2011), ambas possuem aplicação igualitária, sendo a LAI em todos os entes federados no que tange os Municípios, Estados, Distrito Federal e União, conforme Bitencourt, Cristóvam e Tavares (2022). Enquanto que, de acordo com Siderly e Tania (2022), a LGPD é norma nacional aplicável para todos os entes federativos do país, conforme Artigo 1°, Parágrafo Único, da LGPD (BRASIL, 2018), ou seja, igualmente a União, Estados, Distrito Federal e Municípios.

Primeiramente, Limberger (2022) menciona que a própria lei brasileira de proteção de dados aborda no seu Art. 23, Caput, da LGPD (BRASIL, 2018), a compatibilidade entre os institutos, contanto que haja uma interpretação sistemática, integrando direitos aos usuários do serviço público e o tratamento de dados pessoais dos destinatários por parte da administração pública. Por exemplo, é o caso dos gastos com os servidores públicos, o qual o Estado é obrigado a divulgar, sendo que aparecem também os dados pessoais de desconto para o adimplemento de pensão alimentícia e, inclusive, em relação ao plano médico que o indivíduo possui.

Além disso, consoante Limberger (2022), inclusive o Supremo Tribunal Federal na ADPF n° 690/DF e ADI n° 6.387, reconheceu que o direito da transparência e proteção de dados são compatíveis, ou seja, podem ter proteção da Constituição em nível equivalente mediante interpretação sistemática.

Ademais, conforme a Câmara dos Deputados (2021), as ideias de cada uma das leis, ou seja, privacidade e transparência, ambas são compatíveis no sentido de buscar os valores propostos pela Constituição brasileira, no que tange aos direitos de informação e proteção dos dados pessoais, bem como do princípio da publicidade, de acordo com Wimmer. Não obstante, há o enunciado n° 4 da Controladoria Geral da União (BRASIL, 2022) que reforça a possibilidade de integração entre as normas, visto a interpretação entre os regulamentos ser possível, bem como resguardam direitos fundamentais coadunáveis.

Apesar disso, de acordo com Bioni, Silva e Martins (2022) um dos óbices é a falta de clareza de ambas as leis, uma vez que ainda resta opaca a solução para o debate. Assim, resta enfrentar a deficiente literalidade dos textos e as alternativas jurídicas, os quais não apresentam de modo claro como deveria ocorrer o procedimento estudado, bem como o fenômeno de tornar os dados anônimos

realizado pelo Estado e as descrições dos possíveis prejuízos para a proteção de dados pessoais em momento anterior.

Além disso, Carvalho e Rosa (2023) acreditam na interpretação sistemática do ordenamento jurídico pátrio a ser realizada a cada caso a ser verificado pelos aplicadores da lei, o que é um desafio para verificar o que prevalecerá, se o acesso da informação ou a proteção de dados, pois inclusive há intimidade e privacidade que por vezes não podem ser difundidas ao conhecimento público, sob pena de repercussões mais prejudiciais.

Enquanto que, Guichot (2005) menciona as limitações para a compatibilidade da proteção de dados e o acesso das informações, visto que dados poderiam ter seus acessos restringidos, bem como o uso deles, além de a visualização poder ocorrer por meio do cumprimento de determinadas condições impostas ou, ainda, a restrição ao formato do documento não sendo digital.

Ademais, o Regulamento Geral de Proteção de Dados (UNIÃO EUROPEIA, 2016), estabelece na sua norma a capacidade de interação, uma vez que deve ser feita a análise da viabilidade do dado e da maneira de sua divulgação, bem como qual é a informação envolvida e se o titular de dados possui a escolha de não aceitar, além da observância das diretrizes de finalidade e legitimidade.

Enquanto que para Mañas (2016), o dado pessoal mesmo que tenha característica pública, ainda assim deve ter resguardada a condição do titular de dados. Portanto, um não exclui o outro, havendo uma adição.

Já para Cristóvam e Hahn (2020) ao Estado é imposto ser transparente, todavia a ele é proibido ofender o direito da privacidade que os titulares dos dados detenham, como é o caso da divulgação de seus dados pessoais.

Ainda, Rodrigues (2020) apresenta a transparência condicionada, através de sua classificação, recebendo os dados pessoais esse tipo de tratamento, visto que tanto o acesso como o tratamento devem ser restritos ao conhecimento público em relação a eles. Portanto, no momento em que o poder público fornecer documentos com informações pessoais sensíveis, elas devem ter tarjas encobrindo seu conteúdo.

Além disso, de acordo com o Artigo 7°, §3°, da LAI (BRASIL, 2011), existem também os documentos preparatórios, caso de transparência condicionada, os quais possuem restrições no conhecimento de seu conteúdo quanto ao embasamento de

determinados atos decisórios por parte do poder público. No entanto, o acesso não é proibido e sim, a disponibilização é discricionária quando ocorre antes do ato.

Ademais, em relação a outros exemplo de publicidade com o contraste da proteção de dados, Bitencourt, Cristóvam e Tavares (2022), mencionam da arrecadação dos entes federativos relativos aos tributos, como consta no Artigo 162, Parágrafo Único, da CF (BRASIL, 1988), bem como dos dados orçamentários, contábeis e fiscais que os entes federativos devem fornecer acesso no âmbito digital de forma a abranger todas as pessoas e sem requisição necessária, conforme Artigo 163-A, da CF (BRASIL, 1988).

Não obstante, a LAI possui exceções à transparência, tendo que haver a proteção aos dados, sendo eles de acordo com Cotta e Pinheiro (2022), as informações sob resguardo legal, como motivo bancário, fiscal, dentre outros, em conformidade com o Art. 22 (BRASIL, 2011); informações submetidas à classificação, pelo que consta no Artigo 23 (BRASIL, 2011); informações referentes aos indivíduos, no Artigo 31 (BRASIL, 2011); e documentos que subsidiam atitudes do poder público, bem como as suas deliberações, como contido no Artigo 7°, §3° (BRASIL, 2011). Assim, aquele dado não poderia ser disponibilizado de forma íntegra, somente parcialmente com respeito à exceção que estivesse presente com o documento contendo tarja ou outro separado, conforme a Controladoria-Geral da União (2019).

Entretanto, um dos óbices, sendo utilizado o exemplo de Cotta e Pinheiro (2022), é o caso da Corregedoria-Geral da União em que órgãos e suas unidades recusaram requisições para compartilhamento de dados pessoais em investigações e processos acusatórios disciplinares, utilizando como base a LGPD. No entanto, as disposições da LGPD devem ser vistas de forma concomitante com a LAI, no caso de compartilhamento de dados, visto que a LGPD seria legislação procedimental.

Além disso, a interpretação mencionada provocaria uma morosidade maior ao acesso da informação pública que é um dos direitos fundamentais estipulados no Artigo 5°, inciso XXXIII, da Constituição Federal, o qual por sua vez prejudicaria também eventual cumprimento do princípio macro da Carta Magna brasileira no que tange à dignidade humana, bem como o direito da informação, sem falar nos danos advindos pela demora em que várias situações requereriam uma maior celeridade.

Diante disso, após a análise de compatibilidade da LAI quanto a proteção de dados pessoais, será tratado acerca de interoperabilidade e compartilhamento de dados no Brasil, visto ser instituto que envolve tanto a LGPD como a LAI e devido sua importância na democracia com os dados públicos.

4 INTEROPERABILIDADE E COMPARTILHAMENTO DE DADOS NO BRASIL: LIMITES E POSSIBILIDADES

Diante da democracia com uma proposição de participação dos cidadãos nas decisões da administração pública, houve a implementação da governança pública digital. Portanto, o intuito é ofertar instrumentos tecnológicos às pessoas para que consigam ter informações acerca da gestão do Estado, assim fiscalizando, pois também possuem mais acessibilidade para fazê-lo. No entanto, a interoperabilidade, de acordo com Tavares, Bitencourt e Cristóvam (2022), sendo como instrumento que possibilita a interação de dados em diferentes sistemas de variados entes públicos, esferas de poder, bem como pela sociedade e o compartilhamento de dados são necessários, devendo ter tratamento específico, a ser verificado em quais situações cabem ou não. Assim, será comentado das suas definições, benefícios, possibilidades de aplicação ou não, desafios e a relevância para a pessoa jurídica de direito público nos seus serviços em prol do interesse público.

4.1 GOVERNANÇA PÚBLICA DIGITAL: desafios ao tratamento de dados na era digital

Iniciativa que visa melhorar os serviços da administração pública por meio das tecnologias, com contato mais próximo do cidadão por meio do acesso dessas ferramentas. Assim, em decorrência disso existem os desafios pertinentes ao assunto que serão abordados.

Primeiramente, de acordo com Bitencourt, Cristóvam e Tavares (2022), insta salientar a mudança cultural no Estado em virtude do modelo burocrático que era mais hierarquizado e adotado para outro gerencial que fosse capaz de cumprir com os direitos sociais elencados na Constituição Federal de 1988 (BRASIL, 1988), bem como da transparência dos atos públicos e culpabilização de autoridades com caráter público. Assim, a transição começou a ocorrer em 1995 com o Plano Diretor da Reforma do Aparelho do Estado e a Emenda Constitucional n.° 19/1998 (BRASIL, 1998), onde surgiu o conceito de Governança Pública. Enquanto que surgiram novas ferramentas digitais que proporcionam informação e comunicação, tendo evoluído o fenômeno para a Governança Pública Digital com o uso desses equipamentos

virtuais para a publicidade. Entretanto, ainda é remanescente a forma antiga, não estando implementada e devidamente consolidada a ruptura que foi proposta, restando a dificuldade de ainda impulsionar os cidadãos e demais interessados para debate e deliberação.

Enquanto que para Lima e Silva (2022), um grande desafio consiste na tentativa de lidar com as incertezas provocadas pelo fornecimento de serviços públicos no meio virtual, como é o caso da proteção de dados dos cidadãos, a ser realizado pela administração pública, bem como providenciar o acesso aos requerentes ou até mesmo sem a requisição.

