UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE CIÊNCIAS SOCIAIS E HUMANAS
CURSO DE DIREITO

Gabriel do Nascimento da Silva

ADMINISTRAÇÃO PÚBLICA DIGITAL E O DIREITO À PROTEÇÃO DE DADOS PESSOAIS: UMA ANÁLISE DO TRATAMENTO DE DADOS PELO PODER PÚBLICO SOB A ÓTICA DA VIGILÂNCIA ESTATAL

Santa Maria, RS
2023

Gabriel do Nascimento da Silva

ADMINISTRAÇÃO PÚBLICA DIGITAL E O DIREITO À PROTEÇÃO DE DADOS PESSOAIS: UMA ANÁLISE DO TRATAMENTO DE DADOS PELO PODER PÚBLICO SOB A ÓTICA DA VIGILÂNCIA ESTATAL

Monografia apresentada ao Curso de Direito da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do grau de **Bacharel em Direito.**

Orientador: Prof. Me. João Pedro Seefeldt Pessoa

Santa Maria, RS, Brasil
2023

Gabriel do Nascimento da Silva

ADMINISTRAÇÃO PÚBLICA DIGITAL E O DIREITO À PROTEÇÃO DE DADOS PESSOAIS: UMA ANÁLISE DO TRATAMENTO DE DADOS PELO PODER PÚBLICO SOB A ÓTICA DA VIGILÂNCIA ESTATAL

Monografia apresentada ao Curso de Direito da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do grau de **Bacharel em Direito.**

Aprovado em 10 de janeiro de 2023.

JOAO PEDRO SEEFELDT PESSOA:03157191098
Assinado de forma digital por JOAO PEDRO SEEFELDT PESSOA:03157191098
Dados: 2023.01.17 11:33:52 -03'00'

João Pedro Seefeldt Pessoa, Me. (UFSM)

gov.br
Documento assinado digitalmente
FRANCIELLE BENINI AGNE TYBUSCH
Data: 17/01/2023 10:32:45-0300
Verifique em https://verificador.iti.br

Francielle Benini Agne Tybush, Dra. (UFSM)
(Avaliador)

HENDRISY ARAUJO DUARTE:03388125040
Digitally signed by HENDRISY ARAUJO DUARTE:03388125040
Date: 2023.01.17 11:18:02 -03'00'

Hendrisy Araujo Duarte, Mda. (UFSM)
(Avaliador)

Santa Maria, RS
2023

AGRADECIMENTOS

Aos meus pais, Valder e Nedi, sou grato pelo suporte e amor que me foram dados durante todo processo até aqui. Sem vocês não seria possível e, por isso, espero deixá-los orgulhosos.

Aos meus irmãos, Guilherme, Rafael e Miguel, agradeço o companheirismo e fraternidade que foram essenciais durante esse trajeto.

À minha dinda, Vera, presto meus agradecimentos por sempre estar presente conosco e desempenhar um papel importantíssimo desde o meu nascimento.

À Júlia, minha namorada, principal presente desses cinco anos de curso e a maior incentivadora da evolução que tive durante essa trajetória, muito obrigado. Eu dificilmente conseguiria expressar aqui a tua importância em todas as esferas da minha vida, mas deixo meu agradecimento por tudo isso.

Aos amigos Artur, Conrado, Guilherme, Lauany e Luís Felipe, com quem compartilhei o dia a dia e construí memórias que fizeram da graduação um período de muito valor, sou grato por tudo isso e espero tê-los comigo para além desse período.

Ao meu orientador, Professor João Pedro, agradeço a disponibilidade e instruções que foram, sem dúvidas, muito relevantes para a condução do trabalho.

Por derradeiro, também destino meu muito obrigado a todos aqueles que de alguma forma contribuíram para minha jornada, servindo de exemplo para o meu desenvolvimento como pessoa e/ou acadêmico, das quais destaco Leonardo e Charline.

RESUMO

ADMINISTRAÇÃO PÚBLICA DIGITAL E O DIREITO À PROTEÇÃO DE DADOS PESSOAIS: UMA ANÁLISE DO TRATAMENTO DE DADOS PELO PODER PÚBLICO SOB A ÓTICA DA VIGILÂNCIA ESTATAL

AUTOR: Gabriel do Nascimento da Silva
ORIENTADOR: João Pedro Seefeldt Pessoa

O presente trabalho busca analisar, dentro do atual contexto da vigilância exercida pelo Estado, em que medida a atual forma de desenvolvimento da Administração Pública Digital no Brasil, que pressupõe o compartilhamento e unificação de dados dos cidadãos em posse do Poder Público, é compatível com a Lei Geral de Proteção de Dados Pessoais (LGPD), alicerçada na privacidade e no direito fundamental à proteção de dados pessoais. Para tal propósito, analisa-se o moderno estágio evolutivo da vigilância estatal, em destaque no que concerne à utilização das novas tecnologias de informação e comunicação, além do processo de valorização do direito à proteção de dados pessoais e os avanços legislativos acerca do tema, investigando-se, por derradeiro, os ditames que cercam a instauração da Administração Pública Digital no país, com foco no compartilhamento e unificação de dados entre órgãos públicos e sua compatibilidade com o direito à proteção de dados pessoais. Como método de abordagem, adota-se o dedutivo, partindo de uma análise geral da vigilância na sociedade contemporânea e do desenvolvimento do direito à proteção de dados pessoais a nível internacional e, posteriormente, nacional, chegando-se às especificidades acerca da Administração Pública Digital e a compatibilidade dos seus atuais ditames com a legislação vigente. No que se refere ao método de procedimento, faz-se uso do histórico e monográfico, o primeiro para compreender o fenômeno da vigilância exercida pelo Estado e a construção da atual legislação sobre proteção de dados, e segundo para analisar especificamente a atuação da Administração Pública Digital no país e suas especificidades. A título de técnica de pesquisa, utiliza-se a documentação direta, com análise da legislação pertinente à temática discutida, em destaque a Lei Geral de Proteção de Dados Pessoais e o Decreto nº 10.046/2019, e indireta por meio de pesquisa documental, bibliográfica e jurisprudencial. Da pesquisa realizada, conclui-se que o compartilhamento de dados pelo Poder Público, como previsto na atual legislação, apresenta incompatibilidades com a LGPD e o direito à proteção de dados pessoais, em destaque pela utilização de termos estranhos ao diploma mencionado, e pelo afastamento da atuação da Autoridade Nacional de Proteção de Dados. Por fim, entendeu-se que a participação direta do indivíduo no tratamento de disponibilização dos seus dados é essencial para garantir a sua autodeterminação informativa, sendo necessária a promoção de uma contravigilância por parte da população, a fim de garantir a atuação do Estado nos termos da lei, impedindo a utilização de dados pessoais para outros fins que não previamente previstos.

Palavras-chave: Administração Pública Digital; Autodeterminação informativa; Compartilhamento de dados; Direito à proteção de dados pessoais; Vigilância estatal.

ABSTRACT

DIGITAL PUBLIC ADMINISTRATION AND THE RIGHT TO PERSONAL DATA PROTECTION: AN ANALYSIS OF STATE DATA PROCESSING BY PUBLIC AUTHORITIES FROM THE PERSPECTIVE OF STATE SURVEILLANCE

AUTHOR: Gabriel do Nascimento da Silva
ADVISOR: João Pedro Seefeldt Pessoa

This paper seeks to analyze, within the current context of surveillance by the State, to what extent the current form of development of Digital Public Administration in Brazil, which assumes the sharing and unification of citizen data held by the government, is compatible with the General Law of Personal Data Protection (LGPD), based on privacy and the fundamental right to protection of personal data. For this purpose, the modern evolutionary stage of state surveillance is analyzed, especially with regard to the use of new information and communication technologies, as well as the process of valorization of the right to personal data protection and legislative advances on the subject, investigating, lastly, the dictates surrounding the establishment of Digital Public Administration in the country, with a focus on sharing and unification of data between public agencies and its compatibility with the right to personal data protection. As a method of approach, the deductive approach is adopted, starting from a general analysis of surveillance in contemporary society and the development of the right to personal data protection at an international level and, subsequently, at a national level, arriving at the specifics regarding Digital Public Administration and the compatibility of its current dictates with the legislation in force. Regarding the procedural method, we make use of the historical and monographic, the first one as a way of understanding the phenomenon of surveillance exercised by the State and the construction of the current legislation on data protection, and the second one to specifically analyze the performance of the Digital Public Administration in the country and its specificities. As a research technique, direct documentation was used, analyzing the legislation pertinent to the theme discussed, especially the General Law of Data Protection and Decree n. 10.046/2019, and indirect through documentary, bibliographic and case law research. From the research, it was concluded that the sharing of data by the Public Authorities, as provided for in the current legislation, presents incompatibilities with the LGPD and the right to personal data protection, especially due to the use of terms foreign to the mentioned diploma, and the removal of the role of the National Data Protection Authority. Finally, it was understood that the direct participation of the individual in the treatment of making his data available is essential to ensure his informational self-determination, being necessary the promotion of a counter-surveillance by the population, in order to ensure the State's performance under the law, preventing the use of personal data for purposes other than those previously provided.

Keywords: Digital Public Administration; Informative Self-determination; Data Sharing, Right to Personal Data Protection; State Surveillance.

SUMÁRIO

1. INTRODUÇÃO

Sob a ótica do atual estágio de evolução das tecnologias de informação e comunicação, discutir a proteção de dados pessoais e a privacidade dos cidadãos é questão de grande importância a nível global. Nesse sentido, a utilização de informações dos indivíduos passou a ser amplamente realizada por agentes privados no exercício de um novo modelo econômico, em que os dados tornaram-se a principal fonte de matéria-prima, servindo a prever o comportamento dos indivíduos e, mais do que isso, guiá-los a outros.

O Poder Público, no mesmo sentido, também faz uso de tais elementos, o que, por vezes, serve a interesses escusos de vigilância sobre os indivíduos. Conforme recentes vazamentos de informações, diversos países mantêm programas de vigilância a nível global, os quais não apresentam a transparência necessária. No Brasil, inclusive, muito pouco se sabe acerca do tema, existindo programas de observação e cruzamento de informações dos cidadãos.

Dentro desse cenário, iniciaram-se diversas discussões acerca da necessidade de concretização de uma proteção dos dados pessoais, o que, de início, deu-se a partir do direito à privacidade. Já em um estágio mais avançado sobre o tema, a União Europeia veio a publicar o seu Regulamento Geral sobre a Proteção de Dados em 2016, instrumento que buscou unificar as diretrizes já adotadas no bloco europeu e garantir o direito à proteção de dados aos cidadãos.

Além de tais objetivos, a legislação mencionada também influenciou diversos diplomas ao redor do mundo. Destaca-se, nesse sentido, a publicação da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), no Brasil, que possui importância ímpar na condução do tema a nível nacional, gerando diversas discussões acerca dos seus dispositivos.

Por outro lado, considerando o já mencionado avanço tecnológico, também entrou em pauta no país (e no mundo) a necessidade do desenvolvimento de uma Administração Pública Digital, a fim de facilitar a oferta de serviços governamentais aos cidadãos e propiciar maior celeridade à condução de políticas públicas. Isso, todavia, exige a chamada interoperabilidade entre os mais diversos órgãos integrantes da administração, o que inclui as informações sob posse de cada um.

Esse cenário, portanto, reivindica os dados pessoais dos cidadãos para a sua efetivação, os quais necessitam ser compartilhados internamente pelo Poder Público. Isto posto, há de se analisar a adequação dessa transferência de dados para unificação de serviços com o direito à proteção de dados pessoais, sendo o assunto de grande importância social e

jurídica, considerando os perigos envolvidos no amplo acesso a uma base unificada de dados dos cidadãos. Busca-se, assim, estabelecer os limites do compartilhamento de informações pessoais dos indivíduos de forma interna pela Administração Pública e sua conformidade com a legislação vigente.

Dentro dessa conjuntura, a pesquisa ora em comento busca resolver a seguinte problemática: considerando o atual contexto da vigilância exercida pelo Estado, em que medida a atual forma de desenvolvimento da Administração Pública Digital no Brasil, que pressupõe o compartilhamento e unificação de dados dos cidadãos em posse do Poder Público, é compatível com a Lei Geral de Proteção de Dados Pessoais (LGPD), alicerçada na privacidade e no direito fundamental à proteção de dados pessoais?

A fim de encontrar uma resposta ao problema, o presente trabalho tratará acerca do panorama de proteção de dados pessoais na atualidade, com foco no desenvolvimento e nas determinações da Lei Geral de Proteção de Dados Pessoais. Junto disso, analisar-se-ão as normas que regem o plano de inserção da Administração Pública no âmbito digital, em destaque quanto ao compartilhamento de dados e a unificação de tais informações na mesma plataforma.

Desse modo, inicialmente, será explorado o histórico de desenvolvimento da sociedade de vigilância e a influência das novas tecnologias sobre a sua atuação, averiguando-se também o histórico de programas de vigilância a nível nacional e internacional. Além disso, averiguar-se-á o desenvolvimento do direito à proteção de dados pessoais, bem como a condução legislativa do tema no mundo e, após, no Brasil, principalmente no que concerne à Lei Geral de Proteção de Dados Pessoais. Por último, o trabalho abordará o processo de evolução da Administração Pública Digital no Brasil, concentrando-se no compartilhamento de dados e na unificação de serviços através do Cadastro Base do Cidadão.

Para tal, utiliza-se do método de abordagem dedutivo, que será iniciado nos contornos gerais da vigilância e da proteção de dados pessoais, chegando às especificidades do compartilhamento de dados e unificação de serviços no âmbito da Administração Pública Digital através do Cadastro Base do Cidadão. No que se refere ao método de procedimento, faz-se uso do método histórico, a fim de compreender os contornos envolvidos no exercício da vigilância estatal e o desenvolvimento do direito à proteção de dados e da Administração Pública Digital, além do método monográfico, com o objetivo de analisar a legislação e as decisões acerca do compartilhamento e tratamento de dados pelo Poder Público, assim como compreender o entendimento da doutrina específica acerca do tema. Ainda, a técnica de

pesquisa empregada consiste em documentação indireta, por meio de pesquisa bibliográfica, jurisprudencial, e documental em textos normativos, em destaque a Lei Geral de Proteção de Dados e o Decreto 10.046/2019, além de outras normativas acerca do tema.

A construção do texto será realizada em três partes: a primeira, denominada "A vigilância estatal e o tratamento de dados pessoais pelo Poder Público", tem como foco analisar o desenvolvimento da vigilância como política de estado e como um novo modelo econômico, inclusive no Brasil, analisando-se o (des)conhecido sistema de vigilância do país. Na segunda parte, intitulada "O direito à proteção de dados pessoais e a refundação da privacidade no ordenamento jurídico brasileiro", será discutida a construção de um direito fundamental à proteção de dados a nível nacional e internacional, com foco na legislação brasileira.

Por fim, a terceira parte, denominada "A Administração Pública Eletrônica, governo digital e o tratamento de dados pessoais", analisa o processo de integração da Administração Pública com as novas tecnologias de informação e comunicação, bem como das normas que determinam o compartilhamento e a integração de dados dos cidadãos no âmbito do Poder Público, discutindo-se esse desenvolvimento sob a ótica do direito à proteção de dados pessoais e da vigilância estatal.

2. A VIGILÂNCIA ESTATAL E O TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

Conforme se extrai da obra de Michel Foucault (2014), a vigilância hierárquica, constituída pelo controle e observação das ações humanas, foi amplamente utilizada em diversos espaços da vida em sociedade, como na construção de cidades, hospitais, asilos, prisões e instituições de ensino. Nesse sentido, acerca da execução dessa vigilância, percebe-se que "o exercício da disciplina supõe um dispositivo que obrigue pelo jogo do olhar; um aparelho onde as técnicas que permitem ver induzam a efeitos de poder, e onde, em troca, os meios de coerção tornem claramente visíveis aqueles sobre quem se aplicam" (FOUCAULT, 2014, p. 168).

A utilização de tais técnicas, como se vê, compõe o dispositivo da disciplina, que, somado à punição, desenvolve a prática social do poder. Este último, segundo Max Weber (2004, p. 179), é considerado como "a probabilidade de uma pessoa ou várias impor, numa ação social, a vontade própria, mesmo contra a oposição de outros participantes desta".

Destacadamente a partir do século XVIII, a vigilância tornou-se um dos principais instrumentos para o exercício do poder. Para a sua execução, então, tomou-se por base o sistema panóptico, desenvolvido por Jeremy Bentham, onde o indivíduo tinha o receio de estar sendo vigiado, o que, por muitas vezes, sequer estava ocorrendo. Isso porque a construção arquitetônica do ambiente - geralmente circular e com o observador no centro - propiciava a ciência da observação e, ao mesmo tempo, a dúvida se ela realmente estava ocorrendo. Com isso, o controle dos corpos tornou-se completo sem a necessidade de um olhar constante sobre os indivíduos.

Na sociedade atual, contudo, o exercício da observação e do controle sobre a população tomou novos rumos. O que se verifica, na verdade, é que os sistemas e técnicas adotados evoluíram da mesma forma que a comunicação e a tecnologia, especialmente a partir da Segunda Guerra Mundial. Somado a isso, a crescente globalização e troca de dados entre os mais diversos agentes permitiu a criação de um conjunto de informações muito abrangente e perigoso, o chamado Big Data.

Dessa forma, faz-se necessário explorar, a partir do método de procedimento histórico, a vigilância exercida pelos Estados, o que será realizado no primeiro momento, e a contribuição dos entes privados para o seu exercício, principalmente na coleta e tratamento de dados. Além disso, averiguar-se-á o uso de dados pessoais pelo Poder Público na atualidade, com foco nos novos sistemas de vigilância e possíveis violações a direitos.

2.1. EVOLUÇÃO HISTÓRICA DA VIGILÂNCIA EXERCIDA PELO ESTADO

No ano de 2013, o analista de sistemas Edward Snowden se dirigiu à Hong Kong e entregou diversos documentos e informações confidenciais angariadas do governo dos Estados Unidos da América aos jornalistas Glenn Greenwald e Laura Poitras, que levaram a público as questões trazidas através dos portais The Guardian, The Washington Post e The Intercept (GREENWALD, 2013).

Mais especificamente, os documentos expostos tratavam acerca da atuação da Agência Nacional de Segurança estadunidense, revelando diversos programas de espionagem utilizados pelo país, o que culminou na divulgação de outros sistemas similares utilizados pelos mais diversos Estados ao redor do globo (GREENWALD, 2013). O ocorrido, claro, possui uma construção histórica por trás. Anteriormente ao atual estágio de evolução da tecnologia, conforme já referido, os Estados se utilizavam de outros dispositivos de vigilância e controle social.