Ademais, Flôres e Silva (2020), mencionam a inexistência de normas suficientes para o resguardo dos dados das pessoas, não tendo a Lei 12.965/14 (BRASIL, 2014) essa capacidade, bem como quando a administração pública os detém. Portanto, se torna de tamanha importância a criação de nova norma que trate mais a fundo da temática e até mesmo daqueles considerados como sensíveis, senão a proteção fica desestabilizada e, inclusive, a administração pública não consegue o amparo de forma integral. Assim, o Estado fica sujeito às apropriações dos elementos por parte de criminosos que em decorrência disso os divulgam, podendo gerar prejuízos aos titulares, principalmente quanto aos sensíveis que implicam em desigualdades no trato social perante o indivíduo, bem como a violação de direitos.

Ainda, Miguel (2019), complementa afirmando que a Autoridade Nacional de Proteção de Dados (ANPD), é encarregada para averiguar o tratamento de dados, bem como para punir em situações de violações. Porém, inicialmente suprimida na norma, tendo sido prevista em Medida Provisória e junto do poder executivo federal, bem como estruturada com integrantes escolhidos pelo presidente em função comissionada que podem ser mandados embora em virtude de ação investigativa de irregularidade disciplinar, iniciado pelo Ministro da Casa Civil de maior hierarquia do chefe de estado e chefe de governo (presidente), podendo ele ordenar o distanciamento prévio, logo a independência do instituto resta afetada, sendo mais uma das situações de insuficiência normativa.

Não obstante, Davies (2011) exemplifica com os dados governamentais abertos (DGA) e da exposição referente da condição de saúde dos cidadãos da Inglaterra, visto que viola o direito de vida particular, em virtude da exibição e

também há possibilidade de ocasionar suspeita das pessoas com a administração pública quanto esses elementos.

Entretanto, de acordo com Veloso (2012), nem todos cidadãos possuem acesso aos dados, visto que a maioria acaba por ser privilegiada, mas não a minoria que acaba desprovida das benesses. Portanto, isso causa uma maior desigualdade, haja vista que a parcela populacional dominante utiliza do procedimento para aumentar mais ainda seus ganhos financeiros. Assim, possível dificuldade a ser posta é da disponibilização integral da governança pública digital a todos e das vantagens em decorrência disso, sem diferenciações em virtude de quaisquer características diversas que possuam.

Outrossim, Martano (2018) também contribui que a coletividade como um todo não tem a possibilidade de deter esses elementos, como é o caso dos dados governamentais abertos (DGA), seja em virtude do óbice por parte do formato virtual, ter internet disponível para uso, bem como a compreensão e exame. Entretanto, as DGAs podem conter vontades de diferentes grupos que são diferentes umas das outras e deliberações que envolvem determinada classe em detrimento das demais. Assim, dependendo da situação existem ações que estimulam os dados abertos da administração pública para o desenvolvimento econômico das empresas, invés de toda a sociedade ter as mesmas condições.

Não obstante, conforme a CGI.br (2023) com seus indicadores de pesquisa apresentados na “TIC Domicílios 2023”, dentre 23.975 moradias participantes do estudo, apesar de um crescimento entre 2015 a 2023, somente 84% delas possuíam a rede mundial de computadores disponível para uso no ano passado. Outrossim, tiveram 21.271 pessoas que aderiram aos questionamentos realizados, tendo também um crescimento de 2015 a 2023, mas que 84% dos indivíduos a utilizaram nos três meses anteriores da indagação. No entanto, a defasagem se encontra para aqueles de classes com menor condição econômica, raças de origem africana e com baixa instrução, sendo pelo menos alguns dos mais prejudicados. Contudo, possível concluir pelas amostragens que as minorias sociais citadas estão desfavorecidas, o que sem sombra de dúvidas torna-se óbice, uma vez que o suporte estatal deve ser para todos.

Ademais, de acordo com Silva e Takano (2020), outro empecilho são as mudanças da rede mundial de computadores e das Tecnologias de Informação e

Comunicação (TIC), as quais a comunidade não possui capacidade para estar em consonância, restando também uma defasagem normativa em sua regulação. Além disso, também é possível falar dos ajustes realizados frente das incertezas provocadas pela inserção de afazeres fornecidos pela administração pública em meio digital.

Ademais, de acordo com Bitencourt, Cristóvam e Tavares (2022), os municípios, por exemplo, quando requeridos para a abertura dos dados, eles recusam com o argumento de que não há previsão por meio de lei para que tenham de fazê-lo, visto que a Lei 14.129/2021 no Artigo 2°, inciso III, desobrigou tanto os municípios como os estados na aplicação da norma. Assim, esses entes orientam para que seja feito o pedido através do portal de transparência com o uso de filtros e seleções, causando uma demora desnecessária no procedimento e descaracterizando os dados abertos que deixam de sê-lo por perderem sua abrangência. Não obstante, a negativa ocorre também devido ao Artigo 13, do Decreto 7.724/2012 (BRASIL, 2012), sob o argumento de que é pedido não específico, com falta de proporção ou não razoável, bem como incumbência de procedimento extra no estudo, raciocínio ou junção de dados. Entretanto, os municípios se recusam de forma errônea, visto que a obrigação surge nos Artigos 7, 10 e 11, da Lei de Acesso à Informação (BRASIL, 2011), a qual responsabiliza todos os entes federativos e que a Lei de Governo Digital não impede as criações das plataformas que são encargos da administração pública como um todo.

Além disso, a Infraestrutura Nacional de Dados Abertos (INDA) foi criada em 12 de abril de 2012 quando a Instrução Normativa n.° 4 (BRASIL, 2012), teve sua publicação, tendo sido implementado o significado dos dados abertos. Todavia, eles ainda não foram definidos em sua integralidade, deixando espaço para ações de governo aberto que são erradas, como é o caso, por exemplo a exportação dos dados de teor público que apresentam óbice em decorrência da utilização de escolha dos filtros de pesquisa, impossibilitando a visualização de uma só vez em sua integralidade, de acordo com Bitencourt, Cristóvam e Tavares (2022).

Não obstante, Pérez Luño (2005) entende que em relação ao assunto, os direitos positivados na Constituição e defensores da personalidade devem ser pensados em conjunto, apesar é claro, da complexidade envolvida por causa do natural envolvimento do titular de dados em várias frentes. Assim, defende a

exposição da vontade de disposição dos dados por parte das pessoas e que este seja integrado no rol dos direitos fundamentais de forma ampla, tamanha sua importância, apesar das dificuldades que possam advir.

Além disso, há o óbice para que a atuação participativa dos cidadãos seja mantida na administração pública, visto que os dados abertos ou também chamados como abertura de dados, viabilizam o acesso tanto para pessoa de dentro da pessoa jurídica de direito público como as de fora. Portanto, haveria um empecilho para o direito fundamental à informação.

Ainda, o Manual de Gestão de Interoperabilidade confeccionado pelo Ministério do ano de 2012 (gov.br ePING, 2012), cita as dificuldades quanto ao aumento da taxa de êxito dos resultados propostos pelo trabalho da administração pública e que os recursos sejam aproveitados da melhor maneira possível com o máximo de benefícios.

4.2 A RELEVÂNCIA DOS SISTEMAS DE INFORMAÇÕES GOVERNAMENTAIS e compartilhamento de dado para o tema das políticas públicas, serviços públicos e controle da administração pública

Primeiramente, conforme Veloso (2012), as tecnologias de modo geral podem ser conceituadas como criações antes inexistentes e inventadas pelas próprias pessoas, visando ampliar as próprias capacidades, facilitar os afazeres e resultar em uma rotina mais aprazível. Logo, por os sistemas de informações governamentais serem um exemplo do assunto aqui tratado, apresentam grande valia na garantia de direitos fundamentais e inclusive do princípio macro da dignidade humana positivada na Constituição, visto que necessariamente também buscam agregar valor aos seus usuários por meio da satisfação de suas necessidades.

Outrossim, Silva e Lima (2022) comentam também que as transferências informacionais ficaram mais velozes, funcionando a rede mundial de computadores como uma ferramenta à serviços dos usuários.

Ainda, os sistemas de informações governamentais são importantes, como é o caso dos dados abertos que podem ser definidos de acordo com Bitencourt, Cristóvam e Tavares (2022), pelo que é abordado no Artigo 4°, inciso IV, da Lei 14.129/2021 (BRASIL, 2021), como os dados que os cidadãos tenham possibilidade

de acesso, que estejam digitalizados, em formato sem restrições para a visualização, com capacidade de processamento por máquina, bem como com referência na rede e que seja fornecido com licença livre, sendo possível tanto o uso como o tratamento de dados para qualquer pessoa física ou jurídica que fizer questão.

Enquanto que, de acordo com o Open Knowledge International (2015), os primórdios de seu sentido remontam ao The Open Definition que foi criado em 2005, sendo dados abertos aqueles sem restrições de utilização, alteração e transferidos a outrem independente do intuito. Porém, Lathrop e Ruma (2010), ressaltam que quando sejam advindos da administração pública, são chamados de Dados Governamentais Abertos.

Assim, os dados abertos quando existentes, segundo Bitencourt, Cristóvam e Tavares (2022), possibilitam a reutilização de dados para a ciência, comércio, exercício da cidadania e controle social. Portanto, relevantes para os serviços públicos, controle social e políticas públicas, na medida em que esses dados podem servir na averiguação das despesas estatais, onde o dinheiro dos cidadãos são depositados por meio de tributos, bem como quanto a fase de avaliar as políticas públicas elaboradas, visto que as amostras são necessárias para essa finalidade.

Além disso, Silva e Takano (2020) acrescentam acerca do aspecto social, mencionando quanto ao acesso facilitado de informações, estas que antes eram de acesso mais dificultoso em virtude do formato físico e não digital, bem como da autonomia das pessoas e maior adesão aos grupos de indivíduos que resguardam objetivos políticos e sociais. Quanto a administração por parte do governo, ela passa por modificações benéficas, sendo nas áreas regional e internacional. Já as entidades se tornaram mais independentes na gestão das suas atividades e também em alastrar os seus negócios.

Enquanto que, conforme Cotta e Pinheiro (2022), em relação ao compartilhamento de dados entre órgãos, é uma boa solução para a corrupção que vem sendo bem recorrente no país pelos últimos anos haja vista que os delinquentes atuam de forma conjunta e complexa que atenta para a prevenção, detecção, bem como para adquirir provas contra os autores do fato e realização da punição das infrações. Ademais, as unidades correicionais também necessitam dessa divulgação, em virtude da apuração de atividades infracionais em busca de informações e

documentos, sendo que na falta deles ou na respectiva demora, há a prescrição punitiva estatal e a consequente impunidade que não repele com que eventuais criminosos cometam os crimes novamente.

Ademais, a se tratar do compartilhamento restrito de dados para a finalidade das políticas públicas, conforme o Artigo 4°, inciso II, Decreto n.° 10.046/19 (BRASIL, 2019), é esclarecido que dados sigilosos podem ser passados para a administração pública com esse fim. Além disso, Tavares e Bitencourt (2022) explicam que essa capacidade de alcance dos dados para a administração pública e dentro dela é importante a cada etapa das políticas públicas, haja vista que pode ser realizado um planejamento que durará até a avaliação das ações da pessoa jurídica de direito público. Inclusive, a interoperabilidade entre bancos de dados da administração pública é relevante para na análise de diferentes áreas públicas verificar e decidir da melhor maneira possível quanto às políticas públicas. Portanto, simplifica a coleta dos dados, não tendo que repeti-la e tendo melhores ideias de como proceder para o gasto das verbas públicas nesse ramo.

O compartilhamento de dados também pode ocorrer por meio dos APIs que possibilitam com que informações de diferentes sistemas sejam integrados ou compartilhados, a fim de cumprir determinado objetivo, de acordo com Tavares e Bitencourt (2022). Assim, os dados ali depositados são mais visíveis e pode ser feito o cruzamento deles com outras bases de dados, o que facilita o serviço público.

Não obstante, de acordo com o Comitê Central de Governança de Dados (CCGD, 2020), o fenômeno proporciona evolução nos trabalhos executados pelo Estado para a sociedade, dentre eles: menos ônus financeiro e necessidade de dedicação pra recolher todas as informações importantes quanto a administração estatal, visto que todos os entes poderiam ver aquelas que estariam disponíveis, tornando mais simples reconsiderar procedimentos e utilizar novamente o que está ali disposto; mais qualificação dos elementos, tendo em vista que passa a existir menos rigor em prol dessa transferência entre entes, proporcionando o acesso quanto a elementos probos, verídicos, estabelecidos e apropriados, o que implica em recolhimentos benéficos com cumprimento de posturas adequadas e tratamento, bem como no que tange na formulação e conservação; incremento na lisura em prol dos usuários, informando da maneira pela qual ocorre a manutenção e transferência pelos entes estatais, bem como há o surgimento de princípios que regem como deve

ser feito o procedimento, assim é impositivo que os integrantes ajam em consonância com determinadas ações que são as mais resguardadas e das atitudes para cumprir as necessidades dos cidadãos; melhoria em como é feita a deliberação nas diferentes categorias estatais, a fim de ter avanços aos trabalhos prestados da administração pública pras pessoas, porque há mais disponibilidade, celeridade e segurança para adquirir e disponibilizar os elementos, sendo necessário para padrão de administração que delibera segundo fatos comprovados, além disso proporciona o potencial para resolver imbróglios trazidos pelos brasileiros, novas ideias para ações estatais, tornar possíveis a fiscalização, vistoria e a classificação de planos da administração pública, promover diligências recentes e demais melhorias.

4.3 A INTEROPERABILIDADE NO SETOR PÚBLICO BRASILEIRO: possíveis benefícios

Serão abordados eventuais benefícios oriundos da interoperabilidade de informações no setor público brasileiro, haja vista a importância do assunto por envolver a participação da sociedade na administração pública. Ademais, insta definir que o conceito do fenômeno, de acordo com Tavares e Bitencourt (2022, p. 149), é o uso dos dados em tecnologias de variados entes da administração pública. Portanto, colaboram entre si no fornecimento para eventuais necessidades.

Assim, há de se destacar, conforme Lima e Silva (2022), que a interação em diversos softwares se configura como o mínimo da satisfação de socialização que os indivíduos apresentam, inserindo as pessoas na sociedade de forma excepcional a partir do momento em que todos estão unidos uns aos outros. Portanto, possível concluir que proporciona o controle social, ocorrendo a efetivação da democracia que gera também o cumprimento dos direitos fundamentais e a dignidade humana, princípio macro da Carta Magna brasileira.

Ainda, evita de ocorrer a duplicidade de informações e a perda da integridade dos serviços digitais, caso o procedimento recomendado do Padrão de Interoperabilidade em Governo Eletrônico (e-Ping) seja aplicado pelos responsáveis, conforme Oliveira (2017).

Quanto ao que trata a própria lei acerca dos pontos positivos, há o Artigo 39, Caput e incisos, da Lei do Governo Digital (BRASIL, 2021). Assim, mencionam

das políticas públicas serem mais bem utilizadas, os perfis de cadastro da administração pública terem uma fidúcia maior, vias unificadas que são mais fáceis para identificação de determinada pessoa no serviço público, troca de dados facilitada entre diferentes órgãos do Estado e por CPF o tratamento de informações das bases de dados.

Portanto, por exemplo, conforme Tavares e Bitencourt (2022) nas políticas públicas os dados são compartilhados e são mais fáceis de serem acessados, ocorrendo a diminuição do tempo e custo financeiro para ser feita a pesquisa necessária na futura aplicação das medidas. Por fim, existem diversos dados para serem analisados em conjunto, a fim de verificar eventual efetividade e poder intervir para atingir o objetivo por meio da correção de erros obtidos.

Além disso, Bitencourt, Cristóvam e Tavares (2022) mencionam que no Artigo 24, inciso V, da Lei 12.965/2014 (BRASIL, 2014), há a positivação da possibilidade de troca dos dados entre programas diferentes, bem como com os entes federativos diversos e as categorias da comunidade existentes.

4.4 Limites e possibilidades do compartilhamento e interoperabilidade a partir da legislação, doutrina e jurisprudência

Será analisado quanto ao compartilhamento e interoperabilidade dos dados em relação aos seus limites e possibilidades pelo ordenamento jurídico, estudiosos do Direito e decisões judiciais.

Primeiramente, de acordo com Castro e Lovato (2020), a partilha pode acontecer com a anuência do titular e desde que tenha objetivo para atendimento de interesse público, bem como não necessita da concordância quando sejam requeridos em razão de implementação das políticas públicas positivadas em normas ou pactos.

Assim, há de se destacar que, conforme o Artigo 26, Caput, da LGPD (BRASIL, 2018) estabelece que o compartilhamento de dados dos órgãos e entes da administração pública deve ter como finalidade obedecer a implementação de políticas públicas, bem como aquilo disposto por meio de lei e os princípios de tratamento elencados pela LGPD no Artigo 6°. Portanto, a finalidade de atender os direitos fundamentais da sociedade prevalece.

Outra hipótese é a disposta no Artigo 26, §1° e incisos, da LGPD (BRASIL, 2018) que a administração pública pode compartilhar as informações que utiliza com finalidade pública para o âmbito privado, desde que o faça, a fim de descentralizar o seu serviço, dados sejam públicos, em caso de previsão por lei, pra prevenir fraudes ou irregularidades, segurança ou ainda na proteção ao titular, conforme Ruth e Tarcisio (p. 179 – 180, 2022). Aliás, cabe ressaltar que para Cotta e Pinheiro (2022), também caberia a possibilidade mencionada no caso de reprimir ou evitar com que o Estado seja prejudicado.

Além disso, de acordo com Bitencourt, Cristóvam e Tavares (2022), a Lei n.° 12.965/2014 ou chamada de Marco Civil da Internet, aborda sobre a interoperabilidade no Artigo 24 (BRASIL, 2014), em que possibilita que ocorra entre programas diferentes, bem como nos entes da federação brasileira e categorias da comunidade.

Ademais, o Artigo 3°, Inciso V, do Decreto n.° 8.777 (BRASIL, 2016), menciona da interoperabilidade entre diferentes plataformas que armazenam os dados primários, ou seja, aqueles tirados do local em que foram originados, contendo o máximo de especificidade e sem intervenção, explicação do Artigo 4°, Inciso IX, da Lei 12.527/2011 (BRASIL, 2011).

Não obstante, a Lei de Acesso à Informação (BRASIL, 2011) apresenta períodos definidos em que determinada informação pública não será acessível em virtude da segurança para a sociedade e ao Estado, conforme Artigo 23, Caput e incisos, da LAI (BRASIL, 2011). Então, de acordo com os prazos definidos no Artigo 24, §1° e incisos, da LAI (BRASIL, 2011), o dado classificado como ultrassecreto teria prazo máximo de resguardo no que tange a 25 anos, a secreta 15 anos e a reservada 5 anos. Por fim, os dados pessoais são visados pela LAI (BRASIL, 2011), por mais que a LGPD (BRASIL, 2018) seja a principal lei para eles, assim definindo no Artigo 31, §1°, inciso I, da LAI (BRASIL, 2011), restrição de acesso por 100 anos.