O exercício do poder em sociedades ainda intocadas pela evolução comunicacional era limitado a espaços físicos. Nesse sentido, a arquitetura dos espaços se tornou peça necessária no controle do indivíduo, pelo que a utilização do sistema panóptico passou a ser amplamente difundida em prisões, manicômios, fábricas e outros locais do gênero. Em Vigiar e Punir, Michel Foucault (2014, p. 195), acerca disso, afirmou que a vantagem do referido sistema seria de "induzir no detento (lê-se vigiado) um estado consciente e permanente de visibilidade que assegura o funcionamento automático do poder". Assim, o sistema de vigilância tem como permanente os seus efeitos, mesmo que a ação de vigiar não esteja realmente ocorrendo, mas o simples fato de saber que poderia estar sendo vigiado, fazia com que o sujeito se comportasse seguindo às normas.

Jeremy Bentham, nessa linha, prescreveu dois princípios básicos do sistema panóptico: que ele deve ser visível e inverificável. Resumidamente, o observado deve ter ciência de que está sendo espionado, o que se traduz na presença de uma alta construção central de observação e, também, o indivíduo jamais poderia saber se realmente estava sendo vigiado, mesmo sabendo que sempre poderia estar (BENTHAM, 2019, p. 188).

O cumprimento de tais requisitos, ademais, foi previsto pelo autor através das mais diversas construções arquitetônicas e ópticas que pudessem garantir o seu melhor desenvolvimento. Isso se traduziu, então, na utilização de persianas e ângulos que impedissem a visualização do vigia, além da ausência de portas para que não se pudesse perceber movimento no local, dentre outras recomendações.

Mais adiante, a partir da segunda metade do século XVIII, o foco da vigilância foi alterado, transferindo o controle dos corpos individuais para o coletivo. Com isso, o controle social passou a modular o comportamento populacional por meio de novas técnicas de observação. O que se verifica, entretanto, não é a extinção do primeiro sistema de controle, mas sim a sua modificação parcial, porém em uma escala muito maior, a fim de controlar comportamentos de forma massificada, o que seria chamado de "biopolítica" da espécie humana (FOUCAULT, 2005).

Após, considerando o crescente desenvolvimento das tecnologias de informação e comunicação, especialmente a partir da microeletrônica ao fim da Segunda Guerra Mundial, com o consequente aumento das trocas de dados pelos mais variados agentes, a vigilância novamente passou a adotar novos rumos e a se aperfeiçoar. Diferente do que ocorria antes, no entanto, essa observação deixa de ser verticalizada e passa a ser realizada de forma horizontal, expandindo sua atuação para além de instituições fechadas, espalhada por todo o tecido social, em diferentes e numerosos dispositivos de controle contínuo e de comunicação instantânea (DELEUZE, 1992, p. 216-220).

A partir de tal conjuntura, foram criados programas com capacidade de vigilância global, como o sistema Echelon, que, conforme relatório divulgado pelo Parlamento Europeu, foi desenvolvido a partir de um acordo de cooperação firmado entre Estados Unidos e Reino Unido, o denominado *UKUSA Agreement*, também referido como Tratado de Segurança UK-USA, o qual também contou com a ajuda de outros países aliados (UNIÃO EUROPEIA, 2001). O referido acordo, aliás, somente passou a ser conhecido a partir do final do século XX, mesmo que sua criação tenha se dado para utilização na Segunda Grande Guerra, sendo que o tratado só foi confirmado no início do século XXI, permanecendo mais de 50 (cinquenta) anos sem ser admitido por seus integrantes (NORTON-TAYLOR, 2010).

A atuação dos Estados Unidos e do Reino Unido, em resumo, consistia na vinculação de ambos os países a "uma rede mundial de postos de escuta administrados pela GCHQ, a maior organização de espionagem da Grã-Bretanha, e seu equivalente dos EUA, a Agência de Segurança Nacional" (NORTON-TAYLOR, 2010, tradução nossa). Quanto à isso, ainda, Duncan Campbell (2001), autor de um relatório investigativo sobre o sistema Echelon, o qual foi entregue ao Parlamento Europeu e deu publicidade ao caso, afirmou que enormes organizações de decodificação tiveram acesso a informações oriundas de centenas de milhares de sinais alemães e japoneses na Segunda Guerra, as quais foram lidas e analisadas pelos países aliados, o que somente se deu em razão do acordo previamente estabelecido.

O referido sistema Echelon, nessa linha, foi descrito por Rogério da Costa da seguinte

forma: “estações de interceptação de sinais em todo o mundo capturam todo o tráfego de comunicações via satélite, microondas, celular e fibra ótica, processando essas informações em computadores de alta capacidade” (COSTA, 2004, p. 03). O sistema, inclusive, inclui programas de reconhecimento de voz e caracteres, além de procurar por palavras e frases chaves, as quais podem ser marcadas e utilizadas em análises futuras.

O foco inicial do programa, claro, dizia respeito à espionagem militar e diplomática, porém sua atuação se tornou, com o passar do tempo, mais abrangente, também envolvendo questões científicas e econômicas. Mais atualmente, o uso de programas similares passou a ser concentrado em questões como terrorismo e combate aos mais variados crimes, especialmente a partir dos atentados terroristas de setembro de 2001 nos Estados Unidos e do recrudescimento da Guerra ao Terror (GREENWALD, 2013).

A utilização de tais sistemas e programas, contudo, não foi bem aceita por diversos agentes, inclusive indivíduos que atuavam no seu desenvolvimento, como no caso do analista de sistemas Edward Snowden, conforme já exposto. O que se sucedeu por volta do 2010, nessa linha, foi uma série de revelações de documentos confidenciais guardados por entidades governamentais, os quais possuíam caráter ultrassecreto, inclusive com a descoberta da existência da Agência Nacional de Segurança, nos Estados Unidos. As ocorrências, por certo, não foram intencionais, mas sim geradas pelo trabalho de ativistas e pessoas que tinham acesso a informações governamentais ultrassecretas, como Snowden. Com exceção deste, os casos mais relevantes e com repercussão mundial foram os de Chelsea Manning e Julian Assange.

No primeiro, ocorrido em 2010, a ex-integrante do exército americano disponibilizou ao público, por meio da WikiLeaks - uma organização de atuação transnacional que age em favor de uma maior transparência dos governos -, mais de 700 mil arquivos secretos resguardados pelos Estados Unidos da América, o que incluiu “relatos de operações militares no Iraque e Afeganistão [...] ou mesmo milhares de telegramas enviados por diplomatas americanos ao redor do mundo” (FAUS, 2017). Em razão disso, a ativista foi presa e condenada a 35 (trinta e cinco) anos de prisão, período que, em 2017, foi reduzido para 7 (sete) anos pelo então presidente estadunidense, Barack Obama.

A organização mencionada, responsável pela publicação dos documentos disponibilizados por Manning, foi criada em 2006, pelo jornalista Julian Assange, e se autointitula como “uma biblioteca gigantesca dos documentos mais perseguidos do mundo” (WIKILEAKS, 2015). Em resumo, o site atua angariando e publicando documentos originais e confidenciais vazados ou obtidos dos mais diversos governos. Por esse trabalho, no entanto,

Assange possui 18 acusações de espionagem nos Estados Unidos, estando detido na prisão de alta segurança de Belmarsh, em Londres, desde 2019 (REINO UNIDO…, 2020). Atualmente, outrossim, o jornalista tem travado uma guerra judicial com o Reino Unido, a fim de evitar sua extradição para os Estados Unidos. Todavia, a atual Ministra do Interior britânica decidiu de forma desfavorável ao ativista, o que veio a ocorrer em 17/07/2022, ainda cabendo recurso (CARDOSO, 2022).

O que se viu na sequência, então, foi a revelação de diversos outros programas de vigilância global. Dentre os dados expostos, destacam-se a descoberta dos programas *PRISM*, *Boundless Informant*, *X-Keyscore*, *Tempora*, *Muscular* e *Stateroom*, os quais se mostraram com elevado desenvolvimento tecnológico e de capacidade de vigilância. Nesse sentido, diversos países ficaram conhecidos pelo uso de técnicas de observação, em destaque o grupo conhecido como *Five Eyes* (cinco olhos), composto por Estados Unidos, Reino Unido, Austrália, Canadá e Nova Zelândia. Além dos citados, outros Estados também possuem programas de vigilância ou se utilizam daqueles já mencionados, tais como Alemanha, França e Países Baixos (FRAZÃO, 2016, p. 17)[1].

Os programas referidos, guardadas as suas devidas especificidades, coletam, armazenam e analisam dados oriundos de serviços de comunicação, os quais são obtidos junto aos provedores de serviço ou de portadores (UNIÃO EUROPEIA, 2018). Muitos deles, a propósito, tratam de dados obtidos também de não nacionais, expandido sua atuação a nível global, o que é facilitado pela contribuição de grandes agentes do setor econômico, cuja capilaridade atinge populações inteiras, tais como *Google*, *Microsoft*, *Meta* (*Facebook*, *Instagram* e *WhatsApp*) e *Apple*, dentre muitos outros.

Nessa linha, descobriu-se que os mais diversos programas de inteligência têm ou tiveram acesso a muitos dados dos usuários de redes de comunicação. A exemplo, destaca-se a ação da agência de espionagem britânica (GCQH), que, em parceria com a estadunidense (NSA), interceptou milhões de conversas via *webcam* no Yahoo, armazenando as imagens obtidas, conforme publicou o jornal The Guardian, o que foi realizado pelo programa de vigilância denominado Optic Nerve (FIORETTI, 2014). Além disso, outros países, incluindo o Brasil, também foram espionados pelos programas descritos, conforme revelado pelo WikiLeaks (EUA…, 2015), o que gerou, de maneira geral, repercussões condenatórios a nível

[1] "Por exemplo, PRISM, dos Estados Unidos, Austrália, Reino Unido e Países Baixos; XKeyscore, dos Estados Unidos, Alemanha e Austrália e Nova Zelândia; Project 6, da Alemanha e Estados Unidos; Stateroom, dos Cinco Olhos; Lustre, dos Estados Unidos e França; Optic Nerve, dos Estados Unidos e Reino Unido; Turbine, dos Estados Unidos, Reino Unido e Japão; Operation Socialist, do Reino Unido; Tempora, Muscular, Follow The Money, Marina, Dishfire, Mystic, estes todos dos Estados Unidos, podendo haver ou não coordenação com outras agências parceiras." (PESSOA, 2020, p. 33).

mundial.

Esse cenário, então, remonta ao mundo distópico apresentado na obra 1984 (ORWELL, 1949), que descrevia "um futuro trágico em que um governo totalitário, chamado Big Brother (Grande Irmão), fiscaliza e controla as ações de todos os seus cidadãos revogando direitos e liberdades individuais" (FRAZÃO, 2016, p.75). Isso porque a comunicação e a vida humana passaram a utilizar a internet como um dos seus principais instrumentos, o que, contudo, é alvo constante da coleta e tratamento de dados por agentes que sequer são conhecidos pelos usuários.

Em que pese as problemáticas envolvidas nesse contexto, a utilização de programas de vigilância é justificada a nível constitucional e internacional para promoção de segurança pública e defesa nacional, principalmente no combate ao terrorismo. Este último, todavia, permite que seja perpetrada a mais ampla observação possível, uma vez que o inimigo pode ser qualquer pessoa, seja domiciliada no país ou não. O cenário criado, assim, transmite medo à população, que, em razão disso, chancela o ideal vigilante na busca por mais segurança (PESSOA, 2020, p. 36-37).

Além disso, diferente do que acontecia anteriormente, a vigilância estatal da atualidade não necessita da presença de megaestruturas, sendo executada através do monitoramento das informações fornecidas por usuários das novas tecnologias de informação e comunicação espalhadas pelo globo. Dentre tais, por certo, destaca-se a *internet*, cujo desenvolvimento possibilitou a interconexão mundial entre os mais diversos atores sociais, o que também facilitou a coleta e o tratamento dos dados que esses agentes disponibilizam na rede.

Trata-se de um Estado geral da vigilância, que "tende a tornar-se incorporada em diversos dispositivos, serviços e ambientes que usamos cotidianamente, mas que se exerce de modo descentralizado, não hierárquico e com uma diversidade de propósitos, funções e significações nos mais diferentes setores" (BRUNO, 2009, p. 02). O que se vê, na verdade, é que a vigilância estatal passou a um novo patamar, sendo realizada através de dados gerados pelos próprios usuários de redes de comunicação, situação que exige uma melhor análise acerca das suas consequências e limites.

2.2. *BIG DATA* E PROTEÇÃO DE DADOS PESSOAIS NA ATUALIDADE

Dentro do contexto já apresentado, ainda, há de se analisar mais a fundo a atual conjuntura da atividade econômica na coleta e tratamentos de dados pessoais. Conforme descrito, esses agentes também contribuem para o sistema de vigilância mundial

desempenhado pelos Estados, além de exercer observação sobre os indivíduos por si só. Mais do que isso, esses atores deram origem a um novo tipo de capitalismo, chamado de capitalismo de vigilância.

Conforme expõe Shoshana Zuboff (2021, p. 21), esse novo sistema "reivindica de maneira unilateral a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais". Esses dados, em certa parte, são utilizados para melhorias nos serviços e avanços na sua realização, o que, contudo, gera um grande excedente, denominado pela autora como "superávit comportamental".

As informações obtidas, então, passam a ser matéria-prima na criação de produtos de predição, os quais antecipam o comportamento do usuário através das informações previamente disponibilizadas. Tem-se, assim, o desenvolvimento de um mercado de comportamentos futuros, cuja matéria-prima pode envolver desde simples ações na rede até a voz, personalidade e emoções dos indivíduos. Todo esse contexto, por certo, não seria possível sem a utilização de tecnologias e algoritmos ditos "inteligentes", cuja atuação é automatizada.

Ocorre que - mais do que conhecer e prever condutas - a tecnologia utilizada passou a moldar comportamentos em larga escala, instrumentalizando a experiência humana. Segundo Zuboff (2021), a principal inventora e aperfeiçoadora da forma de capitalismo descrita foi a Google, sendo seguida por Facebook (Meta), Microsoft e Amazon. A primeira teve sua atuação inicial beneficiada pela ausência de legislação específica sobre o tema e de concorrentes, além da predisposição governamental quanto a novos mecanismos de vigilância, sendo pioneiro no tipo de serviço disponibilizado.

Nesse sentido, a empresa é um dos maiores exemplos dessa nova realidade social, porque afeta "nós", "o mundo" e "o conhecimento", daí porque se fala em "googlelização de tudo", já que "ao catalogar nossos juízos individuais e coletivos, nossas opiniões e (ainda mais importante) nossos desejos, a empresa também vai se transformando numa das mais importantes instituições globais" (VAIDHYANATHAN, 2011, p. 14). A Google, assim, "impôs a lógica da conquista, definindo a experiência humana como livre para ser apossada, disponível para ser compilada na forma de dados e reivindicada como ativos de vigilância" (ZUBOFF, 2021, p. 405).

Durante a ascensão desses agentes, ainda, foram criadas diversas formas de coleta e armazenamento de dados, o que incluiu *cookies*, *web beacons*, *spywares*, *tagging* e *tracking*, dentre outros, instrumentos esses que se encontram espalhados nos mais diversos ambientes da rede. Sua função, nessa lógica, consiste na extração da matéria-prima essencial para o

sistema, possibilitando a análise do comportamento humano e a criação de "perfis de usuários" (PESSOA, 2020, p. 39). Essa nova lógica, como dito anteriormente, inicia pelo "*superávit comportamental* descoberto mais ou menos já pronto no ambiente on-line, quando se percebeu que a *data exhaust* que entupia os servidores do Google podia ser combinada com as suas poderosas capacidades analíticas para gerar predições de comportamento do usuário" (ZUBOFF, 2021, p. 405).

No caso do Facebook (Meta), o funcionamento do seu sistema ocorre, segundo estudo realizado pelo laboratório Share Lab (2016), em quatro partes, quais sejam a extração de dados, armazenamento, processo algorítmico e determinação do alvo. Nesse contexto, destaca-se que a referida coleta de dados tem origem em cinco fontes principais: informações da conta, ações e comportamentos, *trackers*, informações fora do domínio do Facebook e informações do dispositivo (CARIBÉ, 2019, p. 04).

Na sequência, os dados obtidos são armazenados e processados para tornar possível a definição do perfil do usuário, o que se dá através de *machine learning* e *deep learning*[2], extraindo-se o perfil psicométrico do indivíduo, além de sua posição política, rotina, valores e princípios, dentre outros. Isso feito, analisa-se as suas conexões, interesses, comportamentos e demais informações relevantes, do que resulta o conteúdo que será destinado ao *feed* específico do usuário, cujo teor envolve questões que se apresentam dentro do seu espectro de pensamento e outras que vão de encontro às suas inclinações, ocorrendo também a venda do perfil de conhecimento e consumo obtido a anunciantes interessados na sua utilização.

Dessa forma, verifica-se a problemática envolvida na extração do comportamento e informações dos usuários, o que pode englobar desde informações básicas da conta até dados obtidos pela utilização de funções do próprio *smartphone* do indivíduo, tais como câmeras, microfones e sensores de geolocalização. Acerca disso, salienta-se que a preocupação quanto ao superávit comportamental obtido junto aos usuários independe do grau de relevância dos dados que o constitui, uma vez que mesmo a mais básica das informações pode ser utilizada para diversos fins, principalmente se combinada com outras anteriormente coletadas.

Os preceitos a serem colocados em pauta, então, passam a ser a perda da autonomia individual do ser humano e a ausência de privacidade, direitos básicos que estariam garantidos a todos. Conforme expõe David Lyon (2018, p. 153), a vigilância "não é mais

[2] Nesse sentido, "basicamente, machine learning (aprendizado de máquina) e deep learning (aprendizagem profunda) são pilares da IA. Em primeiro lugar, machine learning diz respeito ao uso de algoritmos para organizar dados, reconhecer padrões e fazer com que computadores possam aprender. Isso para gerar insights inteligentes sem necessidade de pré-programação. Já o deep learning é a parte do aprendizado de máquina que, por meio de algoritmos de alto nível, reproduz a rede neural do cérebro humano. Em resumo, podemos dizer que machine learning estabeleceu as bases para deep learning evoluir." (PUCRS ONLINE, 2020).

apenas algo externo que se impõe em nossa vida", mas "algo que os cidadãos comuns aceitam – deliberada e conscientemente ou não –, com que negociam, a que resistem, com que se envolvem e, de maneiras novas, até iniciam e desejam". Nessa lógica, o autor cunhou o termo "cultura de vigilância", que descrevia o estado atual da sociedade, onde tanto o vigiado e o vigilante contribuem para a observação.