Entretanto, Oliveira (2017, p. 10) diz que os padrões recomendados para a interoperabilidade no que tange ao e-PING são difíceis de serem seguidos devido a poucos integrantes de determinado ente para o cumprimento tanto de exigência dos usuários como da administração pública a nível federal, bem como da rotatividade dos membros e dificuldade na adição para determinadas atividades. Além disso, a falta de capacidade para realização de um plano de Tecnologia da Informação que

seja assertivo e bem delimitado. E ainda, a própria diretriz não aborda acerca da prática de como realizá-la, o que por sua vez faz com que a administração pública haja da forma que melhor lhe aprouver e nem sempre é a maneira correta.

Não obstante, o Artigo 38, Caput e incisos, da Lei do Governo Digital (BRASIL, 2021), menciona que as restrições legais devem ser observadas, requisitos da segurança da informação e comunicações, capacidade tecnológica e rentabilidade da interoperabilidade. Ademais, o aproveitamento de condições favoráveis quanto aos custos no acesso a dados e reaproveitamento da infraestrutura que foi investida, por fim a proteção dos dados pessoais.

Para os APIs explicitados anteriormente, nem sempre há acesso gratuito aos cidadãos perante bancos de dados públicos para eventuais consultas de que necessitem. Portanto, isso descumpre o direito fundamental ao acesso à informação e lesa principalmente os mais pobres que não possuem condições financeiras para alcançarem seu direito fundamental, sendo que o serviço sequer deveria ser pago.

Apesar das medidas mencionadas supra, deve ser levado em conta outro óbice, de acordo com Tavares e Bitencourt (2022) que são os documentos físicos ainda não digitalizados nos bancos de dados da administração pública. Assim, seria impossibilitado por ora que todos os dados fossem interoperáveis.

Não obstante, Silva e Lima (2022) exemplificam a uma maior cooperação entre os setores público e privado, sendo imperiosa que a interoperabilidade seja exitosa, como foi o caso do período de pandemia do Coronavírus em que foi implementado o auxílio emergencial com recebimento pelo Banco da Caixa. Porém, foram constatadas diversas dificuldades na execução, como é o caso do não recolhimento do benefício e quanto ao uso dos aparatos tecnológicos para o atingimento do objetivo em questão, sendo que: 12% dos indivíduos não lograram êxito na utilização do app da instituição bancária, 10% estava com falta de memória para ter o programa, 9% não possuía o conhecimento para incorporar o software no mobile e 9% com carência de rede. Ainda, referente ao desempenho da ferramenta, 73% pediram pela ajuda governamental que está pendente de ser aceita ou ainda está em verificação (PAINEL TIC COVID-19, 2021). Portanto, a interoperabilidade necessita de mais desenvolvimento, visto que ideias como a mencionada acima, pecam na sua implementação, o que não aconteceria caso houvesse uma cooperação entre diversos segmentos digitais.

Quanto a interoperabilidade, conforme o Gov.br (2020), foi regulamentada por meio dos Padrões de Interoperabilidade do Governo Eletrônico (E-PING) com a delimitação de regras para que possa ocorrer, estando os participantes do Sistema de Administração dos Recursos de Tecnologia da Informação (Sisp) subordinados no que estiver disposto.

Primeiramente, quanto a interação mediante transferência de dados, houve a criação do Decreto 8.789/2016 (BRASIL, 2016), o qual não está mais em vigor por causa do surgimento do Decreto 10.046/2019 (BRASIL, 2019). Diante disso, o novo regulamento arbitrou limites para a transferência de informações requeridas na implementação de ações estatais, como é o caso de estar sob a égide da LAI (BRASIL, 2011) e LGPD (BRASIL, 2018). Além disso, a coordenação e diretivas para a cooperação dos entes perante o Cadastro Base do Cidadão. Ainda, também quanto ao surgimento da figura do Comitê Central de Governança de Dados (CCGD) na função de, por exemplo, decidir, coordenar e fornecer instruções para formar os grupos referentes aos partilhamentos amplo, restrito e específico, bem como da sua divulgação com respeito ao resguardo de dados.

Ainda, quanto ao gestor de dados, conforme o Artigo 2°, inciso XIII, do Decreto 10.046/2019 (BRASIL, 2019) e o CCGD Comitê Central de Governança de Dados (2020), é definido como ente, ou seja, órgão ou entidade, com a incumbência de deliberar quanto aos dados envolvidos, realizando sua administração em diferentes aspectos, por exemplo, do compartilhamento de dados. Não obstante, dentre as suas responsabilidades, possível mencionar que deve divulgar internamente as normas e mandamentos a serem seguidos no assunto, bem como realizar as categorizações de dados na definição de dados tidos como de compartilhamento amplo, restrito e específico, enviando ao Comitê Central de Governança de Dados (CCGD) e também na definição para que os dados restritos e específicos possam ser transferidos, além de buscar saber como o Decreto 10.046/2019 (BRASIL, 2019) será executado em participação de eventos realizados pelo CCGD.

Portanto, em relação aos compartilhamentos amplo, restrito e específico, o de primeira espécie se refere aos dados sob gerência do Estado que não são submetidos a alguma confidencialidade e que o acesso deve ser livre, conforme o Artigo 4°, Inciso I, do Decreto 10.046/2019 (BRASIL, 2019). Quanto ao segundo, são

os com resguardo, sendo disponível para os entes que devem obediência à norma e quando façam a implementação de ações estatais, envolvendo também procedimentos estabelecidos por parte do CCGD, de acordo com o Artigo 4°, Inciso II, do Decreto 10.046/2019 (BRASIL, 2019). Por fim, o terceiro são os com restrição, mas que determinados componentes estatais podem ter ciência deles, podendo transferi-los em conformidade com requisitos elencados pelo gestor, em consonância com o Artigo 4°, Inciso III, do Decreto 10.046/2019 (BRASIL, 2019).

Enfim, foi realizada uma tabela com as possibilidades e limites da interoperabilidade e compartilhamento de dados, atribuídos pela legislação:

Limites e possibilidades do compartilhamento de dados.	Limites e possibilidades da interoperabilidade de dados.
Categoria ampla: Deve ser pelo mesmo meio utilizado para os dados abertos e transparência ativa, não necessitando de anuência anterior do gestor de dados, conforme Artigo 11, Caput, do Decreto 10.046/2019 (BRASIL, 2019) e o CCGD Comitê Central de Governança de Dados (2020).	Programa sem restrições para que a interoperabilidade possa ocorrer, por exemplo diferentes sistemas conseguirem se comunicar entre si, de acordo com o E-ping (BRASIL, 2018).
Categoria restrita: Impositivo respeito ao resguardo e segurança das informações envolvidas, pelo que estabelecido e proveniente do CCGD, bem como proibida a retransmissão ou partilhamento com outrem, amenos que o gestor de dados permitir de forma expressa quando der a anuência ou após, tendo em vista também as diretrizes do Artigo 5°, do Decreto 10.046/2019 (BRASIL, 2019), de acordo com Artigo 12, Caput, §1° e §4°, do Decreto 10.046/2019 (BRASIL, 2019) e CCGD Comitê Central de Governança de Dados (2020).	Primar pelos padrões abertos que propiciam a interoperabilidade, bem como não tenham custos aos usuários. Porém, não são exigidos caso ocorram de forma temporária, conforme E-ping (BRASIL, 2018).
Categoria específica: Necessária anuência do gestor de dados e satisfação dos	Prezar pela transparência de dados, em consonância com a Lei de Acesso à

quesitos estabelecidos pela autoridade para que o compartilhamento possa ocorrer, bem como proibida a retransmissão ou partilhamento com outrem, amenos que o gestor de dados permitir de forma expressa quando der a anuência ou após, conforme Artigo 14, Caput, Incisos I e II, §2°, do Decreto 10.046/2019 (BRASIL, 2019) e CCGD Comitê Central de Governança de Dados (2020).	Informação (BRASIL, 2011), pelo exposto no E-ping (BRASIL, 2018).
Independente da categoria de dados requeridos, o demandante deve arcar com o ônus financeiro e também prezar pela confidencialidade, pelo disposto no gov.br (2020).	Respeitar a segurança exigida pela interoperabilidade (BRASIL, 2018).
Não são exigidos pactos entre entes públicos, bem como demais instrumentos congêneres, de acordo com o Artigo 5°, Caput, do Decreto 10.046/2019 (BRASIL, 2019).	Utilizar adequações que estão amplamente em uso nas relações negociais, de acordo com E-ping (BRASIL, 2018).

5 CONCLUSÃO

Em suma, o primeiro capítulo do presente trabalho trata dos dados como direitos fundamentais, uma vez que há relação com a intimidade e vida privada, esses sim tipificados na Constituição Federal no rol de garantias consideradas fundamentais para os cidadãos. Ademais, garantem o direito de personalidade das pessoas para viverem sem influências externas que os impeçam de uma livre gerência de suas vidas, por meio dos direitos de intimidade e vida privada, por mais que na doutrina não exista um consenso entre a diferenciação ou não desses termos.

Ainda, quando os dados das pessoas não recebem tratamento adequado, o impacto é muito prejudicial aos titulares de dados como em jurisprudência do STF com uso para finalidade diversa da coleta, tendo os dados dos eleitores brasileiros sido usados para os créditos do Serasa por meio de acordo com Tribunal Superior Eleitoral (TSE). Outra situação foi a coleta de dados em rede social que era, a princípio, para um teste de personalidade parte de um estudo científico e acadêmico, mas foi utilizado para as eleições estadunidenses nas escolhas dos candidatos, afetando a democracia e a finalidade do tratamento de dados. Além disso, as eleições brasileiras de 2018 tiveram um impulsionamento de notícias falsas por meio de grandes investimentos financeiros, prejudicando o direito de informação e também o regime democrático adotado para optar por políticos de preferência do povo. Por fim, a Medida Provisória (MP) n.° 954/2020 foi julgada pelo STF pela suspensão liminar, visto o compartilhamento de dados dos clientes de linhas telefônicas que merecem proteção legal de privacidade e intimidade.