O filósofo, além do exposto, preceitua que, em razão da crescente digitalização das relações sociais, os sujeitos deixaram de existir apenas como vigiados ou meros portadores de instrumentos de vigilância, mas também como participantes ativos e conscientes da sua realização. Para explicar essa situação, sua obra dispõe acerca dos fatores principais da ocorrência desse fenômeno, senão vejamos:

> Há dois fatores principais. O primeiro tem a ver com a aquiescência generalizada em relação à vigilância. Embora tentativas de resistir à vigilância em certos ambientes sejam relativamente comuns, na maior parte dos cenários e do tempo ela se tornou tão disseminada que a maioria a aceita sem questionar. Essa aliança generalizada com a vigilância contemporânea é algo que intriga aqueles que atravessaram regimes de vigilância de governos autoritários. Mas tal aquiescência pode ser explicada por meio de três fatores bastante lugares-comuns: familiaridade, medo e diversão. (LYON, 2018, p. 160).

Assim, o sistema de controle dos indivíduos é espalhado pelo tecido social, tendo, atualmente, como principal instrumento, os dados gerados na internet e outros espaços. Nessa linha, há de se questionar o tratamento de tais informações, além das responsabilidades envolvidas na sua proteção.

Dentro disso, vive-se atualmente uma era de evolução do modelo panóptico anteriormente estabelecido, o qual, nas palavras de Zygmunt Bauman, "está vivo e bem de saúde, na verdade, armado de músculos (eletronicamente reforçados, ciborguizados) tão poderosos que Bentham, ou mesmo Foucault, não conseguiria nem tentaria imaginá-lo" (BAUMAN, 2013, p. 42). Há, então, o desenvolvimento de um novo modelo, denominado como superpanóptico, cujas bases são retiradas do antigo sistema, porém ultrapassa os limites anteriormente vigentes, tendo em vista o uso e desenvolvimento das novas tecnologias de informação e comunicação (PESSOA, 2021, p. 73).

O que se vê, na verdade, é uma grande coleta de dados e informações dos indivíduos, os quais, muitas das vezes, sequer possuem noção do que estão disponibilizando à rede. A coleta de dados, junto disso, não se restringe somente aos entes privados e *big techs*, uma vez que os mais diversos Estados, além de coletar dados da sua própria população, também passaram a obter informações de outros países, o que deu origem a diversos programas de vigilância em massa. Isso, como já dito, sempre foi justificado por ameaças externas, tais

como o combate ao crime organizado, ao tráfico de drogas e, mais recentemente, ao terrorismo.

Sobre a referida extração de dados, Zuboff (2018, p. 28-29) refere que as informações que constituem o *big data*[3] são obtidas a partir de quatro fontes principais, quais sejam aquelas derivadas de transações econômicas realizadas na rede de internet, sensores acoplados a objetos, corpos e lugares, câmeras de vigilância públicas e privadas, além de outras oriundas de bancos de dados governamentais e corporativos.

Segundo a autora, a propósito, a última fonte apresentada demonstra o caráter heterogêneo e transemiótico da extração de dados. O Google Street View, a exemplo, extrai muito mais que dados de georreferenciamento e imagens de onde circula, conforme processo movido por 39 Estados estadunidenses contra a empresa. Em resumo, consoante descrito pelo Epic (Electronic Privacy Information Center), o Google teria utilizado o serviço para coleta não autorizada de dados de redes sem fio, o que incluiria aqueles provenientes de redes de wi-fi privadas e residenciais. A empresa, em razão do vazamento, se viu obrigada a reforçar sua política de privacidade e ainda sofre com restrições em várias regiões, além de outros processos (ZUBOFF, 2018, p. 30).

Em alusão ao que Siva Vaidhyanathan (2011, p. 17) chamou de "imperialismo de infraestrutura", Zuboff (2018) ressalta que o Google adentra países e regiões sem qualquer permissão, coletando dados e informações do local e seus cidadãos, o que acaba por gerar processos judiciais e pagamento de multas, as quais, contudo, não lhe trazem grandes prejuízos frente aos resultados obtidos com os dados coletados. Apesar de haver oposição, a empresa também conta com apoio de seus usuários, que se sentem beneficiados pela plataforma, senão vejamos:

> Para a grande maioria dos usuários do Google, serviços como o Street View são mais benéficos do que prejudiciais. Os poucos que podem sentir-se agredidos pelas diretrizes padrão e universais do Google não são muito importantes para a empresa. Afinal, nós não somos clientes do Google: somos seus produtos. O Google tem condições de alienar alguns milhares de pessoas porque, para a maioria conectada à cultura global cosmopolita da Internet, viver sem o Google tornou-se algo impensável. Para cada internauta que reclama do Street View, há milhões de outros que o consideram extremamente útil. (VAIDHYANATHAN, 2011, p. 149).

Dessa maneira, a cultura de vigilância é reforçada pelos próprios vigiados, vez que

---

[3] A expressão *big data* é um "termo em evolução que descreve qualquer quantidade volumosa de dados estruturados, semiestruturados ou não estruturados que podem ser explorados para se obterem informações. A primeira propriedade envolvendo Big Data consiste no volume crescente de dados. Pesquisa recente da Cisco estima que, nos próximos anos, a medida em gigabytes será superada e o cálculo da quantidade de dados será feito na ordem zettabyte e até mesmo em yottabyte" (MAGRANI, 2019).

estes assumem os perigos da ausência de privacidade frente à utilidade e/ou facilidade trazida por determinada ferramenta. Além disso, tem-se uma quinta fonte para extração de dados, qual seja a realização de ações não mercantis, que representam o *small data*, tal como ações e discursos gerados pelos indivíduos na utilização das plataformas. Sendo assim, todos os impulsos produzidos pelos usuários são armazenados por empresas, mesmo que aparentemente não possuam a importância necessária para tal.

Com isso, verifica-se uma quebra no modelo capitalista dos últimos anos, onde o trabalhador era também consumidor e, por tal, deveria ser suficientemente valorizado. Atualmente, os clientes das *big techs* são anunciantes e outros agentes que necessitam da análise de dados disponibilizada por tais empresas. Quebra-se, então, com a dependência empresarial em relação à população, que tem suas exigências e supervisão menos consideradas.

Inobstante, é necessário salientar que os dados tratados e utilizados de forma comercial pelas grandes empresas de tecnologia são obtidos através de constantes operações automatizadas, do que resulta um novo tipo de ativo do mercado: os ativos de vigilância. Há, contudo, certa crítica quanto à sua extração, já que tais ativos são obtidos sem a permissão dos usuários, os quais também não são suficientemente beneficiados após a sua obtenção. Assim, a posse das informações extraídas tornou-se um grande atrativo de investimentos, do que se desenvolveu o atual capitalismo de vigilância, já que o modelo de negócio adotado por empresas como a Google veio a ser o padrão aplicado no setor econômico.

Sendo assim, faz-se importante questionar a vigilância que se desenvolve no setor econômico, além do seu entrelaçamento com as entidades públicas. Nessa linha, é imperioso o fortalecimento das instituições com foco na transparência frente ao contexto apresentado, além dos próprios indivíduos, vez que a nova forma de capitalismo em ascensão não depende de reciprocidade com as massas - já que apenas se utiliza dos dados que extrai destas -, o que pode vir a fragilizar as democracias pelo mundo, inclusive no Brasil.

2.3. PANORAMA SOBRE O (DES)CONHECIDO SISTEMA DE VIGILÂNCIA DO BRASIL

No ano de 2002, passou a funcionar no Brasil o Sistema de Vigilância da Amazônia (SIVAM), parte integrante do Sistema de Proteção da Amazônia (SIPAM). Sua execução veio a ser realizada por um convênio entre o governo brasileiro e a empresa estadunidense Raytheon, que contou com o patrocínio e recomendação dos Estados Unidos da América

(BRASIL, 2004), sendo-lhe atribuída a responsabilidade pelo controle ambiental, desenvolvimento regional, controle do tráfego aéreo, coordenação de emergências, monitoramento das condições meteorológicas e o controle de ações de contrabando.

Como um dos objetivos do programa, destaca-se a integração de informações obtidas pelos mais diversos agentes atuantes na Amazônia. O funcionamento desse sistema, assim, buscou a criação de base de dados completa e compartilhada por todos os órgãos atuantes na floresta. A parceria estabelecida com a empresa estadunidense, todavia, gerou uma série de questionamentos referentes ao risco envolvido na influência não nacional sobre a segurança da Amazônia, tendo em vista os interesses econômicos ali envolvidos, além levantar suspeitas da utilização do programa Echelon para benefício da referida companhia no processo de escolha pelo governo brasileiro (LOURENÇÃO, 2013).

O uso do referido sistema, no entanto, revelou a necessidade de maior controle dos dados obtidos no âmbito nacional, em destaque pela possibilidade de tratamento por outros países, além do seu compartilhamento irrestrito entre órgãos governamentais. Quanto à suspeita de utilização do programa Echelon, salienta-se que este não é o único caso desse tipo de espionagem no país.

Conforme revelado pelo site WikiLeaks em 2015, o governo estadunidense, através da sua Agência Nacional de Segurança (NSA, na sigla em inglês), também grampeou a ex-presidente Dilma Rousseff, além de ex-ministros e do próprio avião presidencial, o que totalizou o monitoramento de 29 telefones do governo e aliados (EUA…, 2015). Na época, o episódio ganhou destaque e criou certa crise diplomática entre Brasil e Estados Unidos, o que veio a ser posteriormente minimizado pela então presidente brasileira. O caso, entretanto, serviu de alerta para a vigilância exercida por outros países, além de levantar suspeitas acerca de outros casos de monitoramento não revelados.

Especificamente no âmbito brasileiro, o órgão que exerce papel semelhante à NSA (ou, pelo menos, similar à CIA) é a Agência Brasileira de Inteligência (ABIN), criada em 1999, pela Lei nº 9.883 - embora existisse de fato desde 1995 (CARPENTIERI, 2017, p. 16), com ampla participação militar. Isso, inclusive, foi alvo de diversas críticas desde a sua criação, sendo a ABIN considerada como a sucessora do SNI (Serviço Nacional de Informação), criado em 1964. Segundo o site oficial do governo federal, ainda, o órgão tem como função "fornecer ao presidente da República e a seus ministros informações e análises estratégicas, oportunas e confiáveis, necessárias ao processo de decisão" e, também, "assegurar que o Executivo Federal tenha acesso a conhecimentos relativos à segurança do Estado e da sociedade, como os que envolvem defesa externa, relações exteriores, segurança

interna, desenvolvimento socioeconômico e desenvolvimento científico-tecnológico" (BRASIL, 2020).

O artigo 4º da Lei nº 9.883/1999, nessa linha, descreve as atividades de competência da entidade, sendo elas: I - planejar e executar ações, inclusive sigilosas, relativas à obtenção e análise de dados para a produção de conhecimentos destinados a assessorar o Presidente da República; II - planejar e executar a proteção de conhecimentos sensíveis, relativos aos interesses e à segurança do Estado e da sociedade; III - avaliar as ameaças, internas e externas, à ordem constitucional; IV - promover o desenvolvimento de recursos humanos e da doutrina de inteligência, e realizar estudos e pesquisas para o exercício e aprimoramento da atividade de inteligência (BRASIL, 1999).

No entanto, muito se questiona a competência da ABIN, sua área de atuação a nível nacional e global, além da crescente militarização durante seus anos iniciais e, principalmente, utilização para fins políticos - o que já veio a ocorrer -, conforme expõe José Rafael Carpentieri:

> Além da crescente militarização nos anos seguintes à sua criação, a Agência Brasileira de Inteligência, logo após o seu surgimento e até o momento, passou por diversos episódios que revelaram a sua atuação na espionagem política (ZAVERUCHA, 2008, p. 184). Dentre os fatos, os mais relevantes são: o caso do "Grampo do BNDES", que resultou em um processo criminal perante a Justiça Federal; a suspeita de espionagem do ex-presidente Itamar Franco; a atuação da Abin no chamado "Dossiê Cayman", uma falsa denúncia de contas ilegais no exterior; a atuação nos Correios, constatada durante as investigações de uma Comissão Parlamentar de Inquérito; e a Operação Satiagraha, conduzida pela Polícia Federal e anulada pelo Poder Judiciário em virtude da participação de agentes da Abin. Em 2013, ocorreu a exoneração de um agente da agência sob argumento de quebra de sigilo funcional. Os detalhes do caso não foram divulgados, mas as notícias deram conta de que houve o repasse de informações à CIA norte-americana. Além dos casos envolvendo a Abin, no intervalo de tempo entre a extinção do SNI e a criação da Abin, outros casos de espionagem política foram constatados envolvendo órgãos de inteligência militares. O Centro de Informações da Marinha – antigo Cenimar, órgão com grande atuação na repressão política durante o regime militar – admitiu abertamente monitorar o Movimento dos Trabalhadores Sem-Terra por meio de agentes infiltrados (BRANDÃO, 2002, p. 101). O órgão, ao qual seus dirigentes militares faziam referência pelo antigo nome, também reconheceu possuir um dos maiores arquivos sobre a vida de pessoas no Brasil e monitorar políticos para saber se são simpáticos aos interesses da Marin (CARPENTIERI, 2017, p. 17).

São diversos os casos polêmicos envolvendo a entidade. Mais recentemente, foi revelado, pelo The Intercept Brasil, a intenção da ABIN em adquirir, junto ao Serviço Federal de Processamento de Dados (SERPRO), dados e fotografias de mais de 76 milhões de brasileiros que possuem Carteira Nacional de Habilitação (CNH). O pedido levantou suspeitas acerca de possíveis desvios na utilização das informações obtidas e quanto à atuação da entidade, que não negou ter solicitado as informações mencionadas (DIAS; MARTINS,

2020). A questão, além disso, foi levada ao Supremo Tribunal Federal, através da ADPF nº 695, que será tratada mais adiante.

Junto disso, em 2016, a mesma agência de notícias expôs a atuação do GEO-PR (Sistema Georreferenciado de Monitoramento e Apoio à Decisão da Presidência da República), tratando sobre um megabanco de dados criado em 2005 para apoiar processo de concessão de exploração mineral, o qual veio a ser transformado pelo Gabinete de Segurança Institucional (GSI) e Agência Brasileira de Inteligência (ABIN) em uma poderosa ferramenta de vigilância de movimentos sociais. Oficialmente, o sistema foi desconstituído e seus dados doados à ABIN para reaproveitamento, sendo tal ação considerada, por Priscila Carlos Brandão Antunes (apud FIGUEIREDO, 2016), como "uma estratégia dos militares para assegurar acesso e controle sobre um conjunto determinado de dados".

Outrossim, após o decreto que oficializou a atuação da ABIN, também foram editadas outras regulações no que se refere ao sistema de inteligência brasileiro, conforme elucida Pedro Augusto P. Francisco e Jamila R. Venturini:

> O Decreto 4.376/2002 detalhou ainda a organização e o funcionamento do sistema de inteligência brasileiro, sobretudo em relação à sua composição. [...] Alguns dos parâmetros relevantes para as atividades do sistema de inteligência são descritos no Decreto 3.505/2000 que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal; na Lei 8.159/91, que dispõe sobre a política nacional de arquivos públicos e privados e no Decreto 7.845/2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informações confidenciais com qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento. Apesar de ser mencionado explicitamente em ambas as normas, o Brasil passou mais de duas décadas sem uma política nacional específica para inteligência.41 Esse cenário só veio a se alterar em 2016, com a sanção do Decreto Presidencial 8.793, que define a Política Nacional de Inteligência (FRANCISCO; VENTURINI, 2017, p. 11-12).

Entretanto, em que pese as diversas regulações na área de vigilância, a ABIN carece de regulamentos específicos acerca dos procedimentos que deve adotar, o que pode culminar na realização de atos de vigilância sobre os indivíduos. Ainda, carecem de melhores contornos as obrigações de transparência prestação de contas por parte da agência. Tal contexto, há de se enfatizar, é oriundo da ausência de regulamentos específicos das atividades de inteligência no país após a redemocratização em 1985, situação que gerou a ocupação desse espaço por diversos entes públicos e privados (FRANCISCO; VENTURINI, 2017).

Apesar dos casos mencionados, não é de amplo conhecimento público no país a existência de grandes programas de vigilância, inclusive a nível mundial, como visto na seção anterior, existindo poucos conhecidos que atuam em território nacional. É o caso dos sistemas Córtex e Pandora, o primeiro desenvolvido e utilizado pelo Ministério da Justiça e o segundo

pelo Ministério Público, nas Procuradorias espalhadas pelo território brasileiro.

Ademais, existem programas semelhantes aos mencionados, que foram sondados pelo governo brasileiro e/ou ainda não apresentam pleno funcionamento, como *Pegasus* e *Harpia*, este último, inclusive, foi recentemente contratado pelo governo brasileiro, constituindo uma perigosa ferramenta de monitoramento de pessoas via internet[4]. Apesar disso, segundo reportagem do Uol Notícias, a intenção presidencial era a de adquirir o *spyware Pegasus*, muito mais poderoso e com atuação na espionagem de celulares e computadores em todo o globo. O Tribunal de Contas da União, todavia, atuou de perto no processo licitatório, o que, conjuntamente com a repercussão na mídia, acabou causando a desistência da empresa detentora do programa, a NSO Group, de origem israelense (VALENÇA, 2021).

O Córtex, por sua vez, conforme matéria divulgada pelo The Intercept Brasil (REBELLO, 2020), constitui-se como "uma tecnologia de inteligência artificial que usa a leitura de placas de veículos por milhares de câmeras viárias espalhadas por rodovias, pontes, túneis, ruas e avenidas país afora para rastrear alvos móveis em tempo real." Além disso, o sistema "também possui acesso em poucos segundos a diversos bancos de dados com informações sigilosas e sensíveis de cidadãos e empresas, como a Rais, a Relação Anual de Informações Sociais, do Ministério da Economia" (REBELLO, 2020).

Essa tecnologia, nessa linha, permite que o Estado brasileiro tenha acesso a diversas informações dos indivíduos que fazem parte de empresas, o que incluiria dados cadastrais básicos e outras informações disponibilizadas pelos cidadãos (CPF, endereço, salário, dependentes e etc.). À vista disso, a reportagem mencionada aponta que, apesar da ferramenta descrita se mostrar uma importante arma contra o crime, o seu uso também pode ser traduzido em uma ferramenta de vigilância sobre os brasileiros.

Como se verifica, um dos principais perigos oriundos do uso da referida ferramenta é o cruzamento de dados com outros órgãos governamentais. Segundo a matéria, diversas informações podem ser obtidas a partir da placa de um carro, tais como "sua movimentação pela cidade, com quem você se encontrou, quem te acompanhou nos deslocamentos e quem te visitou" e, somado a isso, os agentes responsáveis pelo sistema "também podem cruzar esse

[4] Conforme o Data Privacy Basil (2022): "em 19 de maio de 2021, o Ministério da Justiça e Segurança Pública lançou o Edital de Licitação n. 03/2021, da modalidade pregão eletrônico, com objetivo de atender as necessidades operacionais da Diretoria de Inteligência da Secretaria de Operações Integradas. Conforme descrito no subitem 1.1. do Edital, o objeto do certame envolvia: '(…) a escolha da proposta mais vantajosa para a aquisição de Solução de Inteligência em Fontes Abertas, Mídias Sociais, Deep e Dark Web compreendendo o fornecimento, instalação e configuração, bem como o suporte técnico, em atendimento às necessidades operacionais da Diretoria de Inteligência da Secretaria de Operações Integradas (DINT/SEOPI)'. [...]. Da abertura da sessão pública, resultou vencedora a empresa Harpia Tecnologia Eireli (Harpia Tech), que ofereceu o menor lance pelo produto, no valor total de R$ 5.415.750,00 (cinco milhões, quatrocentos e quinze mil, setecentos e cinquenta reais)." (ZANATTA, 2022).

histórico com informações pessoais e dados de emprego e salários, incluindo boletins de ocorrência e passagens pela polícia" (REBELLO, 2020).

Os dados obtidos, então, são acessados por diversos servidores das forças de segurança e inteligência a nível federal, estadual e municipal. Além disso, o seu uso e compartilhamento não foram corretamente regulamentados desde a sua criação, o que originou alguns escândalos no que concerne à investigações de cunho político, além da sua utilização em outras oportunidades, tais como eleições e eventos esportivos.

Conforme alerta Manoel Galdino, diretor-executivo da Transparência, em entrevista à Revista Crusoé, a tecnologia discutida pode significar diversos perigos aos cidadãos no caso de sua má utilização ou ausência de controle (GULARTE, 2022). Nesse sentido:

> Não há controle nenhum de quem acessa e os motivos pelos quais irá acessar. Isso é o mais grave. Com a quantidade de dados ofertados, poderá abrir brecha para perseguição de opositores e uso para fins pessoais. O próprio crime organizado pode ter acesso à ferramenta. Basta que haja um policial corrupto com acesso. A falta de um sistema para prevenir isso nos deixa bastante expostos. (GULARTE, 2022).

A revista ainda destaca que, por ser um programa de uso policial, o sistema deveria ser submetido à análise e controle do Ministério Público, além da devida fiscalização pelo Congresso Nacional, a partir da CCAI (Comissão de Controle da Atividade de Inteligência), dada a natureza da ferramenta (GULARTE, 2022).

Ainda, a plataforma em questão, segundo o The Intercept Brasil, teria como origem outros sistemas adotados pelo Poder Público, em destaque aqueles criados a partir do ano de 2014 (REBELLO, 2020). Nesse período, o governo federal criou o Centro Integrado de Comando e Controle Nacional, o qual possuía informações acerca das cidades-sede da realização da Copa do Mundo no país. Assim, foram obtidas imagens em tempo real disponibilizadas por câmeras em vias públicas e de segurança espalhadas pelos locais-sede, sob o argumento de que fossem evitados eventuais ataques terroristas, do crime organizado ou de manifestações (REBELLO, 2020).

Mais adiante, em 2015, um decreto presidencial organizou e oficializou o uso da plataforma Alerta Brasil, que já era utilizada pela Polícia Rodoviária Federal desde 2013 e, posteriormente, foi integrada ao Córtex, sendo uma das suas tecnologias precursoras (REBELLO, 2020). Após, já em 2018, foi criado o Sistema Único de Segurança Pública (SUSP) - cujas determinações estabeleciam o compartilhamento de diversos dados oriundos das secretarias de segurança estaduais com o Ministério da Justiça, além de parcerias com municípios, sendo que o estado que não o fizesse sofreria com o não repasse de verbas federais para segurança pública (REBELLO, 2020). Esse conjunto de órgãos e sistemas,

assim, contribuíram para criação e ampliação do sistema Córtex, que se encontra em pleno funcionamento nos dias atuais.

Junto disso, como mencionado, tem-se no país a utilização do sistema Pandora, o qual foi idealizado, desenvolvido e implementado pelo Ministério Público da Paraíba (MPPB), através do seu Núcleo de Gestão do Conhecimento e Segurança Institucional, sendo utilizado como apoio às investigações desenvolvidas pelo MPPB. A plataforma, em resumo, tem como principal objetivo a disponibilização da análise de um grande número de dados ao sistema de Justiça, o que permitiria a detecção de "riscos de crimes contra a administração pública", consoante informa a própria página do órgão (PARAÍBA, 2021).

Segundo o jornalista Suetoni Souto Maior (2022), o referido sistema "consegue cruzar milhares de informações para auxiliar na elucidação de crimes que vão desde desvio de recursos públicos, a questões como sonegação, processos criminais e muitas outras aplicações". A ferramenta, ainda, é capaz de obter informações acerca de conexões e inquéritos policiais a partir da coleta de dados de DNA do suspeito, o que demonstra o seu poder de atuação.

Em cartilha emitida pelo Conselho Nacional do Ministério Público no ano de 2021, inclusive, é destacado que a ferramenta já estaria sendo operada pelo Ministério Público de outras unidades federativas, como os do Rio de Janeiro, Paraná, Rio Grande do Sul e Espírito Santo (CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO, 2021). A problemática, contudo, é verificada em razão da ausência de mais informações acerca da utilização do sistema Pandora, uma vez que não há previsão legal específica para tal, além da ausência de explicações detalhadas do seu funcionamento e da composição dos dados analisados, o que não seria disponibilizado por questões de segurança.

Nessa lógica, não se verifica exatidão quanto à extensão do sistema, quais dados são utilizados e de onde são obtidos. Ainda, não há especificação no que concerne aos órgãos que possuem acesso à plataforma, bem como acerca dos dados que podem ser cruzados de forma sistemática. De maneira geral, portanto, a utilização do Pandora, mesmo que apenas para os fins descritos pelo MPPB, ocorre de forma arbitrária, podendo se dar de forma a exercer vigilância sobre os cidadãos.

Aliado à isso, mais especificamente no âmbito do Estado do Rio Grande do Sul, local onde a presente pesquisa é realizada, foi implementado em 2004 o Sistema de Consulta Integradas - CSI, cujo funcionamento "permite que consultas sobre identificação de indivíduos sejam realizadas através da Internet, a partir de um único acesso, que integra e automatiza a pesquisa às diferentes bases de dados e sistemas do Estado do Rio Grande do

Sul" (RIO GRANDE DO SUL, 2004). A Secretária de Segurança Pública do RS é o órgão responsável pelo programa, o qual incluiu dados disponibilizados pela Brigada Militar, DETRAN, IGP, Polícia Civil, Tribunal de Justiça e SUSEPE, dentre outros.

O foco do sistema, nesse sentido, é a cooperação para o auxílio na "na busca de pistas, características, e ocorrências relacionadas a suspeitos". Em sua base de dados, é possível a pesquisa em três categorias: indivíduos, detentos e visitantes, o que demonstra que sua atuação pode exceder o sistema penitenciário e de segurança. O acesso e compartilhamento de informações definidas como de segurança pública, ademais, também é feito em parceria com municípios do Estado e outros órgãos, os quais, em 2010, já totalizavam 49 usuários (SISTEMA…, 2010). O funcionamento do sistema, no entanto, também carece de maior transparência, sendo de difícil obtenção maiores informações a seu respeito.

Além do exposto, é necessário trazer à baila as ações governamentais que se sucederam ao início da pandemia de COVID-19 no país, em 2020. Como é de amplo conhecimento público, a época mencionada exigiu rápidas medidas de restrição à circulação de pessoas e distanciamento social, a fim de evitar aglomerações e diminuir a curva de contágio da doença, pelo que tornou-se imperiosa a realização de controle, fiscalização e vigilância epidemiológica sobre os cidadãos.

Dentro desse contexto, sobrevieram leis que, embora demandassem uma reflexão maior, foram editadas dentro de um período de pandemia que exigia celeridade. Nessa linha, foi publicada, na época, a Lei nº 13.979/2020, que, em seu artigo 6º, determinou a obrigatoriedade do compartilhamento de dados de pessoas infectadas ou com suspeita de infecção pelo coronavírus pelos órgãos e entidades da Administração Pública federal, estadual, distrital e municipal, a fim de, exclusivamente, evitar a sua propagação (BRASIL, 2020)[5].

Não se discute aqui a legitimidade do Poder Público na execução da vigilância epidemiológica, que é importante, mas é preciso ponderar os riscos à privacidade dos cidadãos no seu desempenho, principalmente no que concerne ao compartilhamento de dados dos indivíduos. A saber, o Estado de São Paulo, a fim de monitorar o cumprimento da

[5] Art. 6º É obrigatório o compartilhamento entre órgãos e entidades da administração pública federal, estadual, distrital e municipal de dados essenciais à identificação de pessoas infectadas ou com suspeita de infecção pelo coronavírus, com a finalidade exclusiva de evitar a sua propagação.
§ 1º A obrigação a que se refere o caput deste artigo estende-se às pessoas jurídicas de direito privado quando os dados forem solicitados por autoridade sanitária.
§ 2º O Ministério da Saúde manterá dados públicos e atualizados sobre os casos confirmados, suspeitos e em investigação, relativos à situação de emergência pública sanitária, resguardando o direito ao sigilo das informações pessoais. (BRASIL, 2020).

quarentena no estado durante o período de maior contágio da doença, firmou parceria com as principais empresas de telefonia do país e utilizou-se de suas infraestruturas para tal, o que incluiu dados que permitiram a identificação de locais com aglomeração no estado (SÃO PAULO…, 2020).

Por fim, o governo federal editou a Medida Provisória nº 954/2020, cujos dispositivos permitiam o compartilhamento de dados por empresas de telefonia fixa imóvel com o Instituto Brasileiro de Geografia e Estatística (IBGE), a fim de possibilitar a produção estatística oficial durante a pandemia, já que sua execução restou prejudicada pelo período de crise. A Medida Provisória, todavia, teve seus efeitos suspensos pelo Supremo Tribunal Federal através de medidas cautelares deferidas pela ministra Rosa Weber em cinco Ações Diretas de Inconstitucionalidade (ADIs 6387, 6388, 6389, 6390 e 6393), tendo em vista que suas determinações violavam o direito constitucional à intimidade, à vida privada e ao sigilo de dados (BRASIL, 2020), decisão que foi posteriormente referendada pelo Tribunal.

Isto posto, verifica-se que os sistemas de vigilância brasileiros possuem certo grau de desenvolvimento e capacidade de rápida evolução em determinados cenários, apesar de carecerem de maior regulamentação e transparência. O risco da utilização das plataformas e dispositivos descritos para fins políticos e/ou de vigilância, com efeito, é a grande problemática advinda do cenário descrito, o que veio a ser limitado, suficientemente ou não, pela Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), que será melhor explorada mais adiante.

3. O DIREITO À PROTEÇÃO DE DADOS PESSOAIS E A REFUNDAÇÃO DA PRIVACIDADE NO ORDENAMENTO JURÍDICO BRASILEIRO

A vigilância estatal, conforme dito anteriormente, está inserida na sociedade através de diversos dispositivos e sistemas que buscam a manutenção do poder e controle sobre os cidadãos. Com o desenvolvimento das novas tecnologias de informação e comunicação, no entanto, a observação realizada pelos entes públicos adquiriu novos rumos e desenvolveu-se de maneira acelerada, inclusive no Brasil, havendo importante parcela de contribuição de agentes privados - em destaque as *big techs* -, considerando a massiva quantidade de dados que obtêm dos indivíduos. Atualmente, assim, os dados pessoais atingiram um novo patamar de importância, sendo imperiosa a devida regulação sobre a sua proteção, especialmente no combate à vigilância indevida.

Pretende-se compreender, nessa linha, as origens do direito à proteção de dados pessoais, desde sua construção a nível internacional, em destaque no que concerne à Convenção nº 108 para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais, elaborada em 1981, além de outros diplomas que a sucederam, mas, com destaque na promulgação do Regulamento Geral de Proteção de Dados da União Europeia (RGPD).

Considerando o contexto apresentado, há de analisar o atual estágio de desenvolvimento da legislação brasileira no que concerne à proteção de dados pessoais, bem como o processo percorrido para sua caracterização como direito fundamental autônomo, com a inclusão no rol de direitos e garantias individuais na Constituição Federal do Brasil, especialmente a partir da promulgação da Lei Geral de Proteção de Dados Pessoais.

Faz-se necessário explorar, a partir do método de procedimento histórico, o processo de desenvolvimento do direito à privacidade até o entendimento de um direito à proteção de dados pessoais, seguido dos marcos normativos sobre o tema. Por derradeiro, averiguado o desenvolvimento do direito que a baseia e dos diplomas que lhe servem como alicerce, analisar-se-á a legislação brasileira no que concerne à proteção de dados pessoais.

3.1. DO DIREITO À PRIVACIDADE AO DIREITO À PROTEÇÃO DE DADOS PESSOAIS

Inicialmente, há de se analisar a refundação do direito à privacidade e, posteriormente, do direito à proteção de dados pessoais. Nesse sentido, a distinção entre o público e o privado,

por certo, data de muito antes dos conceitos mencionados. Segundo Cancelier (2017, p. 02), a Antiguidade Clássica teria sido definida por Habermas como o ponto de partida para diferenciação entre as duas esferas, sendo a *pólis* um âmbito comum aos cidadãos livres e a chamada *oikos* a parte particularizada aos indivíduos. Tais conceitos mantinham muita relação com a vida política dos cidadãos das sociedades da época, inexistindo a percepção de um direito à privacidade como percebido atualmente, mesmo que em relação ao conceito de "privado".

Apesar de discussões anteriores, a percepção acerca do tema no sentido atual tomou maior importância a partir da publicação, em 1890, do artigo "The right to privacy", escrito em colaboração por Samuel Warren e Louis Brandeis, ambos estadunidenses. O texto, de maneira geral, buscou modificar a visão atribuída ao direito à privacidade, retirando-lhe de discussões a nível de propriedade e o aproximando da necessidade de maior proteção à vida privada, além de trazer maior relação com a personalidade humana (PESSOA, 2020, p. 60).

Os autores, nessa perspectiva, trouxeram à tona o direito de ser deixado só, principalmente em decorrência da evolução das novas tecnologias de informação e comunicação, devendo ser garantida a proteção da vida privada e o direito de não torná-la pública (BRANDEIS; WARREN, 1890). A publicação, dessa maneira, constituiu um importante marco à discussão acerca do direito à privacidade, cuja conceituação, apesar das diversas concepções acerca do tema, foi descrita da seguinte forma por João Pedro Seefeldt Pessoa:

> Trata-se, em apertada síntese, do direito de cada um de garantir uma paz, uma tranquilidade, uma reserva de parte de sua vida que não esteja afetada por uma atividade pública; ou de evitar que fatos de sua vida que são entendidos privados sejam expostos, devendo o Estado abster-se de interferir indevidamente em tal âmbito de cada indivíduo e, inclusive, proibir a ingerência também de terceiros. [...]. O direito à privacidade é, nessa concepção, regido por três atributos, quais sejam, a solidão, o direito de estar só; o segredo, o direito de exigir sigilo; e a autonomia, o direito de decidir sobre si mesmo. (PESSOA, 2020, p. 60-61).

Mais adiante, já no século XX, com o aumento exponencial da circulação de informações, motivado pelo crescente desenvolvimento de tecnologias de informação e comunicação, e as mudanças nos processos da sociedade com o espaço público e privado, atingiu-se uma maior democratização do direito à privacidade (CANCELIER, 2017, p. 07). Nessa lógica, essa garantia passou a ocupar outros espaços que anteriormente não faziam parte, expandindo-se a novos sujeitos.

A fim de proporcionar uma aplicação prática ao conceito de privacidade, a doutrina alemã, a partir de 1980, adotou a Teoria das Esferas, que a dividia em três classes, as quais deveriam ser observadas no formato de círculos concêntricos para analisar a qualidade de violação de uma informação pessoal. A primeira delas foi considerada a esfera da vida privada (*Privatsphäre*), que compreende as informações pessoais que não se pretende que sejam de domínio público, seguida da esfera íntima (*Intimsphäre*) - a qual diz respeito às questões que o indivíduo compartilha com pessoas de sua confiança, excluindo-se as demais; por fim, tem-se a mais restrita entre as classes, a esfera do segredo (*Geheimsphäre*), compreendia como a esfera do sigilo, da vida íntima *stricto sensu*, o que incluiria informações nunca compartilhadas ou reveladas a pessoas muito próximas (VIEIRA, 2007, p. 29-30).

Tal teoria foi utilizada de forma prática pelo Tribunal Constitucional Federal alemão (VIEIRA, 2007, p. 30), sendo posteriormente criticada em razão da sua ideia de categorização da privacidade e a subjetividade que a envolvia - apesar de sua importância para diferenciação de alguns conceitos relativos à privacidade -, senão vejamos:

> Farinho (2006, p. 45) busca na teoria alemã das esferas (que propõe um critério de valoração da privacidade) o alicerce para diferenciar intimidade da vida privada. Assim, à esfera privada corresponderiam relações de maior proximidade emocional, enquanto na esfera íntima estaria inserido o mundo intrapsíquico do sujeito. O autor faz coro às críticas constantes à ideia de categorização da privacidade, lembrando que além da "[...] dificuldade em reconduzir conteúdos a cada uma das esferas, existe a possibilidade de, pela sua fluidez, os conteúdos migrarem de uma esfera para outra". No entanto, ressalta como vantagem dessa teoria, graças aos seus fortes componentes formais, a possibilidade de tentativa de discernimento, de maneira objetiva, das esferas pública e privada. (CANCELIER, 2017, p. 10)

Em razão das críticas recebidas - e a consequente perda de credibilidade -, bem como do surgimento de inovações tecnológicas, a teoria mencionada perdeu espaço (PESSOA, 2020, p. 63). No seu lugar, então, surge a Teoria do Mosaico, cujo foco concentra-se na forma de utilização de informações, independente se pertencentes à esfera da vida íntima, privada ou pessoal. A teoria cunhada por Fulgêncio Madrid Conessa (1984) também ressalta que determinados dados podem ser considerados inofensivos se vistos de forma isolada, porém a sua análise junto a outras informações pode oferecer grave perigo ao seu titular (VIEIRA, 2007, p. 31).