Por fim, quanto as normas interpretativas de dados, em 1766 os países escandinavos foram os pioneiros em informações públicas com a invenção de um comitê. Enquanto que em 1789 na Revolução Francesa houve a Declaração de Direito do Homem e do Cidadão com a possibilidade de pedir prestação de contas. Já em 1951 surgiu na Finlândia a segunda lei no assunto e em 1970 Noruega e Dinamarca elaboraram suas leis. Enquanto que quanto a proteção de dados pessoais, foi a Alemanha a precursora com a lei no Land de Hesse. Ademais, em 1978 a França inventou a Comissão Nacional para Proteção de Dados, sendo que fez a própria lei com inspiração na da União Europeia, tendo Portugal se inspirado

nela e o Reino Unido também elaborou sua própria norma. Afinal, em 2000 houve a Carta de Direitos Fundamentais da União Europeia e em 2018 o General Data Protection Regulation (GDPR) que inspirou a Lei Geral de Proteção de Dados (LGPD) do Brasil e do mundo.

No segundo capítulo, a Lei Geral de Proteção de Dados é abordada, sendo vigente para todo o país e seus entes federativos, inclusive as pessoas físicas e jurídicas de direito privado e público, com proteção de dados físicos e digitais. Além disso, incide em situações com modificação de dados e tratamento ocorrido no Brasil para ofertar ou providenciar bens. Ainda, adota o modelo ex ante com a proteção prévia dos dados pessoais de determinadas pessoas identificadas ou que possam ser identificadas, sendo necessário que o responsável pelo tratamento motive em um dos motivos justificáveis em lei. Enquanto que quanto aos dados protegidos, estão os meramente pessoais e os sensíveis, último termo o qual possui proteção maior pela legislação, visto tratar daquilo que quando exposto em público pode prejudicar de forma mais grave o titular dos dados e ocorrendo o seu tratamento por hipóteses mais rígidas.

Ademais, quanto aos deveres de proteção e tratamento dos dados pela administração pública e sujeitos privados, existem as instituições de ensino superior que são consideradas controladoras e possuem legítimo interesse no tratamento, realizando constante coleta de dados, assim necessitando de requisição expressa do interessado para portabilidade, estar conforme a lei e segredo industrial, bem como o comercial. Enquanto que o poder público detém a incumbência de tratamentos dos dados tanto na administração pública direta como na indireta, devendo publicizá-los. Contudo, ambas as instituições devem se pautar pelos princípios dos tratamentos de dados pessoais estabelecidos.

Ainda, sobre a competência legislativa em matéria de proteção de dados e a Autoridade Nacional de Proteção de Dados (ANPD), a União possui a competência privativa para legislar em proteção e tratamento de dados pessoais, bem como a administrativa quanto a ANPD. Ademais, a autoridade competente é órgão da administração pública federal, integrando o poder executivo da União, tendo funções consultivas como regulamentações e elaboração de relatórios, bem como de supervisão como fiscalização e sanções, além disso a de promoção ou

aperfeiçoamento como um disseminador de informações para o procedimento correto de proteção e tratamento de dados pessoais.

Por fim, quanto aos desafios da compatibilidade de proteção de dados com a Lei de Acesso à Informação, a LGPD protege os dados pessoais enquanto que a LAI busca a publicidade dos dados, tendo uma aparente contradição e as suas vigências se estendem igualmente por todo o território nacional e entes federativos. Assim, deve ser feita uma interpretação sistemática, visto que ambos os direitos são compatíveis, devendo ser averiguado qual deve prevalecer em determinada situação, por mais que também possa causar uma maior morosidade. Não obstante, em algumas situações há a transparência condicionada com a publicidade do que pode ser divulgado e preservação da privacidade e intimidade do titular.

Afinal, o terceiro e último capítulo comenta da interoperabilidade e compartilhamento de dados no Brasil com seus limites e possibilidades, começando pela governança pública digital e os desafios no tratamento de dados na era digital, o qual apresenta uma mudança cultural que provoca necessidade de adaptação que é a inserção no meio virtual, tendo que estabelecer maneiras para proteção dos titulares dos dados ali envolvidos, bem como do fornecimento de acesso. Além disso, não existem legislações aptas a protegerem os usuários, considerando também que a tecnologia muda muito rápido e torna as leis defasadas, colocando os direitos das pessoas em eventuais prejuízos, bem como um exemplo de insuficiência legal é a Autoridade Nacional de Proteção de Dados sem dependência para exercer suas funções. Ademais, as desigualdades para acesso dos dados não possibilitam a devida implementação do instituto, inclusive fomentando as diferenças.

Ainda, em relação da relevância dos sistemas de informações governamentais e compartilhamento de dados para as políticas públicas, serviços públicos e controle da administração pública, as tecnologias proporcionam a satisfação das necessidades humanas e inclusive por sua velocidade que proporciona, como por exemplo os dados abertos que proporcionam acesso para quem tiver interesse e necessitar, proporcionando também vantagens no serviço público. Ademais, quanto ao controle social, as informações por estarem mais dispostas para as pessoas, proporcionam uma ideia dos serviços prestados pelo Estado que possui essa incumbência. Enquanto que em relação ao compartilhamento, ajudam de maneira importante em situações de crimes como é o caso da corrupção. Ademais, tanto o

compartilhamento como a interoperabilidade são importantes nas políticas públicas, em virtude da melhora na captação de dados.

Além disso, os benefícios que podem advir da interoperabilidade no poder público do Brasil, proporcionam na realização de necessidades, bem como o controle social, melhor uso de serviços e informações, bem como políticas públicas mais bem aproveitadas.

Enfim, dos limites e das possibilidades do compartilhamento e interoperabilidade a partir da legislação, doutrina e jurisprudência, a partilha de dados pode ocorrer com concordância do titular de dados e ter necessidade pública, exceto em políticas públicas. Enquanto que a interoperabilidade ocorre entre sistemas diferentes. Entretanto, nenhum dos dois poderá ocorrer em situação de dados com sigilo, bem como tem de cumprir com as normas estabelecidas apesar de necessitar de mais regulamentação e proporcionar mais acesso para as pessoas usuárias.

Contudo, quanto ao problema do presente trabalho, a começar pelo compartilhamento de dados, apresenta como possibilidades elencadas pela legislação, a partilha dos considerados da categoria ampla que não estão sujeitos ao sigilo, não é necessária a autorização da autoridade competente, bem como o procedimento deve ser realizado aos dados abertos e transparência ativa. Enquanto que, a restrita envolve aqueles com resguardo, mas ainda assim possível em virtude de norma e políticas públicas, devendo seguir o que o Comitê Central de Governança de Dados (CCGD) dispuser, bem como o sigilo e não retransmitir ou compartilhar novamente, amenos que a autoridade autorize. Ainda, a específica trata daqueles que também possuem restrição, porém determinados entes governamentais podem acessá-los e transferi-los em conformidade com o que o CCGD estabelecer, sendo também proibida a retransmissão ou o novo compartilhamento, amenos que a autoridade dê sua anuência.

Além disso, em termos gerais, independente da categoria de dados, quem requer os elementos a serem partilhados, deve arcar com os custos, respeitar o resguardo deles, caso necessário e não são necessários pactos ou outras espécies para que aconteça o fenômeno.

Ainda, a doutrina menciona que depende da anuência do titular de dados, exceto em caso de política pública, sendo necessária a finalidade pública em qualquer caso.

Não obstante, a falar da interoperabilidade, os programas envolvidos não podem ter restrições de uso, devem ser abertos, amenos que sejam proprietários de forma temporária. Além disso, não envolver custos aos usuários, bem como respeitar a transparência de dados promovida pela Lei de Acesso à Informação (BRASIL, 2011), respeitar a segurança exigida no serviço e estar adequado ao que vem sendo usado no mercado.

Enquanto que, doutrinariamente, pode ocorrer entre diferentes sistemas envolvidos, desde que haja o meio virtual, visto que não há a possibilidade de compartilhamento de arquivo em mídia física no debate em questão. Entretanto, deve respeitar o sigilo de determinados dados submetidos a ele, bem como resta carente que a sociedade consiga usar melhor os aparelhos tecnológicos em questão.

REFERÊNCIAS

AFONSO TAVARES, André; MÜLLER BITENCOURT, Caroline; DA SILVA CRISTÓVAM, José Sérgio. SOLICITAÇÃO DE ABERTURA DE BASE DE DADOS PERANTE A ADMINISTRAÇÃO PÚBLICA MUNICIPAL: UMA ANÁLISE A PARTIR DOS SEUS PARÂMETROS TÉCNICOS E FUNDAMENTOS NORMATIVOS CONSTITUCIONAIS E INFRACONSTITUCIONAIS. Constituição, Economia e Desenvolvimento: Revista Eletrônica da Academia Brasileira de Direito Constitucional, *[S.I]*, v. 14, n. 26, p. 18-40, 2022. Disponível em: https://www.abdconstojs.com.br/index.php/revista/article/view/491. Acesso em: 17 jun. 2024.

ALLEN, Anita L. The Natural Law Origins of the American Right to Privacy: Natural Law, Slavery, and the Right to Privacy Tort. Fordham Law Review, v. 81, n. 3, p. 1.187 – 1.216. Disponível em: https://ir.lawnet.fordham.edu/flr/vol81/iss3/8/. Acesso em: 30 maio 2024.

ALMEIDA, Siderly do Carmo Dahle de; SOARES, Tania Aparecida. Os impactos da Lei Geral de Proteção de Dados – LGPD no cenário digital. Perspectivas em Ciência da Informação, v. 28, 2023. DOI: https://doi.org/10.1590/1981-5344/25905. Disponível em: https://www.scielo.br/j/pci/a/tb9czy3W9RtzgbWWxHTXkCc/#. Acesso em: 12 ou. 2023.

ALMEIDA, Thiago Martins. PROTEÇÃO DE DADOS PESSOAIS E DEMOCRACIA: os impactos do tratamento de dados nas eleições brasileiras de 2018. 2021. Monografia (graduação em Direito). Centro Universitário UNDB, São Luís, 2021. Disponível em: http://repositorio.undb.edu.br/handle/areas/554. Acesso em: 16 jun. 2024.