Desse entendimento, extrai-se que os dados devem ser compreendidos como parte de um todo maior, devendo ser oferecida a mesma intensidade de proteção a cada um deles. Por esse ângulo, o direito à privacidade há de ser interpretado a partir da inserção dos indivíduos

na sociedade da informação[6], tendo em vista a crescente e massiva coleta e tratamento de dados que a sucede.

Nessa perspectiva, considerada a tendência de menor diferenciação entre o âmbito público e o privado, a intimidade e vida privada passaram a ser mais passíveis de violação. Assim, a autodeterminação informativa surge como o "direito de manter controle sobre as suas informações e de determinar a maneira de construir sua esfera particular", esta última compreendida como "aquele conjunto de ações, comportamentos, opiniões, preferências, informações pessoais, sobre os quais o interessado pretende manter um controle exclusivo" (KORKMAZ; SACRAMENTO, 2021, p. 03 apud RODOTÁ, 2008, p. 15, 92).

O contexto atual, dessa maneira, torna superada a lógica "pessoa-informação-sigilo", dando lugar à ideia de "pessoa-informação-circulação-controle", noção esta que concede ao indivíduo não só o direito de interrupção no fluxo de informações que lhe digam respeito, mas também de controlar a sua circulação (RODOTÁ, 2008). Assim, segundo Danilo Doneda (2011, p. 95) "por meio da proteção de dados pessoais, garantias a princípio relacionadas à privacidade passam a ser vistas em uma ótica mais abrangente", pelo que há de se considerar outros interesses, "abrangendo as diversas formas de controle tornadas possíveis com a manipulação de dados pessoas".

O desenvolvimento do direito à proteção de dados, de acordo com Doneda (2011, p. 06), deu-se em quatro estágios, conforme segue:

> O tratamento autônomo da proteção de dados pessoais é uma tendência hoje fortemente enraizada em diversos ordenamentos jurídicos e é caso emblemático de uma tendência que, a princípio, parecia apenas destinada a mudar determinado patamar tecnológico e a solicitar previsões pontuais no ordenamento, mas que, em seus desdobramentos, veio a formar as bases para o que vem sendo tratado, hoje, como um direito fundamental à proteção de dados. Esse desenvolvimento foi intenso nas cerca de quatro décadas que a disciplina ostenta. A mudança do enfoque dado à proteção de dados nesse período pode ser brevemente entrevista na classificação evolutiva das leis de proteção de dados pessoais realizada por Viktor Mayer-Scönberger, que vislumbra quatro diferentes gerações de leis que partem desde um enfoque mais técnico e restrito até a abertura mais recente a técnicas mais amplas e condizentes com a profundidade da tecnologia adotada para o tratamento de dados, em busca de uma tutela mais eficaz e também vinculando a matéria aos direitos fundamentais. (DONEDA, 2011, p. 06).

[6] "A expressão sociedade da informação define uma nova forma de organização social, política e econômica que recorre ao intensivo uso da tecnologia da informação para coleta, produção, processamento, transmissão e armazenamento de informações. Por tecnologia da informação entende-se a microeletrônica, a computação (*software* e *hardware*), as telecomunicações, a optoeletrônica, a engenharia genética e todos os processos tecnológicos interligados por uma interface e linguagem comuns, na qual a informação é gerada, armazenada, recuperada, processada e transmitida. Informação consiste em um dado ou conjunto de dados, processado ou não, em qualquer suporte, capaz de produzir conhecimento. Nesse sentido, informação pode ser uma imagem, um som, um documento físico ou eletrônico, ou, até mesmo, um dado isolado." (VIEIRA, 2007, p. 157).

O autor, dessa forma, esclarece que a primeira geração de leis a respeito do tema tratava de questões relativas à autorização para que fossem criados grandes bancos de dados e o seu posterior controle pelo Estado, também incluindo regramentos para o uso de informações pelos próprios entes públicos, isso tudo de forma mais ampla e abrangente, perspectiva que se estendeu até a edição da lei federal da República Federativa da Alemanha sobre proteção de dados pessoais em 1977. Na sequência, a segunda geração, iniciada pela Lei Francesa de Proteção de Dados Pessoais de 1978 e pelo diploma alemão já referido, veio a dar maior importância à privacidade e proteção de dados pessoais como uma liberdade negativa, que seria exercida pelo próprio cidadão (DONEDA, 2011, p. 07).

Após, a partir de 1980, uma vez compreendido que a tutela do direito à proteção de dados ultrapassa a liberdade de fornecê-los ou não - já que a participação da vida em sociedade, muitas vezes, passou a exigir a sua realização -, novas legislações buscaram proporcionar o efetivo exercício da autodeterminação informativa, em destaque para oferecer proteção ao indivíduo nas ocasiões em que a deliberação quanto ao fornecimento de suas informações é cerceada por outras condicionantes (DONEDA, 2011, p. 08). Nesse período, conforme Ingo Sarlet (2020, p. 03), o reconhecimento de um direito fundamental à proteção de dados pessoais passou a ser gradualmente incorporado à gramática jurídico-constitucional, o que ainda vem ocorrendo em determinados países nos dias atuais.

Por fim, uma quarta geração de leis também pode ser observada a partir do reconhecimento de um desequilíbrio na relação entre pessoas e entidades responsáveis pelo tratamento de dados pessoais, atribuindo-se um caráter coletivo à proteção de tais informações. Concedeu-se, assim, maior grau de proteção a determinados tipos de informações, ocorrendo a disseminação do modelo de autoridades independentes para condução do tema e de normas específicas para determinados setores (DONEDA, 2011, p. 08). A título de exemplo, foram editadas dentro desse contexto, na União Europeia, as Diretivas 95/46/CE e 2000/58/CE, que serão analisadas mais adiante.

Dessa forma, chega-se ao fim "de um longo processo evolutivo experimentado pelo conceito de privacidade: de uma definição original como o direito de ser deixado em paz, até o direito de controle sobre as informações de alguém e determinar como a esfera privada deve ser construída" (RODOTÁ, 2008, p. 17). Trata-se de uma refundação do direito à privacidade, que deu espaço para a construção de novas figuras jurídicas de tutela da personalidade humana, especialmente o direito à proteção de dados pessoais, com o objetivo de proteger o indivíduo no tratamento das suas informações pessoais.

3.2. DO HISTÓRICO NORMATIVO INTERNACIONAL SOBRE O TEMA

Salienta-se, de início, que o direito à proteção de dados não foi expressamente previsto nos principais pactos de proteção a Direitos Humanos firmados no século XX, tais como a Declaração Universal de Direitos Humanos (1948), a Declaração Americana dos Direitos do Homem e o Pacto San José da Costa Rica (1969). Dessa maneira, a sua proteção deriva, em um primeiro momento, das garantias previstas ao direito de privacidade, cuja salvaguarda está prevista nos referidos diplomas (artigos 12 e 11, respectivamente). Na realidade europeia, outrossim, o direito à privacidade também foi previsto de forma importante na Convenção para Proteção dos Direitos do Homem e das Liberdades Fundamentais (1950), a teor do seu artigo 8º.

Conforme Ingo Salert (2020), as primeiras legislações com foco na proteção de dados pessoais, mesmo que não voltadas ao mundo digital, foram promulgadas no início da década de 1970, como em Hessen, na Alemanha. Junto disso, no que se refere aos Estados Unidos da América, sua contribuição deu-se a partir de regras para evitar o abuso na utilização de dados pessoais por parte do Estado, cuja criação foi realizada pelo o Departamento de Saúde, Educação e Bem-Estar Social do país, em 1972, regulamentação que serviu como base para uma estrutura principiológica acerca do tema e possui influência até os dias atuais (DATA PRIVACY BRASIL, 2018). Na época, ainda, foi publicada a primeira lei nacional sobre o tema, na Suécia, nomeada Estatuto para Bancos de Dados, em 1973, além do *Privacy Act* estadunidense, de 1974. O foco de tais legislações, consoante já referido, concentrou-se nos grandes bancos de dados pessoais e no seu posterior controle que seria realizado por órgãos públicos (DONEDA, 2008).

Após, considerando a evolução dos sistemas de coleta de dados, o assunto passou a ser melhor regulamentado no bloco europeu, como através da Lei Francesa de Proteção de Dados Pessoais de 1978 e, mais adiante, pela Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, de 1981, pela Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas.

A Convenção nº 108, do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, em destaque, serviu

como orientação e base para a edição de outras regulamentações a nível nacional no continente europeu. Atualmente, a convenção conta com 55 signatários, incluindo membros do Conselho da Europa, como França, Alemanha e Reino Unido, além de outros países não compreendidos neste grupo, como Argentina, México e Uruguai (UNIÃO EUROPEIA, 2022); o Brasil, por sua vez, se tornou observador no ano de 2018 (DATA PRIVACY BRASIL, 2018). Suas disposições, com efeito, foram muito influenciadas pelos princípios oriundos da regulação estadunidense de 1972, cuja atuação também se estendeu às diretrizes para privacidade formuladas pela Organização para a Cooperação de Desenvolvimento Socioeconômico (OCDE) em 1980.

A Diretriz da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais (1980) prevê, por exemplo, que os países-membros devem adotar legislação doméstica apropriada; encorajar e apoiar a autorregulamentação, seja na forma de códigos de conduta ou em outra forma; fornecer aos indivíduos meios razoáveis para exercerem seus direitos; trazer sanções e soluções apropriadas em caso de inobservância das medidas; garantir que não haja injusta discriminação contra os sujeitos dos dados; e impulsionar a cooperação internacional em matéria de defesa da proteção de dados.

Nesse sentido, os diplomas referidos foram importantes para consolidação dos principais princípios aplicáveis ao tema, tais como os da finalidade, exatidão e livre acesso, dentre outros. A Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, por sua vez, visou "harmonizar a defesa dos direitos e das liberdades fundamentais das pessoas singulares em relação às atividades de tratamento de dados e assegurar a livre circulação de dados pessoais entre os Estados-Membros" (UNIÃO EUROPEIA, 1995).

Sua atuação, destarte, contribuiu para limitar a utilização dos chamados "dados sensíveis" dos cidadãos, os quais seriam descritos como os "que revelassem a origem racial ou étnica da pessoa tutelada, suas opiniões políticas, convicções religiosas ou filosóficas e filiação sindical" (DONEDA, 2008). Além disso, outros tipos de informações também foram protegidas pelo diploma, havendo exceções em que poderia ocorrer a utilização de tais elementos, como no caso de que estes sejam considerados de interesse público.

Outrossim, vieram a ser editadas outras regulamentações sobre o tema, das quais se destacam a Diretiva 97/66 do Parlamento Europeu e do Conselho de 15 de Dezembro de 1997 relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das telecomunicações, e a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de

Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas (Diretiva relativa à privacidade e às comunicações eletrônicas) - que veio a ser alterada pela Diretiva 136/2009 do Parlamento Europeu. Sobre tais regulamentos, elucidam Regina Linden Ruaro e Daniel Piñeiro Rodriguez (2010, p. 06):

> Posteriormente, a Diretiva 97/66 CE, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das telecomunicações, complementa a diretiva anterior, trazendo, por exemplo, determinações de segurança em determinados setores. Assim, determina que, havendo risco especial de violação da segurança de rede dos serviços de telecomunicações acessíveis ao público, o seu fornecedor estará obrigado a informar tal fato aos assinantes e quais as possíveis soluções, incluindo os respectivos custos da reparação pretendida. Em 2002 foi promulgada outra diretiva atinente ao tema – Diretiva 2002/58/CE –, visando à regulamentação da proteção de dados pessoais no âmbito da comunicação eletrônica. Em que pese não tenha inovado o ordenamento da comunidade européia, tal disposição permitiu a adequação das finalidades presentes na Diretiva 95/46/CE à realidade tecnológica não presente à época de sua promulgação. (RUARO; RODRIGUEZ, 2010, p. 06).

Esta última, inclusive, apesar de não trazer grandes inovações, buscou traçar condutas que deveriam ser realizadas no que concerne aos mais diversos tipos de informações coletadas, como a exclusão ou anonimização de dados de tráfego ou a necessidade de permissão ou anonimização para o tratamento de dados de localização. Junto disso, a diretiva atribui deveres de informações que devem ser prestadas aos usuários, tais como os motivos e o destino do tratamento dos seus dados (UNIÃO EUROPEIA, 2002). A alteração realizada pela Diretiva 136/2009 do Parlamento Europeu, ademais, introduziu regulações acerca do uso de *cookies*[7], tendo como foco o dever de informação ao usuário, o qual deve ser cientificado da sua utilização e dos seus objetivos.

Além do exposto, destaca-se a importância da previsão trazida pelo artigo 16 do Tratado sobre o Funcionamento da União Europeia (TFUE) - este oriundo das alterações trazidas pelo Tratado de Lisboa em 2009 - o qual determina a competência para o estabelecimento de normas relativas à proteção de dados, cujo funcionamento se dá de forma compartilhada entre a UE e os Estados-membros. Somado a isso, há previsões acerca da proteção de dados pessoais no artigo 8º da Carta dos Direitos Fundamentais da União Europeia (2000), que prevê a sua salvaguarda e a necessidade do consentimento do usuário quanto ao seu tratamento (UNIÃO EUROPEIA, 2016).

---

[7] O Google define Cookie como “um pequeno arquivo que é salvo no computador das pessoas para ajudar a armazenar as preferências e outras informações usadas nas páginas da Web que elas visitam. Os cookies podem salvar as configurações das pessoas em determinados sites e, às vezes, podem ser usados para acompanhar como os visitantes chegam aos sites e interagem com eles.” (GOOGLE, 2022).

Ademais, ambos os diplomas determinam que o cumprimento das suas regras referentes à proteção de dados devem ser fiscalizadas por uma "autoridade competente" (MASSENO, 2020). Da mesma forma, de acordo com Alessandra Silveira e João Marques (2016) outras fontes também foram determinantes para o atual estágio de proteção de dados, em destaque a jurisprudência, como no acórdão proferido pelo Tribunal de Justiça da União Europeia (TJUE) no Processo C-131/12 (acórdão *Google Spain*), oportunidade em que, dentre diversas questões, foi reconhecido o direito ao esquecimento de dados pessoais de usuários que estivessem acessíveis via motores de busca em site de terceiros. Outras decisões também contribuíram para a construção do tema, destacadamente os acórdãos *Schrems* (Processo C - 362/14) e *Digital Rights Ireland* (Processos apensos C - 293/12 e C - 594/12).

Nesse contexto, veio a ser publicado o principal diploma europeu no que concerne à proteção de dados na atualidade, i.e., o 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 e à livre circulação desses dados e que revoga a Diretiva 95/46/CE, conhecido como Regulamento Geral sobre a Proteção de Dados (RGPD) ou pela expressão em inglês *General Data Protection Regulation* (GDPR) (UNIÃO EUROPEIA, 2016).

Em um panorama geral, o diploma buscou assegurar um nível de proteção coerente e elevado no que tange aos dados pessoais dos indivíduos, a fim de eliminar os obstáculos que impediam a sua circulação dentro da União Europeia. Sua aplicação, nessa lógica, visa a homogeneidade das regulamentações dos Estados-membros sobre o tema, o que, porém, não impede a adoção de ditames específicos em cada um dos países que integram o bloco, conforme descrito no próprio Regulamento (UNIÃO EUROPEIA, 2016).

A publicação do referido regulamento serviu para consolidação dos ditames já conhecidos e para o seu aperfeiçoamento. Nessa linha, o diploma prevê a sua não aplicação em matéria penal (art. 2º, n.º 2), bem como estabelece sobre o tratamento de dados oriundos de agentes situados no território da União Europeia, mesmo que o manejo de tais informações ocorra em locais exteriores, o que representou um grande avanço a fim de propiciar maior segurança aos cidadãos europeus (SILVEIRA et al., 2016).

Destacam-se, além disso, as normativas que preveem a aplicação de multas aos transgressores das suas determinações, além de outras novidades no que concerne às obrigações daqueles responsáveis pelo tratamento de dados, como a de notificar as autoridades competentes ou o próprio titular dos dados quando da sua violação resultarem riscos aos indivíduos. Isso, portanto, representou uma importante alteração no que concerne

ao modelo até então vigente, sendo os responsáveis pelos dados pessoais encarregados da sua autorregulação, a fim de que sejam cumpridas todas as determinações impostas com a nova normativa.

Apesar disso, Alessandra Silveira e João Marques (2016) também ressaltam o reforço dos princípios já existentes, não havendo grandes mudanças nesse sentido, senão vejamos:

> Esta possibilidade (de aplicação de sanções de elevado valor) liga-se a mais uma das novidades deste regulamento, qual seja, a da obrigatoriedade de os responsáveis por tratamentos de dados pessoais que não tenham estabelecimento na UE designarem "por escrito" um representante (artigo 27.º), a fim de que se possam fazer cumprir todas as suas obrigações e, bem assim, respeitar todos os direitos reconhecidos aos titulares dos dados. Em termos estruturais, no que aos princípios relativos à proteção de dados pessoais respeita, não existem novidades de monta. Mantêm-se como válidos os pressupostos inscritos na Diretiva 95/46, sendo obrigatório que o princípio da licitude, o princípio da finalidade, o princípio da qualidade dos dados, o princípio do tratamento leal e o princípio da responsabilidade sejam respeitados integralmente. Alteração relevante é aquela que respeita às crianças e ao respeito pela sua especial vulnerabilidade neste contexto. Saúdam-se as menções particulares às condições de licitude do tratamento [artigo 6.º, n.º 1, alínea f], bem como as reforçadas exigências relativas ao consentimento prestado por crianças – seja quanto à idade mínima para esse consentimento ser prestado de forma válida, seja quanto ao caráter explícito e apreensibilidade da informação prestada (artigo 8.º). (SILVEIRA; MARQUES, 2016, p. 110).

Da mesma forma, outras questões são passíveis de destaque, como a possibilidade dos usuários terem acesso aos dados que foram coletados e dispor destes. O direito ao esquecimento[8] também recebeu respaldo da normativa, o que demonstra a influência do acórdão *Google Spain*. Além disso, termos como o "consentimento" sofreram alterações, sendo este descrito expressamente no diploma como "uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento" (UNIÃO EUROPEIA, 2016), o que impôs maior limitação ao que era anteriormente previsto.

Assim, o diploma serviu como um consolidador dos atos regulatórios em matéria de proteção de dados já existentes. Por outro lado, ainda introduziu novos procedimentos e conceitos, a fim de promover maior segurança ao tratamento de dados e o seu

[8] Nessa linha, "por meio do direito ao esquecimento o afetado reclama proteção contra a difusão de dados pessoais que são processados/propagados e se tornam acessíveis por intermédio de motores de busca – ou seja, um direito originariamente concebido para ser exercido online. Nessa medida, o direito ao esquecimento se distingue do direito ao apagamento originariamente previsto na Diretiva 95/46 para ser exercido offline, pois o último implica que os dados pessoais sejam conservados apenas por um certo período de tempo, exigindo-se o seu apagamento a partir de um prazo adequado às finalidades do tratamento." (SILVEIRA et al., 2016).

compartilhamento. Somado a isso, sua influência se estendeu a outros países exteriores à União Europeia[9], dos quais, aqui, destaca-se o Brasil, cuja legislação específica sobre o tema veio a ser introduzida em 2018, através da Lei n.º 13.709 (LGPD).

Percebe-se, por outro lado, certa pressão do bloco europeu para que outros países adotem regras mais protetivas no que concerne à proteção de dados pessoais. A exemplo, destaca-se a recente revogação do Privacy Shield EU-USA, em 2020, consoante decisão proferida pelo Tribunal de Justiça da União Europeia (UNIÃO EUROPEIA, 2020). O acordo - constituído de princípios, compromissos e declarações oficiais de várias autoridades dos Estados Unidos da América no que concerne ao trânsito de dados entre o país e a União Europeia -, foi adotado em substituição ao *Safe Harbor Privacy Principles*, uma vez que, de acordo com o bloco, os dados pessoais dos cidadãos europeus não se encontravam devidamente protegidos nas transferências com o país estadunidense (CASIMIRO, 2020, p. 119-120). Isso, contudo, não impediu que a União Europeia, novamente, entendesse pela insuficiência de segurança no tratamento de dados realizado pelos Estados Unidos da América, o que foi realizado.

De acordo com o exposto, verifica-se o amplo desenvolvimento da legislação europeia acerca da proteção de dados pessoais. Com efeito, suas diretrizes serviram de base para a criação de diplomas semelhantes em outros países, em destaque pela influência do Regulamento Geral de Proteção de Dados em relação ao tema. A nível nacional, como se sabe, criou-se, nos moldes da legislação europeia, a Lei Geral de Proteção de Dados, instrumento que contribuiu de forma significativa para levantar a discussão sobre privacidade e dados no país, além de traçar importantes princípios e normativas para sua proteção, contexto que será analisado no próximo subcapítulo.

3.3. A LEGISLAÇÃO BRASILEIRA SOBRE A PROTEÇÃO DE DADOS PESSOAIS

No Brasil, em um primeiro momento, a proteção de dados pessoais não constava expressamente na Constituição Federal. Sua aplicação, assim, poderia se dar a partir da interpretação extensiva de alguns direitos ali previstos, como aquele presente no art. 5º, XII e LXXII, os quais trazem, respectivamente, o sigilo das comunicações (também previsto pelo

[9] O RGPD gerou grande impacto internacional, com previsão de medidas de cooperação sobre o tema e requisitos ao fluxo transfronteiriço de dados pessoais, especialmente no que tange à concessão de decisão de adequação ou conformidade, isto é, chancela, por parte da Comissão Europeia, de que os países possuem nível adequado de proteção de dados e podem realizar a transferência internacional de dados, inclusive sem o consentimento do titular (UNIÃO EUROPEIA, 2016)

art. 3º, inc. V, da Lei nº 9.472/97) e a garantia do cidadão de ter acesso a dados governamentais que fossem relativos à sua pessoa ou até mesmo de retificá-los por meio do *habeas data* (BRASIL, 1988). Além disso, o inciso X do referido artigo prevê a proteção da intimidade e da vida privada dos indivíduos, do que também se extrai, por analogia, certa proteção no tratamento de dados pessoais (BRASIL, 1988).

Destaca-se, ainda, a Política Nacional de Informática de 1984 (Lei nº 7.232/84), cujas normativas, dentre outras considerações, tratavam acerca da proteção de dados armazenados (art. 2º, inciso VIII); e o direito dos cidadãos de acessar e retificar tais informações (art. 2º, inciso IX), este último também garantido no Código de Defesa do Consumidor (Lei n 8.079/90), especificamente no que concerne aos bancos de dados e cadastros consumeristas, sendo, além disso, determinadas outras obrigações para abertura desses registros (artigos 43 e 44). Nesse contexto, merece destaque a publicação da Lei do Habeas Data em 1997 (Lei nº 9.507/97). O diploma determinou o rito a ser adotado para garantia do direito de acesso à informação e sua eventual retificação, conforme garantido na Constituição Federal (BRASIL, 1997), servindo, da mesma forma que os diplomas supramencionados, como importante instrumento para promoção do direito à autodeterminação informativa.

O Código Civil, por sua vez, garante a inviolabilidade da vida privada da pessoa natural, conforme seu artigo 21, no tópico sobre direitos da personalidade. Assim, a proteção de dados pessoais, em um primeiro, deriva do direito à privacidade constitucionalmente previsto, além dos pactos internacionais incorporados pelo Brasil, em destaque aqueles já expostos, quais sejam a Declaração Universal de Direitos Humanos (1948) e o Pacto San José da Costa Rica (1969).

Em conjunto com as legislações até então vigentes, o Brasil, em 2004, tornou-se signatário do documento final da XIII Cimeira Íbero-Americana de Chefes de Estado e de Governo, conhecido como da Declaração de Santa Cruz de La Sierra, este firmado no ano de 2003. Dentre suas previsões, ressalta-se o item 45, uma vez que reconhece a proteção de dados pessoais como um direito fundamental e aborda a importância de iniciativas reguladoras ibero-americanas para proteger a privacidade dos cidadãos (SECRETARIA-GERAL IBERO-AMERICANA, 2003).

Novamente no âmbito nacional, a Lei do Cadastro Positivo (Lei nº 12.414/11), editada em 2011, serviu a disciplinar "a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito" e trouxe à baila princípios que vieram a ser posteriormente abarcados pela LGPD, como o da finalidade, livre acesso e transparência (BRASIL, 2011). Dentro do mesmo

período, outrossim, entrou em vigor a Lei de Acesso à Informação (Lei n° 12.527/11), cujo objeto principal seria a regulamentação do direito constitucional de acesso às informações públicas, conforme previsão do art. 5º, XXXIII, da Constituição Federal (BRASIL, 1998). O diploma, apesar das poucas previsões, determina a transparência e o respeito a direitos fundamentais (intimidade, privacidade, honra e etc.), no tratamento de informações pessoais, na forma do seu artigo 31, sendo um importante instrumento no que se refere à transparência do Poder Público (BRASIL, 2011).

Mais adiante, o Marco Civil da Internet (Lei nº 12.965/2014) passou a legislar de forma mais abrangente sobre a proteção de dados e o uso da internet no país. Seu artigo 3º, incisos II e III, nesse sentido, determinam como princípios da disciplina no uso da internet a privacidade e a proteção de dados pessoais, este último, contudo, dependia de norma regulamentar à época da publicação do diploma, o que, mais tarde, deu origem à LGPD. No instrumento legal, ainda, é previsto o dever de informação acerca da coleta, tratamento e proteção de dados pessoais dos usuários, além de prever os casos em que estes possam ser utilizados e a necessidade de consentimento expresso do usuário.

Dessa forma, não estão delimitados os meios e procedimentos que devem ser realizados por operadores ou controladores de dados[10], terminologia esta que não é utilizada no instrumento. Apesar disso, os princípios e direitos fundamentais dos usuários foram devidamente delimitados e garantidos, servindo o diploma como um importante marco para o estabelecimento da legislação atualmente em vigor, apesar do artigo mencionado depender de regulamentação, tratando-se de norma de eficácia contida ou limitada.

Após, com o objetivo de estabelecer normas mais específicas e abrangentes, tendo como base o regulamento aprovado na União Europeia, foi aprovada, no Brasil, a Lei nº13.709/18, conhecida como Lei Geral de Proteção de Dados Pessoais - LGPD, a qual veio a entrar em vigor no ano de 2020. O diploma em questão é considerado um marco acerca do tema no país, estabelecendo determinações que abrangem o tratamento de dados pessoais executados "por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (PESSOA, 2020, p. 77).

---

[10] Conforme dispõe a Lei Geral de Proteção de Dados: Art. 5º Para os fins desta Lei, considera-se:
VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; (BRASIL, 2018).

O instrumento legal aprovado, nessa linha, buscou resguardar os direitos de privacidade e intimidade dos indivíduos, tecendo conceitos e princípios necessários ao tratamento de dados pessoais. Quanto à sua competência, no mesmo sentido do regimento europeu, aliás, a LGPD é aplicável de forma extraterritorial, na forma do seu artigo 3º, ressalvadas as exceções previstas no instrumento.[11]

Dentre os seus dispositivos, ainda, é imperioso mencionar a criação de novos "sujeitos" relacionados ao tratamento de dados pessoais: titular, controlador, operador e encarregado. Nos termos do art. 5º, da LGPD, o titular é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; o controlador é pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; enquanto o operador é quem realiza o tratamento de dados pessoais em nome do controlador; por sua vez, o encarregado é pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), ficando conhecido pela sigla, em inglês, *DPO (Data Protection Officer)* (BRASIL, 2018).

A Lei Geral de Proteção de Dados Pessoais reforça o padrão de comportamento esperado e exigido dos agentes de tratamento, sinalizando que o tratamento de dados pessoais deve observar o princípio da boa-fé. Além disso, estipula outros princípios que devem ser observados no tratamento de dados pessoais, quais sejam, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas (BRASIL, 2018).

Destaca-se, nessa linha, o art. 7º do instrumento, cujos incisos preveem as hipóteses permitidas para o tratamento de dados - o que corresponde a toda operação realizada com dados pessoais -, dentre elas os casos de consentimento do titular (inc. I) e do uso pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos,

---

[11] Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
I - a operação de tratamento seja realizada no território nacional;
II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei. (BRASIL, 2018).

convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei, conforme inciso III do artigo, objeto desta pesquisa (BRASIL, 2018). Há de se salientar, também, a proteção aos dados considerados sensíveis, sendo necessário o consentimento específico dos titulares para o seu uso, ressalvados os casos especificamente ali descritos, a forma do seu artigo 11, incisos I e II (BRASIL, 2018).

Outrossim, salienta-se que a LGPD, no que concerne ao tema em comento, criou e/ou consolidou diversos direitos importantes aos titulares de dados sob tratamento, conforme destaca João Pedro Seefeldt Pessoa (2020, p. 78):

> Pela LGPD, o titular, à semelhança do RGPD, possui, de maneira gratuita e facilitada, os direitos à confirmação da existência de tratamento; ao acesso aos dados; à correção de dados incompletos, inexatos ou desatualizados; à anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na legislação; à portabilidade dos dados a outro fornecedor de ou produto, mediante requisição expressa, de acordo com a regulamentação a ser emanada da autoridade nacional, observados os segredos comercial e industrial; à eliminação dos dados pessoais tratados com o consentimento do titular; à informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; à informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e à revogação do consentimento.

No âmbito específico da Administração Pública, o Capítulo IV do instrumento prevê regras específicas, as quais são aplicadas nos entes da Administração Pública direta e indireta, fazendo, inclusive, referência às pessoas jurídicas de direito público mencionadas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) (BRASIL, 2018). No caso das empresas públicas e das sociedades de economia mista, ainda, as determinações previstas no referido capítulo são aplicáveis somente quando da operacionalização de políticas públicas e no âmbito de execução destas (BRASIL, 2018).

De maneira geral, o interesse público é posto como regra maior para o tratamento de dados pelo Poder Público, conforme dispõe o art. 23 da LGPD, sendo necessária uma finalidade específica para tal (BRASIL, 2018). Outrossim, o diploma também prevê o dever de informação dos entes públicos no que concerne ao tema, em destaque quanto à finalidade, os procedimentos e as práticas realizadas na atividade, bem como o encarregado da sua execução (artigo 31 da Lei) (BRASIL, 2018).

Nesse sentido, a LGPD prevê um espaço específico sobre o tratamento de dados pessoais pelo Poder Público:

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua

> finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:
> I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;
> II - (VETADO); e
> III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei.
> III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e
> IV - (VETADO).
> § 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento.
> § 2º O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no caput deste artigo de instituir as autoridades de que trata a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .
> § 3º Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data) , da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo) , e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .
> § 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei.
> § 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo. (BRASIL, 2018).

Assim, busca-se garantir a transparência dos entes públicos no manejo dos dados que lhe são disponibilizados, evitando seu uso indevido. O artigo 25 do diploma, por sua vez, determina que os dados sob tratamento deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, "com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral" (BRASIL, 2018). Dentro desse espectro, ademais, o artigo 26 do mesmo instrumento aponta que o compartilhamento de dados pelo Poder Público deve "atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei" (BRASIL, 2018).

Ainda, veja-se que, embora o tratamento de dados pessoais seja realizado pelo Poder Público, tal fato não exime a responsabilidade do agente de tratamento, inclusive porquanto, em se tratando de Administração Pública, a responsabilidade pelos danos é objetiva, conforme art. 37, §6º, da Constituição Federal (BRASIL, 1988). Nessa linha, o art. 42, da LGPD, dispõe que o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo (BRASIL, 2018).

Quanto às sanções administrativas, a LGPD prevê que a Autoridade Nacional poderá, em razão das infrações cometidas às normas de proteção de dados pessoais, aplicar advertência; multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; multa diária; publicização da infração após devidamente apurada e confirmada a sua ocorrência; bloqueio e/ou eliminação dos dados pessoais a que se refere a infração; suspensão parcial do funcionamento do banco de dados; suspensão e/ou proibição parcial ou total do exercício da atividade de tratamento dos dados pessoais (BRASIL, 2018). Com exceção às multas, as demais sanções podem ser aplicadas às entidades e aos órgãos públicos, sem prejuízo de outras penalidades aos servidores públicos ou até mesmo de apuração de improbidade administrativa (BRASIL, 2018).

Além disso, no que se refere à Administração Pública, o art. 55-A da Lei Geral de Proteção de Dados determinou a criação de órgão independente responsável por fiscalizar a aplicação das disposições ali previstas, nomeada de Autoridade Nacional de Proteção de Dados (ANPD) (BRASIL, 2018). Em que pese inicialmente prevista como integrante da Presidência da República, o que gerou severas críticas por parte da doutrina, a Medida Provisória nº 1.124/2022, convertida na Lei nº 14.460/2022, transformou a ANPD em autarquia de natureza especial, garantindo a independência do órgão (BRASIL, 2022).

Dessa forma, regulamenta-se a possibilidade do compartilhamento de dados pelos entes públicos, os quais devem observar o princípio da finalidade, este expressamente previsto no art. 6º do diploma mencionado (BRASIL, 2018). A questão, contudo, levantou diversas discussões na doutrina e jurisprudência, nesta última resultando na proposição da ADI 6.649 e da ADPF 695 junto ao Supremo Tribunal Federal, a primeira distribuída por dependência a esta última, demandas que serão tratadas no próximo capítulo.

A fim de consolidar a garantia de proteção de dados pessoais, por último, foi promulgada a Emenda Constitucional de nº 115, em fevereiro de 2022. Dentre as suas alterações, o diploma acrescentou ao artigo 5º, da Constituição Federal, o inciso LXXIX, que assegura aos indivíduos a proteção de dados pessoais, inclusive no meio digital, além de estabelecer a competência da União para legislar sobre o tema, na forma do inciso XXX do artigo 22 da carta constitucional (BRASIL, 1988).

Assim, o direito à proteção de dados possui uma fundamentalidade material, concernente na "relevância, para a esfera individual de cada pessoa e para o interesse coletivo (da sociedade organizada e do Estado), dos valores, princípios e direitos fundamentais

associados à proteção dos dados pessoais e por ela protegidos", especialmente o direito à dignidade da pessoa humana, direito ao livre desenvolvimento da personalidade e direito à privacidade (SARLET, 2020, p. 47).

Atualmente, está sob discussão a promulgação de um diploma de regulação de dados para fins de segurança do Estado, de defesa nacional, de segurança pública e persecução penal, tendo em vista a lacuna legislativa deixada pela LGPD, conforme o seu artigo 4º, inc. III, que excluiu da sua aplicação os temas referidos. Além disso, o §1º do referido artigo também prevê que a regulação específica de tais assuntos deverá ser objeto de legislação específica.

A fim de suprir essa lacuna, foi apresentado, em 2020, o Anteprojeto de Lei de Proteção de Dados Pessoais para Segurança Pública e Persecução Penal (APL), documento que teve suas determinações amplamente discutidas de forma democrática. Mais recentemente, no entanto, foi apresentado o Projeto de Lei nº 1515/2022, o qual busca suprir o mesmo vácuo legislativo deixado pela LGPD.

Há de se destacar, de maneira geral, as diferenças existentes entre os dois projetos, sendo o primeiro de aplicação somente no que concerne à segurança pública e persecução penal, em consonância com outros diplomas internacionais sobre o tema, principalmente no que concerne à Diretiva 680/16, já aprovada no Parlamento Europeu. O PL, por outro lado, busca tratar também dos demais assuntos já elencados, além da atividade de inteligência, sendo mais abrangente que o Anteprojeto. Ainda, os projetos se diferenciam no órgão encarregado pela fiscalização do tratamento de dados, uma vez que o APL prevê que sua realização se dará pelo Conselho Nacional de Justiça, enquanto o PL determina que a própria ANPD o fará.

Em síntese, conforme Nota Técnica emitida pelo Instituto Referência em Internet e Sociedade (2022), o APL adota uma lógica mais garantista, privilegiando o devido processo legal, a proteção de dados pessoais e a privacidade. O Projeto de Lei 1515/2022, por sua vez, causaria certa fragilização dos referidos direitos, em destaque no que concerne ao acesso e compartilhamento de dados pessoais e dados pessoais sensíveis.

Percebe-se, nessa linha, que houve grandes mudanças e evoluções na proteção de dados pessoais na legislação brasileira, principalmente a partir da promulgação da LGPD, diploma que concentrou importantes determinações sobre o tema. A legislação, contudo, ainda carece de complementos, o que se dá em razão de certas lacunas deixadas a instrumentos legais específicos, ainda pendentes de discussão e maior aprofundamento, o que ainda será tratado no presente trabalho.