ARENDT, Hannah. A CONDIÇÃO HUMANA. Rio de Janeiro: Forense Universitária, 2007. *E-book* (174 p.). ISBN 978-85-218-0255-6 e 85-218-0255-2. Disponível em: https://edisciplinas.usp.br/pluginfile.php/1130009/mod_resource/content/1/A%20condi%C3%A7%C3%A3o%20humana-%20Hannah%20Arendt.pdf. Acesso em: 30 maio 2024.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2019. 328 p.

BIONI, Bruno Ricardo; SILVA, Paula Guedes Fernandes; MARTINS, Pedro Bastos Lobo. Interssecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso. Cadernos Técnicos da CGU, v. 1. Disponível em: https://revista.cgu.gov.br/Cadernos_CGU/article/view/504. Acesso em: 17 jun. 2024.

BRANDEIS, Louis D; WARREN, Samuel D. The right to privacy. Harvard Law Review, v. 4, n. 5, 1890. Disponível em: https://faculty.uml.edu/sgallagher/Brandeisprivacy.htm. Acesso em: 31 maio 2024.

BRASIL. ENUNCIADO N° 4, DE 10 DE MARÇO DE 2022. Brasília, DF: Controladoria-Geral da União/Gabinete do Ministro, 2022. Disponível em: https://repositorio.cgu.gov.br/bitstream/1/67735/3/Enunciado_4_2022.pdf. Acesso em: 17 jun. 2024.

BRASIL. Decreto n.° 8.777, de 11 de maio de 2016. Institui a Política de Dados Abertos do Poder Executivo federal. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8777.htm. Acesso em: 16 jun. 2024.

BRASIL. LEI N° 9.507, DE 12 DE NOVEMBRO DE 1997. Regula o direito de acesso a informações e disciplina o rito processual do *habeas data*. Brasília, DF: Presidência da República, 1997. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9507.htm. Acesso em: 16 jun. 2024.

BRASIL. DECRETO N° 7.724, DE 16 DE MAIO DE 2012. Regulamenta a Lei n° 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5°, no inciso II do §3° do art. 37 e no §2° do art. 216 da Constituição. Disponível em: . Acesso em: 16 jun. 2024.

BRASIL. LEI 12.965, DE 23 DE ABRIL DE 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 16 jun. 2024.

BRASIL. INSTRUÇÃO NORMATIVA N° 4, 13 de abril de 2012. Institui a Infraestrutura Nacional de Dados Abertos – INDA. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.gov.br/agricultura/pt-br/acesso-a-informacao/dadosabertos/arquivos-raiz/in04_2012.pdf. Acesso em: 16 jun. 2024.

BRASIL. LEI N.° 13.709, DE 14 DE AGOSTO DE 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 16 jun. 2024.

BRASIL. [Constituição (1988)]. CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988. Brasília, DF: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 16 jun. 2024.

BRASIL. LEI N° 12.527, DE 18 DE NOVEMBRO DE 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5°, no inciso II do §3° do art. 37 e no §2° do art. 216 da Constituição Federal; altera a Lei n° 8.112, de 11 de dezembro de 1990; revoga a Lei n° 11.111, de 5 de maio de 2005, e dispositivos da Lei n° 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF: Presidência da República, 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 14 out. 2023.

BRASIL. LEI N° 14.129, DE 29 DE MARÇO DE 2021. Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública e altera a Lei n° 7.116, de 29 de 1983, a Lei n° 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), a Lei n° 12.682, de 9 de julho de 2012, e a Lei n° 13.460, de 26 de junho de 2017. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm.

BRASIL. LEI N° 10.406, DE 10 DE JANEIRO DE 2002. Institui o Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 16 jun. 2024.

BRASIL. 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: Mesa da Câmara dos Deputados e Mesa do Senado Federal, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#:~:text=EMENDA%20CONSTITUCIONAL%20N%C2%BA%20115%2C%20DE,e%20tratamento%20de%20dados%20pessoais. Acesso em: 31 maio 2024.

BRASIL. EMENDA CONSTITUCIONAL N° 19, DE 04 DE JUNHO 1988. Modifica o regime e dispõe sobre princípios e normas da Administração Pública, servidores e agentes políticos, controle de despesas e finanças públicas e custeio de atividades a cargo do Distrito Federal, e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc19.htm. Acesso em: 14 jun. 2024.

BRASIL. DECRETO N° 10.046, DE 9 DE OUTUBRO DE 2019. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Disponível em: https://www.planalto.gov.br/ccivil_03/%5C_ato2019-2022/2019/Decreto/D10046.htm. Acesso em: 06 jun. 2024.

BRASIL. DECRETO N° 8.789, DE 29 DE JUNHO DE 2016. Dispõe sobre o compartilhamento de bases de dados na administração pública federal. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8789.htm. Acesso em: 06 jun. 2024.

BRASIL. LEI N° 8.078, DE 11 DE SETEMBRO DE 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 10 jun. 2024.

BRASIL. Supremo Tribunal Federal (Plenário). Segundo Ag. Reg. Na Suspensão de Segurança 3.902 São Paulo. Suspensão de segurança. Acórdãos que impediam a divulgação, em sítio eletrônico oficial, de informações funcionais de servidores públicos, inclusive a respectiva remuneração. Deferimento da medida de suspensão pelo presidente do STF. Agravo Regimental. Conflito aparente de normas constitucionais. Direito à informação de atos estatais, neles embutida a folha de

pagamento de órgãos e entidades públicas. Princípio da publicidade administrativa. Não reconhecimento de violação à privacidade, intimidade e segurança de servidor público. Agravos desprovidos. Agravante: Sindicato dos Especialistas de Educação do Ensino Público do Município de São Paulo – SINESP. Agravante: Associação dos Engenheiros, Arquitetos e Agrônomos municipais de São Paulo e Outros. Agravado: Município de São Paulo. Relator: Ministro Ayres Britto, 09 de junho de 2011. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=628198. Acesso em: 13 jun. 2024.

CÂMARA DOS DEPUTADOS. Acesso à informação não pode ser prejudicado por conta de Lei de Proteção de Dados, dizem especialistas: Deputados e sociedade civil denunciam uso equivocado da LGPD pela administração pública para impedir acesso a informações. Disponível em: https://www.camara.leg.br/noticias/828370-acesso-a-informacao-nao-pode-ser-prejudicado-por-conta-de-lei-de-protecao-de-dados-dizem-especialistas/. Acesso em: 17 jul. 2024.

CALSING, Renata de Assis. Proteção de dados pessoais e autoridade de controle: perspectivas e desafios para o Brasil sob a ótica do direito comparado. 2019. Tese (pós-doutorado em Direito). Universidade de Lisboa, Lisboa, Portugal, 2019. Disponível em: https://repositorio.cgu.gov.br/handle/1/66225. Acesso em: 16 jun. 2024.

CARTOLARI, Lucas Rabello; SILVA, Danilo Pierote. A LEI GERAL DE PROTEÇÃO DE DADOS COMO FERRAMENTA DE PROTEÇÃO DOS DIREITOS FUNDAMENTAIS. 2019. Trabalho de Conclusão de Curso (Bacharelado em Direito) - Fundação de Ensino Eurípides Soares da Rocha, Marília, São Paulo, 2019. Disponível em: https://aberto.univem.edu.br/handle/11077/1853?locale-attribute=en. Acesso em: 12 jun. 2024.

CARVALHO, Eliseu Fernando Silveira de; ROSA, Kenya de Freitas. Resenha do artigo intitulado “Lei geral de proteção de dados (LGPD) e a Lei de acesso à informação pública (LAI): um diálogo (im)possível? As influências do direito europeu”. Revista Processus Multidisciplinar, *[S.I.],* v. 4, n. 8, p. 80-87, 2023. Disponível em: https://periodicos.processus.com.br/index.php/multi/article/view/975. Acesso em: 13 jun. 2024.

CASTRO, Rodrigo Pironti Aguirre de.; LOVATO, Rafael Porto. LGPD e os Tribunais de Contas. Fórum administrativo – FA, Belo Horizonte, ano 20, n. 236, p. 71-74, outubro 2020. Disponível em: file:///C:/Users/User/Desktop/9%C2%B0%20Semestre/Trabalho%20de%20Curso%20em%20Direito%20B/LGPD%20E%20OS%20TRIBUNAIS%20DE%20CONTAS%20-%20Rodrigo%20Pironti.pdf. Acesso em: 01 jun. 2024.

CCGD Comitê Central de Governança de Dados. Regras para Compartilhamento de Dados. Versão 1 – 04/05/2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/interoperabilidade. Acesso em: 07 jun. 2024.

CGI.br. Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: TIC Domicílios 2023. Disponível em:

https://cetic.br/pt/arquivos/domicilios/2023/domicilios/#tabelas. Acesso em: 03 jun. 2024.

CONTROLADORIA-GERAL DA UNIÃO; OUVIDORIA-GERAL DA UNIÃO. Aplicação da Lei de Acesso à Informação na Administração Pública Federal, 4ª edição revista, atualizada e ampliada. Brasília: Controladoria-Geral da União; Ouvidoria-Geral da União, 2019. Disponível em: https://repositorio.cgu.gov.br/bitstream/1/46641/1/aplicacao_da_lai_2019.pdf. Acesso em: 13 jun. 2024.

CRISTÓVAM, José Sérgio da Silva; HAHN, Tatiana Meinhart. ADMINISTRAÇÃO PÚBLICA ORIENTADA POR DADOS: GOVERNO ABERTO E INFRAESTRUTURA NACIONAL DE DADOS ABERTOS. Revista de Direito Administrativo e Gestão Pública, v. 6, n. 1, p. 1-24, jan./jun. 2020. DOI: https://doi.org/10.26668/IndexLawJournals/2526-0073/2020.v6i1.6388. Disponível em: https://www.indexlaw.org/index.php/rdagp/article/view/6388. Acesso em: 12 jun. 2024.

DAVIES, T. *Evaluating the Autumn Statement Open Data Measures*. 2011. Disponível em: https://www.timdavies.org.uk/2011/12/02/3090/. Acesso em: 04 jun. 2024.

DONEDA, Danilo Cesar Maganhoto. DA PRIVACIDADE À PROTEÇÃO DE DADOS PESSOAIS: FUNDAMENTOS DA LEI GERAL DE PROTEÇÃO DE DADOS. São Paulo: Thomson Reuters Brasil, 2020. *E-book*. 432 p. ISBN 978-65-5065-030-8. Disponível em: https://read.amazon.com/?asin=B089QV2MZ9&ref_=kwl_kr_iv_rec_1. Acesso em: 08 jun. 2024.

FACHIN, Zulmar. O direito fundamental à proteção de dados pessoais: análise da decisão paradigmática do STF na ADI 6.387-DF: ANÁLISIS DE LA DECISIÓN PARADIGMÁTICA DEL STF EN LA ADI 6.387-DF. Revista Videre, [S.l.], v. 14, n. 29, p. 298-313, 2022. DOI: 10.30612/videre.v14i19.15629. Disponível em: https://ojs.ufgd.edu.br/index.php/videre/article/view/15629. Acesso em: 13 jun. 2024.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Revista da Faculdade de Direito da USP, *[S.l.]*, v. 88, p. 439-459, 1993. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/67231. Acesso em: 10 jun. 2024.

FORNASIER, Mateus de Oliveira; BECK, Cesar. CAMBRIDGE ANALYTICA: ESCÂNDALO, LEGADO E POSSÍVEIS FUTUROS PARA A DEMOCRACIA. Revista Direito em Debate, *[S.l.]*, v. 29, n. 53, p. 182-195, 2020. DOI: 10.21527/2176-6622.2020.53.182-195. Disponível em: https://www.revistas.unijui.edu.br/index.php/revistadireitoemdebate/article/view/10033. Acesso em: 12 jun. 2024.

FLÔRES, M. R. de; SILVA, R. L. da. Desafios e perspectivas da proteção de dados pessoais sensíveis em poder da administração pública: entre o dever público de informar e o direito do cidadão de ser tutelado. Revista de Direito, [S.I.], v. 12, n. 02,

p. 01-34, 2020. DOI: 10.32361/2020120210327. Disponível em: https://periodicos.ufv.br/revistadir/article/view/10327. Acesso em: 05 jun. 2024.

GARCEL, Adriane; MORO, Sergio Fernando; SOUZA NETTO, José Laurindo de; HIPPERTT, Karen Paiva. Lei geral de proteção de dados: diretrizes e implicações para uma sociedade pandêmica. Coletâneas de artigos jurídicos: em homenagem ao Professor José Laurindo de Souza Netto. Viviane C. de S. K., Adriane G., José L. de S. N. 1.ed., Curitiba: Clássica Editora, 2020. ISBN 978-65-87965-03-1. Pg 319-344. Disponível em: https://www.tjpr.jus.br/documents/18319/47149551/42.+Artigo+Lei+Geral+de+Prote%C3%A7%C3%A3o+de+Dados.pdf/f4e4281e-2318-9799-39a8-f394a68230b3. Acesso em: 12 jun. 2024.

GARCIA, Rafael de Deus. Os direitos à privacidade e à intimidade: origem, distinção e dimensões. Revista da Faculdade de Direito do Sul de Minas, [S.I.], v. 34, n. 1, 2018. Disponível: https://revista.fdsm.edu.br/index.php/revistafdsm/article/view/257. Acesso em: 16 jun. 2024.

Gov.br. Comitê Central de Governança de Dados (CCGD). Governança de dados, Comitê, Comitê Central de Governança de Dados. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/comite-central-de-governanca-de-dados. Acesso em: 06 jun. 2024.

Gov.br. Padrões de Interoperabilidade: Interoperabilidade, Padrões de Interoperabilidade (ePING), integração. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/padroes-de-interoperabilidade#:~:text=A%20ado%C3%A7%C3%A3o%20do%20ePing%20pelos,25%20de%20setembro%20de%202019. Acesso em: 17 jun. 2024.

Gov.br ePING. Padrões de Interoperabilidade de Governo Eletrônico Documento de Referência. Versão 2018. Disponível: https://www.gov.br/governodigital/pt-br/governanca-de-dados/ePING_v2018_20171205.pdf. Acesso em: 17 jun. 2024.

Gov.br ePING. Padrões de Interoperabilidade de Governo Eletrônico: Guia de Interoperabilidade Manual do Gestor. Versão 2012. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/Guia_de_Interoperabilidade_Manual_do_Gestor_2012.pdf. Acesso em: 17 jun. 2024.

GUERREIRO, Ruth; TEIXEIRA, Tarcisio. Lei Geral de Proteção de Dados Pessoais (LGPD): Comentada artigo por artigo. 4. ed. São Paulo: Saraiva, 2022. *E-book*. Disponível em: https://bds.minhabiblioteca.com.br/epub/2463f315-19d3-429f-9002-2536ff7f9041?title=Lei%20Geral%20De%20Prote%C3%A7%C3%A3o%20De%20Dados%20Pessoais:. Acesso em: 17 jun. 2024.

GUICHOT, Emilio. Datos personales y administración pública. Navarra: Thomson & Civitas, 2005.

GUIDI, Guilherme Berti de Campos. PROTEÇÃO DE DADOS PESSOAIS: A COMPOSIÇÃO DE SISTEMAS PELO DIREITO INTERNACIONAL. 2021. Tese

(Doutorado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021. Disponível em: https://journal.nuped.com.br/index.php/revista/article/view/1250/1008. Acesso em: 11 out. 2023.

HIRATA, Alessandro. Direito à privacidade. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Administrativo e Constitucional. Vidal Serrano Nunes Jr., Maurício Zockun, Carolina Zancaner Zockun, André Luiz Freire (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade. Acesso em: 23 mai. 2023.

JABORANDY, Clara Cardoso Machado; PORTO, Carolina Silva; 1984 E O DIREITO À PRIVACIDADE: RUMO À DISTOPIA?. Revista da Faculdade de Direito da UERJ – RFD, *[S.l],* n. 40, p. 295-314, 2022. DOI: 10.12957/rfd.2021.48882. Disponível em: https://www.e-publicacoes.uerj.br/rfduerj/article/view/48882. Acesso em: 16 jun. 2024.

JÚNIOR, José Lázaro. Anders Chydenius, o pioneiro das Leis de Acesso à Informação. 2018. LIVRE.JOR. Disponível em: https://livre.jor.br/anders-chydenius-o-pioneiro-das-leis-de-acesso-informacao/. Acesso em: 16 jun. 2024.

LATHROP, D.; RUMA, L. Open government: Collaboration, transparency, and participation in practice. [S.l.]: O'Reilly Media, 2010. Tradução. Disponível em: https://archive.org/details/OpenGovernment. Acesso em: 03 jun. 2024.

LIMBERGER, Têmis. Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação Pública (LAI): um diálogo (im)possível? As influências do direito europeu. Revista de Direito Administrativo, *[S. l.]*, v. 281, n. 1, p. 113–144, 2022. DOI: 10.12660/rda.v281.2022.85654. Disponível em: https://periodicos.fgv.br/rda/article/view/85654. Acesso em: 12 out. 2023.

MAÑAS, José Luis Piñar. Transparencia y proteccion de datos. Uma referencia de la Ley Española de transparência, acesso a la información y buen gobierno. In: SARLET, Ingo Wolfgang et al. (Coord.). Acesso à informação como direito fundamental e dever estatal. Porto Alegre: Livraria do Advogado, 2016.

MARTANO, Andrés Mantecon Ribeiro. OPEN DATA DAY: DADOS ABERTOS GOVERNAMENTAIS E DEMOCRACIA. Discussão sobre iniciativas de dados governamentais abertos e seus desafios. Elucidare, Manaus, 2018.

MIGUEL, Fernando Gomes. Os desafios do Brasil na nova era da proteção de dados pessoais e da privacidade. Migalhas, n° 5.871, 2019. Disponível em: https://www.migalhas.com.br/depeso/298736/os-desafios-do-brasil-na-nova-era-da-protecao-de-dados-pessoais-e-da-privacidade. Acesso em: 14 jun. 2024.

MONTEIRO, Luis Felipe. Desafios para a transformação digital no setor público brasileiro. Revista do Tribunal de Contas da União, 145, ano 51, jan.-jun.2020.

Disponível em: https://revista.tcu.gov.br/ojs/index.php/RTCU/article/view/1662. Acesso em: 17 jun. 2024.

NETA, Vellêda Bivar Soares Dias. VIDA PRIVADA E INTIMIDADE: ESTRUTURA, CONCEITO, FUNÇÃO E LIMITES NA BUSCA DA TUTELA INTEGRAL DA PESSOA HUMANA. 2010. Artigo – Anais do XIX Encontro Nacional do CONPEDI, Fortaleza, 2010. Disponível em: file:///C:/Users/User/Desktop/9%C2%B0%20Semestre/Trabalho%20de%20Curso%20em%20Direito%20B/Neta.pdf. Acesso em: 08 jun. 2024.

NOVO, Benigno Núñez. A Declaração dos Direitos do Homem e do Cidadão de 1789. 2021. Jusbrasil. Disponível em: https://www.jusbrasil.com.br/artigos/a-declaracao-dos-direitos-do-homem-e-do-cidadao-de-1789/1259443861. Acesso em: 16 jun. 2024.

OLIVEIRA, Alberto Dumont Alves. Um método para aplicação de diretrizes de interoperabilidade do padrão e-PING em portais governamentais de organizações públicas brasileiras. Dissertação (Mestrado em Sistemas de Informação). São Paulo: Universidade de São Paulo, 2017.