4. ADMINISTRAÇÃO PÚBLICA DIGITAL, GOVERNO ELETRÔNICO E O TRATAMENTO DE DADOS PESSOAIS

Considerando o panorama apresentado, com o processo de desenvolvimento do direito à proteção de dados no país e com a edição da Lei Geral de Proteção de Dados Pessoais, verifica-se a importância do tema na atualidade. Os dados pessoais, nessa perspectiva, tornaram-se um importante ativo em disputa, sendo também utilizados no desenvolvimento de políticas públicas e serviços, o que vem ocorrendo no cenário nacional. Apesar disso, considerando a possibilidade da criação de novas ferramentas para efetivação da vigilância estatal, a discussão quanto aos limites a serem estabelecidos no uso de dados pelo Poder Público é latente.

Dentro desse cenário, a Administração Pública nacional vem adotando medidas para tornar real o desenvolvimento de um Governo Digital, com a criação de programas e sistemas que permitam a sua execução. Um dos pilares para a implementação desse modelo é o amplo compartilhamento de dados entre órgãos e entes integrantes da Administração Pública - a fim de que possam ser disponibilizados serviços aos cidadãos por meio digital -, do que se destaca a criação de um Cadastro Base do Cidadão, sistema que pretende integrar diversas informações em posse de órgãos e entes estatais. Isso, entretanto, levanta o debate acerca do enquadramento do modelo descrito aos princípios e regras estabelecidos pela LGPD e por outros diplomas referentes à proteção de dados pessoais.

Neste capítulo, portanto, analisar-se-á o processo de instauração da Administração Pública Digital no país, considerando os sistemas já em funcionamento, com foco no Cadastro Base do Cidadão, além da recente legislação sobre o tema e seu (não) enquadramento ao atual estágio de proteção de dados no Brasil. Por fim, estabelecer-se-á um diálogo entre privacidade, proteção de dados e Administração Pública Digital, com foco na controvésia acerca da vigilância estatal.

4.1. A ADMINISTRAÇÃO PÚBLICA DIGITAL E O DESENVOLVIMENTO DO GOVERNO ELETRÔNICO NO BRASIL

É de percepção geral, de acordo com o já apresentado, que o atual estágio de evolução de tecnologias da informação e comunicação, do que se destaca a *Internet*, contribui para a remodelação das bases sociais, havendo influência em campos como a economia, política e a sociedade de maneira geral. Desenvolveu-se, então, a chamada “sociedade em rede”, que,

conforme teorizou Manuel Castells (2005, p. 18), possui suas bases alicerçadas nas redes de comunicação digital, tendo esta atuação a nível global, senão vejamos:

> Além disso, a comunicação em rede transcende fronteiras, a sociedade em rede é global, é baseada em redes globais. Então, a sua lógica chega a países de todo o planeta e difunde-se através do poder integrado nas redes globais de capital, bens, serviços, comunicação, informação, ciência e tecnologia. [...] A sociedade em rede, em termos simples, é uma estrutura social baseada em redes operadas por tecnologias de comunicação e informação fundamentadas na microelectrónica e em redes digitais de computadores que geram, processam e distribuem informação a partir de conhecimento acumulado nos nós dessas redes. A rede é a estrutura formal (vide Monge e Contractor, 2004). É um sistema de nós interligados. E os nós são, em linguagem formal, os pontos onde a curva se intersecta a si própria.

Como referido anteriormente, os usuários das redes sociotécnicas produzem, em larga escala, quantidades imensas de dados, sejam comportamentais, pessoais, sensíveis, dentre outros, em referência à expressão *big data*. Neste panorama, cidadãos também produzem dados que podem ser captados e servir para que o Estado execute políticas públicas variadas, cujo fenômeno não pode passar despercebido pela Administração Pública, necessitando uma integração cada vez maior do ente estatal com as tecnologias de informação e comunicação.

No contexto do Estado em rede (CASTELLS, 2005), os governantes, através da Administração Pública, buscam a inserção do Estado nesse novo sistema social, o que se dá por meio de serviços oferecidos no âmbito digital. De acordo com Gustavo da Silva Santanna (2019, p. 179), a interoperabilidade e a interconexão dos sistemas são duas das principais características inerentes à chamada *e*-Administração.

Nessa linha, o compartilhamento de dados e a cooperação entre os entes públicos é uma tendência dos novos tempos, inclusive no Brasil, o que está legitimado no país através da Lei Geral de Proteção de Dados Pessoais, mais especificamente em seu artigo 26 (BRASIL, 2018). A Lei nº 14.129 de 2021, no mesmo sentido, busca estabelecer regras, princípios e instrumentos para o Governo Digital, sendo aplicável, conforme seu artigo 2º, aos seguintes entes: I - aos órgãos da administração pública direta federal, abrangendo os Poderes Executivo, Judiciário e Legislativo, incluído o Tribunal de Contas da União, e o Ministério Público da União; II - às entidades da administração pública indireta federal, incluídas as empresas públicas e sociedades de economia mista, suas subsidiárias e controladas, que prestem serviço público, autarquias e fundações públicas; e III - às administrações diretas e indiretas dos demais entes federados, nos termos dos incisos I e II do caput deste artigo, desde que adotem os comandos desta Lei por meio de atos normativos próprios (BRASIL, 2021).

Apesar de se reconhecer as facilidades advindas do tipo de serviço fornecido por uma Administração Pública mais digital, destaca-se que sua realização deve ocorrer estritamente

dentro das permissões legais, em razão do próprio princípio da legalidade que rege a atuação do ente estatal. A transparência da administração, assim, deve ocorrer da melhor forma possível, já que a disponibilidade de enormes conjuntos de dados representa, em caso de uso para fins ilícitos, um grande perigo aos administrados.

Nota-se, aqui, que os preceitos adotados pela Lei Geral de Proteção de Dados Pessoais não diferenciam o cuidado que os mais variados dados devem receber, com exceção daqueles dito sensíveis, que merecem guarida especial. A coleta ilegal de um dado isolado, nessa linha, pode parecer inofensiva em um primeiro momento, mas a sua utilização com outras bases de dados e informações pode expor questões caras aos indivíduos, o que deve receber a devida atenção do Poder Público.

Além disso, as problemáticas da integração de massivas quantidades e uma maior facilidade do seu compartilhamento vão além da própria Administração. Conforme se verifica, megavazamentos de dados vêm ocorrendo com frequência no país, o que também incluiu o Poder Público, de modo que tais incidentes de segurança devem ser monitorados e evitados para resguardar os direitos dos titulares de dados.

Segundo reportagem do jornal Estado de S. Paulo, foram vazados, em 2020, dados de mais de 240 milhões de brasileiros junto ao SUS, incluindo de pessoas já falecidas (NOVA…, 2020). Em 2021, foi comunicado pelo Banco Central o vazamento de dados pessoais vinculados a 160 mil chaves pix (CARAM, 2022). Segundo o Ministério da Saúde e Banco Central, no entanto, tais dados incluíam apenas informações cadastrais, não havendo exposição de dados sensíveis.

De acordo com a CNN Brasil, junto disso, sites, arquivos e outros serviços virtuais oferecidos por mais de 20 instituições federais foram alvos de ataques cibernéticos nos dias 10 e 12 de dezembro de 2021 (TOLEDO, 2021). Em outra oportunidade, ainda no ano de 2021, a Controladoria Geral da União, a Polícia Rodoviária Federal e o Instituto Federal do Paraná afirmaram terem sofrido com invasões nos seus respectivos sistemas (MORENO; MORANI, 2022). Nesse contexto, verifica-se que as fragilidades presentes em diversos sistemas da administração pública, o que, todavia, não impede a adoção de um governo cada vez mais digital[12].

Dessa forma, a Administração Pública brasileira tem buscado evoluir seus processos e a prestação de serviços públicos com o auxílio das Tecnologias da Informação e Comunicação

[12] Vide, também, recentes casos de conhecimento público sobre incidentes de segurança envolvendo o Superior Tribunal de Justiça, o Tribunal Superior Eleitoral e diversos Tribunais de Justiça, que indisponibilizaram o acesso aos sistemas de informação e comprometeram a cibersegurança das instituições, o que abala a confiança do público.

(TIC), o que teve início no ano de 2000. Neste período, foi iniciado o Programa de Governo Eletrônico (ou e-Gov), que trouxe adaptações, inovações e desafios para a melhoria da qualidade do serviço público. Seu desenvolvimento deu-se através do Grupo de Trabalho em Tecnologia da Informação (GTTI), formalizado pela Portaria da Casa Civil nº 23 de 12 de maio de 2000, cujo objetivo consistia em examinar e propor políticas, diretrizes e normas relacionadas ao e-Gov. No mesmo ano, o Comitê Executivo do Governo Eletrônico foi criado com o intuito de formular políticas, estabelecer diretrizes, coordenar e articular a implementação de ações e normas que moldaram o desenvolvimento do e-Gov no país (BRASIL, 2019a).

Na sequência, foram editados diversos diplomas para o desenvolvimento do modelo de governo eletrônico no país, como a Medida Provisória 2.200/2001, que criou a ICP-Brasil – Infraestrutura de Chaves Públicas, cujas previsões possibilitaram o uso de assinaturas eletrônicas, certificação digital e a validação legal de documentos eletrônicos. Em termos de acessibilidade digital, foi lançado, em 2005, o Modelo de Acessibilidade de Governo Eletrônico (e-MAG), que serviu para recomendar a adoção de medidas para garantir que os serviços e informações disponibilizados pelo governo sejam acessíveis a todos, incluindo pessoas com deficiência. Sua observação nos sítios e portais do governo brasileiro foi tornada obrigatória através da Portaria nº 3, de 7 de maio de 2007 (BRASIL, 2019a).

Junto disso, a instauração do Portal da Transparência serviu como importante passo rumo a um governo mais digital. No âmbito do governo federal, sua oficialização deu-se através do Decreto nº 5.482/2005, diploma que, inicialmente, tinha como foco a publicação de informações acerca da execução orçamentária e financeira da União, por meio da Rede Mundial de Computadores - Internet (BRASIL, 2005). Atualmente, contudo, sua função foi ampliada, englobando outras informações da administração pública e servindo, conjuntamente com a Lei de Acesso à Informação (BRASIL, 2011), como um importante instrumento para uma maior transparência no setor público.

Também dentro desse espectro, em 2012, deu-se a criação da Infraestrutura Nacional de Dados Abertos (INDA), sistema que traçou a metodologia a ser utilizada por órgãos públicos para divulgação de informações no Portal Brasileiro de Dados Aberto, com foco na transparência e publicidade de dados no âmbito da Administração Pública Federal. A partir de 2015, entretanto, "o paradigma de 'governo eletrônico' trouxe a informatização dos processos internos de trabalho (visão interna), evoluindo para o conceito de "governo digital", cujo foco tem como centro a relação com a sociedade (visão do cidadão), a fim de tornar-se mais

simples, mais acessível e mais eficiente na oferta de serviços ao cidadão por meio das tecnologias digitais", conforme informa o sítio eletrônico do *gov.br* (BRASIL, 2019a).

Dentro dessa ideia, em 2016, foi publicada a Estratégia de Governança Digital (EGD), que implantou um novo paradigma de gestão pública e das relações entre o Estado e a sociedade. Alguns dos ideais do programa consistiram no compartilhamento de infraestrutura e serviços dos órgãos federais com a iniciativa do governo digital, buscando acelerar a transformação digital no governo e a melhoria dos serviços públicos no país. Como consequência da transformação pretendida, foi instituído o portal *gov.br* através do Decreto nº 9.756/2019, cuja atuação se concentra na reunião de diversos serviços e informações governamentais para facilitar o acesso ao cidadão (BRASIL, 2019a).

Mais recentemente, o governo federal instituiu, através do Decreto nº 10.332/2020, a Estratégia de Governo Digital para o período de 2020 a 2022, que organizou princípios, objetivos e iniciativas para a transformação do serviço governamental por meio das tecnologias digitais. Por fim, em 2021, foi publicada a Lei nº 14.129/2021, que "dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública" e também altera a Lei de Acesso à Informação (BRASIL, 2021). Dentre suas diretrizes, destaca-se a interoperabilidade de dados entre órgãos públicos, na forma do seu artigo 38 e seguintes[13], determinação que engloba diversos entes do Poder Público, os quais estão descritos no artigo 2º do mesmo diploma[14].

Observa-se esse fenômeno, a exemplo, com a instituição do portal *gov.br*, que representa a unificação de diversos serviços disponibilizados pelo governo federal. O próprio site da funcionalidade, acerca do assunto, apresenta a evolução histórica do Governo

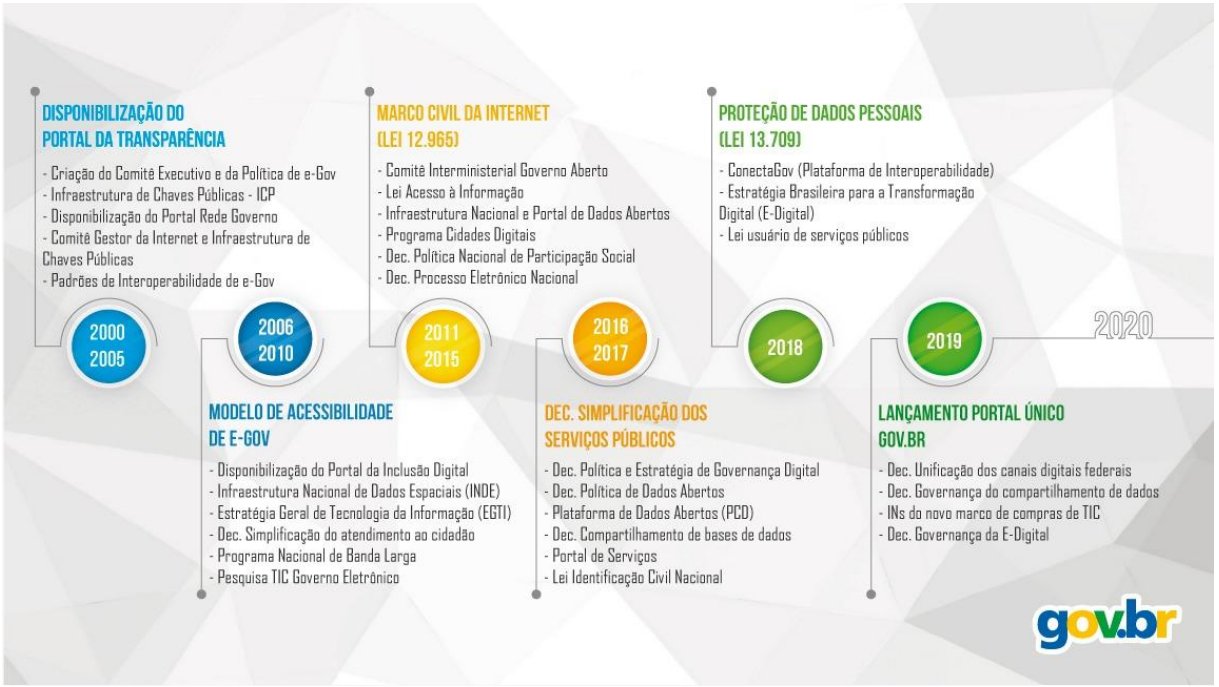
---

[13] Art. 38. Os órgãos e as entidades responsáveis pela prestação digital de serviços públicos detentores ou gestores de bases de dados, inclusive os controladores de dados pessoais, conforme estabelecido pela Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), deverão gerir suas ferramentas digitais, considerando:
I - a interoperabilidade de informações e de dados sob gestão dos órgãos e das entidades referidos no art. 2º desta Lei, respeitados as restrições legais, os requisitos de segurança da informação e das comunicações, as limitações tecnológicas e a relação custo-benefício da interoperabilidade (BRASIL, 2021)

[14] Art. 2º Esta Lei aplica-se:
I - aos órgãos da administração pública direta federal, abrangendo os Poderes Executivo, Judiciário e Legislativo, incluído o Tribunal de Contas da União, e o Ministério Público da União;
II - às entidades da administração pública indireta federal, incluídas as empresas públicas e sociedades de economia mista, suas subsidiárias e controladas, que prestem serviço público, autarquias e fundações públicas; e
III - às administrações diretas e indiretas dos demais entes federados, nos termos dos incisos I e II do caput deste artigo, desde que adotem os comandos desta Lei por meio de atos normativos próprios.
§ 1º Esta Lei não se aplica a empresas públicas e sociedades de economia mista, suas subsidiárias e controladas, que não prestem serviço público.
§ 2º As referências feitas nesta Lei, direta ou indiretamente, a Estados, Municípios e ao Distrito Federal são cabíveis somente na hipótese de ter sido cumprido o requisito previsto no inciso III do caput deste artigo (BRASIL, 2021).

Eletrônico, o qual teria se iniciado em 2000, com a disponibilização do Portal de Transparência, conforme segue.

Figura 1 - Linha do tempo - Governo Eletrônico



Fonte: (BRASIL, 2019a)

Verifica-se, de acordo com a figura juntada, o destacamento da instituição do ConectaGov, cuja atuação, conforme o próprio Governo Federal, "promove a troca automática e segura de informações entre os sistemas para que o cidadão não tenha que reapresentar informações que o governo já possua", de modo que "essa integração de dados, conhecida como interoperabilidade, desonera o cidadão, simplifica o serviço público, reduz fraude e traz segurança e economia para todo o processo" (BRASIL, 2022). A plataforma, assim, busca facilitar o acesso dos mais diversos entes governamentais aos dados dos cidadãos, o que tornaria mais ágil o atendimento e a execução de serviços.

Há de se questionar, todavia, quais os dados estão incluídos no referido compartilhamento, bem como os critérios adotados para o seu repasse entre órgãos. A exemplo das plataformas já integradas, tem-se o Cadastro Base de Endereço, Cadastro Base do Cidadão - que será melhor explorado no próximo capítulo -, Carteira de Documentos gov.br, Validação biométrica digital e facial e Consulta Certidão Negativas de Débitos, dentre muitos outros.

Percebe-se, a partir do exposto, que o Poder Público vem realizando amplos esforços para promoção do governo digital. A interoperabilidade e o compartilhamento de dados entre os seus órgãos, como visto, possui papel fundamental para o desenvolvimento dos programas e estratégias traçadas. Contudo, questões como o nível de segurança fornecido ao titular de dados e quem deles poderá dispor é essencial para o exercício do direito à proteção de dados e da autodeterminação informativa. Consoante se extrai das informações trazidas pelo Governo Federal, o objetivo da plataforma é integrar cada vez mais a administração pública, estendendo o compartilhamento de dados a entes ainda não vinculados, o que por certo não era do conhecimento dos cidadãos quando do fornecimento de dados.