OPEN KNOWLEDGE INTERNATIONAL. The Open Definition. 2015a. Disponível em: https://opendefinition.org/. Acesso em: 03 jun. 2024.

OPEN KNOWLEDGE INTERNATIONAL. History of the Open Definition. 2015b. Disponível em: https://opendefinition.org/history/. Acesso em: 03 jun. 2024.

PEREIRA, Marcelo Cardoso. Direito à intimidade na internet. Paraná: Juruá, 2006.

PÉREZ LUÑO, Antonio-Enrique. Derechos humanos, Estado de Derecho y Constitución. 9. ed. Madri: Editorial Tecnos, 2005.

Pesquisa web sobre o uso da Internet no Brasil durante a pandemia do novo coronavírus: Painel TIC COVID-19 [Livro eletrônico]. Web survey on the use of Internet in Brazil during the new coronavirus pandemic: ICT Panel COVID-19. Núcleo de Informação e Coordenação do Ponto BR. 1. Ed. São Paulo: Comitê Gestor da Internet no Brasil, 2021. Disponível em: https://cetic.br/pt/publicacao/painel-tic-covid-19/. Acesso em: 03 jun. 2024.

PINHEIRO, Maria Amélia Eugênia; COTTA, Carla Rodrigues. O compartilhamento de dados pessoais entre instituições públicas para fins de apuração disciplinar. Artigo. Cadernos Técnicos da CGU, v. 3. Disponível em: https://revista.cgu.gov.br/Cadernos_CGU/article/view/601/342. Acesso em: 13 out. 2023.

POUCHAIN, Pedro. A teoria das três esferas da privacidade. Linkedin. Disponível em: https://pt.linkedin.com/pulse/conhece-teoria-das-tr%C3%AAs-esferas-da-privacidade-pouchain-ribeiro. Acesso em: 17 jun. 2024.

QUEIROZ, Renata Capriolli Zocatelli. A proteção de dados pessoais: A LGPD e a disciplina jurídica do Encarregado de Proteção de Dados Pessoais. 2021. Tese

(Doutorado em Direito Civil) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021. DOI: 10.11606/T.2.2021.tde-23082022-085834. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2131/tde-23082022-085834/pt-br.php. Acesso em: 12 jun. 2024.

RODRIGUES, Karina Furtado. Desvelando o conceito de transparência: seus limites, suas variedades e a criação de uma tipologia. Cadernos EBAPE.BR [Online]. 2020, v. 18, n. 2, pp. 237-253. Disponível em: https://www.scielo.br/j/cebape/a/x7BckSpN4dvNMqQmkM5QHcq/?lang=en. Acesso em: 17 jun. 2024.

SANTOS, Raquel Gitirana Torquato dos. A Lei Geral de Proteção de Dados Brasileira: Uma política pública regulatória. 2020. Trabalho de Conclusão de Curso (Especialização em Avaliação de Políticas Públicas) – Escola Superior do Tribunal de Contas da União, Instituto Serzedello Corrêa, Brasília, DF, 2020. Disponível em: file:///C:/Users/User/Downloads/raquel%20Lei%20Geral%20de%20Protecao%20de%20Dados%20Brasileira_4888_%20revisado.pdf. Acesso em: 12 jun. 2024.

SARLET, Ingo Wolfgang. PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL NA CONSTITUIÇÃO FEDERAL BRASILEIRA DE 1988: CONTRIBUTO PARA A CONSTRUÇÃO DE UMA DOGMÁTICA CONSTITUCIONALMENTE ADEQUADA. Revista Brasileira de Direitos Fundamentais & Justiça, *[S. l.]*, v. 14, n. 42, p. 179–218, 2020. DOI: 10.30899/dfj.v14i42.875. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/875. Acesso em: 19 mai. 2024.

SARLET, Ingo Wolfgang et al. Coord. Danilo Doneda et al. Tratado de Proteção de Dados Pessoais. Fundamentos constitucionais: o direito fundamental à proteção de dados. Rio de Janeiro: Forense, 2023. *E-book*. ISBN 978-65-5964-209-0. Disponível em: https://read.amazon.com/?asin=B0BHLYXZPX&ref_=kwl_kr_iv_rec_2. Acesso em: 19 mai. 2024.

SILVA, Lucas Gonçalves da; LIMA, Bruna Dias Fernandes. A COLABORAÇÃO COMPARTILHADA DE DADOS NO GOVERNO DIGITAL BRASILEIRO: A NECESSIDADE DE INTEROPERABILIDADE DOS SERVIÇOS DA ADMINISTRAÇÃO PÚBLICA. Revista Jurídica, [S.I.], v. 1, n. 68, p. 527 – 548, mar. 2022. ISSN 0103-3506. Disponível em: https://revista.unicuritiba.edu.br/index.php/RevJur/article/view/5743. Acesso em: 29 maio 2024.

SILVA, Letícia Brum da; SILVA, Rosane Leal da. A PROTEÇÃO JURÍDICA DE DADOS PESSOAIS NA INTERNET: análise comparada do tratamento jurídico do tema na União Europeia e no Brasil. 2018. Artigo (Graduação em Direito) – Faculdade de Direito, Centro Universitário Franciscano (UNIFRA), Santa Maria, 2018. Disponível em: https://egov.ufsc.br/portal/conteudo/prote%C3%A7%C3%A3o-jur%C3%ADdica-de-dados-pessoais-na-internet-an%C3%A1lise-comparada-do-tratamento-jur%C3%ADdico-do. Acesso em: 14 jun. 2024.

SILVEIRA, Alessandra; FROUFE, Pedro. Do mercado interno à cidadania de direitos: a proteção de dados pessoais como a questão jusfundamental identitária dos nossos

tempos. 2018. Artigo. UNIO – EU Law Journal. Vol. 4, No. 2, p. 4 – 20. Escola de Direito – Universidade do Minho, Braga, Guimarães, Portugal, 2018. Disponível em: http://www.unio.cedu.direito.uminho.pt/Uploads/UNIO%204%20.%20Vol%201/Unio%204%20n.%202%20PT/Alessandra%20Silveira%20&%20Pedro%20Froufe.pdf. Acesso em: 11 jun. 2024.

SPIECKER GENANNT DÖHMANN, Indra. A Proteção de Dados Pessoais sob o Regulamento de Proteção de Dados da União Europeia. Direito Público, *[S.l]*, v. 17, n. 93, 2020. DOI: 10.11117/rdp.v17i93.4235. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/4235. Acesso em: 10 jun. 2024.

TAKANO, C. C; SILVA, L. G. da. O constitucionalismo digital e as novas tecnologias da informação e comunicação (TIC). Revista de Direito, Governança, e Novas Tecnologias, v. 6, n. 1, p. 1-15, 2020. e-ISSN 2526-0049. Disponível em: https://www.indexlaw.org/index.php/revistadgnt/article/view/6392/pdf. Acesso em: 29 mai. 2024.

TAVARES, André Afonso; BITENCOURT, Caroline Müller. Avaliação de políticas públicas e interoperabilidade na perspectiva da governança pública digital. Revista de Direito Econômico e Socioambiental, Curitiba, v. 13, n. 3, p. 687-723, set./dez. 2022. Doi: 10.7213/revdireconsoc.v13i3. 30240. Disponível em: https://periodicos.pucpr.br/direitoeconomico/article/view/30240. Acesso em: 17 jun. 2024.

TEPEDINO, Gustavo; DONEDA, Danilo. A outra face da liberdade. O Globo, 15 jun. 2010. Disponível em: https://oglobo.globo.com/in/a-outra-face-da-liberdade-2993811. Acesso em: 12 jun. 2024.

UNIÃO EUROPEIA. Carta dos Direitos Fundamentais da União Europeia. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=EN. Acesso em: 11 jun. 2024.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434. Acesso em: 11 jun. 2024.

UNIÃO EUROPEIA. Regulamento (CE) n.° 1049/2001 do Parlamento Europeu e do Conselho, de 30 de maio de 2001, relativo ao acesso do público aos documentos do Parlamento Europeu, do Conselho e da Comissão. Bruxelas: Parlamento Europeu. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A32001R1049. Acesso em: 16 jun. 2024.

UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Luxemburgo: Parlamento Europeu. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A31995L0046. Acesso em: 16 jun. 2024.

UNIÃO EUROPEIA. CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA. Jornal Oficial das Comunidades Europeias. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 16 jun. 2024.

VALLE, Vivian Lima López; BARBOSA, Bruna Gavron. Os desafios quanto a preservação da privacidade e da proteção de dados em face dos equipamentos IoT. International Journal of Digital Law, Belo Horizonte, v. 4, n. 1, p. 35-61, jan./abr. 2023. DOI: 10.47975/digital.law.vol.4.n.1.valle. ISSN: 2675-7087. Disponível em: file:///C:/Users/User/Desktop/9%C2%B0%20Semestre/Trabalho%20de%20Curso%20em%20Direito%20B/Os+desafios+quanto+a+preservac%CC%A7a%CC%83o+da+privacidade+e+da+protec%CC%A7a%CC%83o+de+dados+em+face+dos+equipamentos+IoT%20(2).pdf. Acesso em: 10 jun. 2024.

VELOSO, Renato. Tecnologias da informação e comunicação: desafios e perspectivas. Ed. Especial Anhanguera. São Paulo: Saraiva, 2012. Disponível em: https://www.academia.edu/33231149/Tecnologias_da_Informa%C3%A7%C3%A3o_e_Comunica%C3%A7%C3%A3o_Renato_Veloso. Acesso em: 29 maio 2024.

VIEIRA, Tatiana Malta. O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. 2007. Dissertação (Mestrado em Direito) - Universidade de Brasília, Brasília, 2007. Disponível em: http://icts.unb.br/jspui/handle/10482/3358. Acesso em: 27 mai. 2024.