Santanna (2019, p. 242) elucida, ademais, que outra problemática consiste na eventual obrigatoriedade da utilização do sistema integrado, não havendo outra opção ao cidadão que não fornecer seus dados:

> A e-Administração, também, deve ter uma gestão neutra, ou seja, deve ser acessível em qualquer plataforma, não podendo obrigar o cidadão a utilizar um único sistema. De nada adiantaria garantir o acesso à rede e a sua neutralidade (como direito fundamental) se a própria Administração obrigasse o cidadão (como o faz) a utilizar um ou outro sistema. Da mesma forma, a Administração Eletrônica deve acompanhar o progresso tecnológico, tanto na atualização de seus programas/softwares, como na máxima busca pela segurança (ou cibersegurança). A utilização de softwares livres é uma boa prática na garantia do avanço tecnológico, haja vista que permite sua atualização e modificação de maneira gratuita ou a baixo custo.

Nesse sentido, a Administração Pública Digital é uma tendência imparável, que precisa, no entanto, respeitar os limites legais, éticos e os direitos dos administrados, especialmente considerando o horizonte em que o ente estatal vai demandar cada vez mais dados e precisa estar autorizado a fazer compartilhamentos. Dessa forma, cabe analisar as diretrizes já traçadas no que concerne ao compartilhamento de dados e criação de uma plataforma única de integração dessas informações, o que será realizado no próximo tópico.

4.2. SOBRE A EXPANSÃO DO COMPARTILHAMENTO DE DADOS E A CRIAÇÃO DE UM CADASTRO BASE DO CIDADÃO

De acordo com a tendência de desenvolvimento de uma Administração Pública Digital, o governo brasileiro vem avançando e criando novas normativas que autorizam o compartilhamento de dados entre seus órgãos, a fim de garantir a interoperabilidade necessária ao desenvolvimento da *e*-Administração. A questão, contudo, não foi amplamente

aceita no país, muito em razão dos perigos envolvidos no compartilhamento irrestrito de informações.

Nesse cenário, destaca-se a publicação do Decreto nº 10.046/2019, que 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. Seu objetivo, em resumo, muito se assemelha ao que prevê o exercício da administração pública digital, estabelecendo normas e diretrizes com as seguintes finalidades: I - simplificar a oferta de serviços públicos; II - orientar e otimizar a formulação, a implementação, a avaliação e o monitoramento de políticas públicas; III - possibilitar a análise das condições de acesso e manutenção de benefícios sociais e fiscais; IV - promover a melhoria da qualidade e da fidedignidade dos dados custodiados pela administração pública federal; e V - aumentar a qualidade e a eficiência das operações internas da administração pública federal (BRASIL, 2019b).

Da sua análise, entretanto, são extraídas diversas violações aos princípios e normas estabelecidas pela Lei Geral de Proteção de Dados Pessoais. O art. 3º, inc. I, do Decreto nº 10.046/2019, a exemplo, prevê que "a informação do Estado será compartilhada da forma mais ampla possível, observadas as restrições legais, os requisitos de segurança da informação e comunicações e o disposto na Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais" (BRASIL, 2019b). Nessa linha, apesar de mencionar a exigência de observância à LGPD, o dispositivo ignora o artigo 26 da própria lei de remissão[15], que restringe o uso de dados para "finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas" (BRASIL, 2018).

Dessa forma, o decreto parece inverter a ordem estabelecida pela lei que delimita o uso de dados pelo Poder Público. Isso porque as informações dos cidadãos devem ser utilizadas para fins específicos, e não da forma mais ampla possível dentro de eventuais limites previamente estabelecidos. Somado a isso, o Decreto nº 10.046/2019 prevê, em seu artigo 4º, a categorização do compartilhamento de dados em níveis a partir do seu grau de confidencialidade, quase que inspirado na já superada teoria das esferas, norma que igualmente contrária à legislação vigente, conforme segue:

> Outrossim, há a criação de três níveis de compartilhamentos de dados, "de acordo com a sua confidencialidade": amplo, restrito e específico. Basicamente, a

[15] Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei. (BRASIL, 2018).

> classificação dispõe que os dados não sigilosos não estarão "sujeitos a nenhuma restrição de acesso". Ora, os níveis desconsideram toda a teoria na qual se funda a novel legislação de proteção de dados. Como visto, a proteção de dados é direito autônomo positivado na Constituição, e não se submete à dicotomia dado público e privado. Na realidade, todo dado relativo à pessoa natural, ainda que publicizado, merece algum nível de proteção, não havendo espaço, portanto, para compartilhamento amplo ou irrestrito, ou, ainda, compartilhamento restrito, porém, "simplificado" e a ser acessado por diversos órgãos e entidades. (MIRANDA et al, 2022, p. 15).

Nessa perspectiva, o diploma adota termos e conceitos estranhos à LGPD, que trata de dados pessoais, sensíveis, públicos e etc., enquanto aquele traz atributos biográficos e biométricos, estes incluídos em um rol não taxativo (art. 2º, incs. I e II, do Decreto nº 10.046/2019), ampliando a extensão dos dados passíveis de coleta pelo Poder Público. Dessa forma, há de se informar especificamente os dados coletados e a sua distinção, sob pena de uma coleta massiva executada sob o argumento de adoção de políticas públicas com a oferta de serviços digitais. Acerca disso:

> O conteúdo dos dados biográficos inclui dados inexistentes nas anteriores bases cadastrais e de conceituação extremamente vaga, como "fatos da sua vida" (art. 2º, I, do Decreto nº 10.046/2019) e "grupo familiar". Atualmente o conceito de família já não se limita à família biológica, mas inclui a família socioafetiva, o que, por si só, amplia a base de dados biográficos dos cidadãos. Como a chamada Biometria Comportamental está em franca expansão, sendo exponencial da inteligência artificial, como o reconhecimento facial. Tais informações especialmente incorporada pelas tecnologias de monitoramento, temos um indício de que a coleta desses dados poderá ser massiva, com o argumento de que o Estado está adotando políticas públicas para evitar fraudes e para promover maior segurança para a população. Essas políticas deveriam ser adotadas com maior grau de transparência, sob pena de se criar um estado de permanente vigilância, com drásticas consequências para os direitos individuais. Além disso, as chamadas base integradora e base temática (art. 2º, incisos VI e VII do Decreto nº 10.046/2019), que integrarão os atributos biográficos previstos no art. 2º, I, e os atributos biométricos, provocam indagações sobre o contexto em que ocorrerão o tratamento e a utilização dessas novas bases e o cruzamento desses dados, especialmente diante do avanço dos sistemas de tratamento automatizado e dos mecanismos de decisão automatizada decorrentes do crescimento podem ser utilizadas para um controle político intenso dos cidadãos, típico de regimes totalitários. (RIO DE JANEIRO, 2020, p. 22).

Além disso, outras incongruências também merecem ser apontadas, como a criação de um órgão "gestor de dados", termo inexistente na Lei Geral de Proteção de Dados, que trata de controlador, operador e encarregado. O Decreto 10.046/2019, entretanto, aponta diversas responsabilidades a esse novo ente, como, em destaque, a categorização do nível de compartilhamento de dados no âmbito da Administração Pública[16]. Ademais, destaca-se

[16] Art. 4º O compartilhamento de dados entre os órgãos e as entidades de que trata o art. 1º é categorizado em três níveis, de acordo com sua confidencialidade:
[...]

também a ausência de qualquer menção à Autoridade Nacional de Proteção de Dados, que possui função central na promoção e fiscalização do tratamento de dados no país. Esse papel, no âmbito do diploma em questão, é atribuído ao Comitê Central de Governança de Dados.

Em que pese a necessidade de cumprimento ao princípio constitucional da publicidade e o direito de acesso a informações governamentais, consoante já mencionado, há se de destacar que a publicização de tais informações não possui relação com os dados pessoais em posse da administração pública. O diploma publicado, todavia, não determina distinção entre tais informações, o que representa perigo ao direito fundamental à proteção de dados pessoais (MIRANDA, 2022, p. 16).

Além do exposto, a criação de um Cadastro Base do Cidadão, na forma do art. 16, do Decreto nº 10.046/2019[17], carece de melhores regulamentações, principalmente quanto aos órgãos destinatários dos dados obtidos, bem como quais informações farão parte do sistema, havendo a previsão do acréscimo de outros dados não previstos no diploma - estes considerados como o mínimo a ser obtido. O §2º do art. 18 do instrumento legal, nessa lógica, prevê que "a base integradora será acrescida de outros dados, provenientes de bases temáticas, por meio do número de inscrição do CPF, atributo chave para a consolidação inequívoca dos atributos biográficos, biométricos e cadastrais", (BRASIL, 2019b).

Há de se mencionar que, na lógica do exposto, os princípios da eficiência e da supremacia do interesse público parecem se sobrepor àqueles concernentes ao direito fundamental à proteção de dados. Em razão dos argumentos trazidos, no entanto, sobrevieram demandas judiciais que reclamaram as inconsistências das normas trazidas pelo Decreto nº 10.046/2019, especialmente a Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 695/DF e a Ação Direta de Inconstitucionalidade (ADI) nº 6649/DF.

---

§ 1º A categorização do nível de compartilhamento será feita pelo gestor de dados, com base na legislação. (BRASIL, 2019b).

[17] Art. 16. Fica instituído o Cadastro Base do Cidadão com a finalidade de:

I - aprimorar a gestão de políticas públicas;

II - aumentar a confiabilidade dos cadastros de cidadãos existentes na administração pública, por meio de mecanismos de manutenção da integridade das bases de dados para torná-las qualificadas e consistentes;

III - viabilizar a criação de meio unificado de identificação do cidadão para a prestação de serviços públicos;

IV - disponibilizar uma interface unificada de atualização cadastral, suportada por soluções tecnológicas interoperáveis das entidades e órgãos públicos participantes do cadastro;

V - facilitar o compartilhamento de dados cadastrais do cidadão entre os órgãos da administração pública; e

VI - realizar o cruzamento de informações das bases de dados cadastrais oficiais a partir do número de inscrição do cidadão no CPF.

Parágrafo único. É vedado o uso do Cadastro Base do Cidadão, ou o cruzamento deste com outras bases, para a realização de tratamentos de dados que visem mapear ou explorar comportamentos individuais ou coletivos de cidadãos, sem o consentimento expresso, prévio e específico dos indivíduos afetados e sem a devida transparência da motivação e finalidade. (Incluído pelo Decreto nº 11.266, de 2022). (BRASIL, 2019b).

A ADPF, primeira demanda proposta, foi levada a juízo pelo Partido Socialista Brasileiro (PSB), e buscou tratar acerca do compartilhamento de um grande volume de dados dos cidadãos brasileiros, mais especificamente aqueles referentes aos registros de carteiras de habilitação de mais de 76 milhões de brasileiros, onde constariam informações como nomes, filiação, endereços, telefones, dados dos veículos e fotos de todo portador de Carteira Nacional de Motorista, o que seria realizado pelo Serviço Federal de Processamento de Dados (SERPRO) à Agência de Inteligência (ABIN), conforme noticiado pelo portal *The Intercept* em junho de 2020 e depois confirmado pelo Governo Federal. A ação do partido, nesse sentido, baseou-se nas determinações expostas pelo Decreto nº 10.046/2019 acerca do compartilhamento de dados.

No decorrer da sua petição inicial, o partido autor discorreu acerca da violação direta aos direitos à liberdade e à dignidade da pessoa humana, além da privacidade, proteção de dados e autodeterminação informativa, estes previstos pela Constituição Federal e Lei Geral de Proteção de Dados Pessoais. Como argumento, ainda, a parte autora afirmou que os dados objetos do compartilhamento foram coletados para fins diferentes do seu uso pela ABIN, pelo que estariam sendo desconsiderados os princípios da publicidade e transparência, considerando que os titulares não foram, *a priori*, informados de tais circunstâncias (BRASIL, 2022).

Além de destacar o desrespeito a preceitos fundamentais, a petição inicial também teceu considerações acerca dos perigos no uso de tais dados de forma ao exercício da vigilância estatal, o que representaria um grande potencial lesivo. Ainda, é apontado que a aplicação do decreto mencionado, conforme expressamente descrito no próprio diploma, deve ser realizado em consonância com a Lei Geral de Proteção de Dados Pessoais, o que não estaria sendo realizado no caso. Assim, o partido autor pediu pela cessação do referido compartilhamento de dados, além da inutilização daqueles já tratados (BRASIL, 2022).

O Laboratório de Políticas Públicas e Internet - LAPIN, legitimado como *amicus curie* na demanda, concordou com os termos expostos, pedindo, dentre outros requerimentos, pela não aplicação do Decreto 10.046/19 à atividade de inteligência, uma vez que não haveria previsão para tal. Junto disso, argumentou que qualquer tratamento de dados pelo Poder Público deveria ser realizado com base nos preceitos adotados pela LGPD, salientando os princípios da finalidade, adequação, necessidade e transparência. Por fim, arguiu que a utilização de dados sensíveis dos cidadãos é ainda mais limitada pela legislação, na forma do art. 11 da Lei Geral de Proteção de Dados, sendo necessário o estrito cumprimento dos princípios previstos no artigo 6º do instrumento legal (BRASIL, 2022).

Em defesa da União, a Procuradoria-Geral da República, no mérito, arguiu a total observância aos preceitos adotados pela LGPD, ressaltando que o Decreto nº 10.046/2019 não possibilitaria o compartilhamento indiscriminado de dados pessoais, mas que tornaria mais ágil o fluxo de informações entre órgãos e instituições que detenham autorização legal para isso. Salientou, ainda, que a LGPD faculta o compartilhamento e o tratamento de dados pela Administração Pública para execução de políticas públicas legalmente previstas, bem como que a utilização indevida das previsões previstas no instrumento não o torna inconstitucional, devendo ocorrer a análise de cada caso, pedindo, de maneira geral, pela improcedência dos pedidos expostos pelo autor (BRASIL, 2022).

A demanda foi julgada conjuntamente com a ADI 6649/DF, ajuizada em face da integralidade dos dispositivos estabelecidos pelo Decreto nº 10.046/19, em afronta ao art. 84, inc. IV e VI, "a", da Constituição Federal, por supostamente exorbitar os poderes normativos concedidos pela Constituição ao Presidente da República, e por violação direta aos art. 1º, *caput*, inc. III e art. 5º, *caput*, e inc. X, XII e LXXII da Constituição Federal, que garantem, respectivamente, a dignidade da pessoa humana; a inviolabilidade da intimidade, da privacidade e da vida privada, da honra e da imagem das pessoas; o sigilo dos dados; a garantia do habeas data, a proteção de dados pessoais e a autodeterminação informativa (BRASIL, 2022).

No corpo da inicial, o Conselho Federal da Ordem dos Advogados do Brasil afirmou que, com a justificativa de facilitação do acesso a serviços públicos, o decreto discutido estaria dando forma a "uma ferramenta de vigilância estatal extremamente poderosa". Assim, pediu pela declaração de inconstitucionalidade de todo o teor do diploma discutido, bem como do Decreto 10.403/2020, que lhe alterou certos dispositivos (BRASIL, 2022).

Ao final, o Supremo Tribunal Federal julgou pela parcial procedência dos pedidos expostos na inicial, elegendo diversos pressupostos para o compartilhamento de dados no âmbito da administração pública e exigindo, dentre outras questões: e eleição de propósitos legítimos, específicos e explícitos quanto ao tratamento de dados (art. 6º, inciso I, da Lei 13.709/2018); a compatibilidade do tratamento com as finalidades informadas (art. 6º, inciso II); e a limitação do seu uso ao mínimo necessário para o atendimento da finalidade informada (art. 6º, inciso III) (BRASIL, 2022).

Junto disso, o Tribunal determinou a rigorosa observância à LGPD, com ampla publicidade dos atos realizados pela Administração Pública, na forma do art. 23, inc. I, do diploma, além de um rígido controle de acesso ao Cadastro Base do Cidadão - que deverá ser realizado pelo Comitê Central de Governança de Dados -, no exercício das competências

aludidas nos arts. 21, inc. VI, VII e VIII do Decreto nº 10.046/2019. Outrossim, a decisão determinou a aplicação dos arts. 42 e seguintes da Lei 13.709/2018 para o caso de descumprimento dos preceitos estabelecidos. Ademais, no que concerne à atividade inteligência, foi decidido pela observação aos requisitos fixados no julgamento da ADI 6.529/DF (BRASIL, 2022)[18].

Em razão da decisão proferida, o governo federal publicou o Decreto nº 11.266/2022, que alterou disposições do Decreto nº 10.046/2019, a fim de adequá-las às determinações presentes no conteúdo decidido, incorporando-as ao texto. Dessa maneira, o novo texto impôs a total observância ao direito à preservação da intimidade e da privacidade da pessoa natural, bem como da proteção dos dados pessoais. Ainda, restou normatizada a exigência de autorização do gestor de dados para compartilhamentos de dados de níveis restritos e específicos, bem como a impossibilidade do uso do Cadastro Base do Cidadão para fins de vigilância[19].

As mudanças realizadas, em uma primeira análise, representam uma evolução da Administração Pública Digital no que concerne à proteção de dados pessoais. Apesar disso, tendo em vista a imparável evolução dessa nova forma de gestão, ainda persistem problemáticas quanto ao tratamento de dados no âmbito do Poder Público, em destaque pela categorização do compartilhamento das informações protegidas, a persistência de conceito

---

[18] [...]. 4. O compartilhamento de informações pessoais em atividades de inteligência observará o disposto em legislação específica e os parâmetros fixados no julgamento da ADI 6.529, Rel. Min. Cármen Lúcia, quais sejam: (i) adoção de medidas proporcionais e estritamente necessárias ao atendimento do interesse público; (ii) instauração de procedimento administrativo formal, acompanhado de prévia e exaustiva motivação, para permitir o controle de legalidade pelo Poder Judiciário; (iii) utilização de sistemas eletrônicos de segurança e de registro de acesso, inclusive para efeito de responsabilização em caso de abuso; e (iv) observância dos princípios gerais de proteção e dos direitos do titular previstos na LGPD, no que for compatível com o exercício dessa função estatal. [...] (BRASIL, 2022)

[19] Art. 5º [...]

§ 3º O compartilhamento de dados nos níveis de categorização restritos e específicos serão autorizados pelo gestor de dados e seu processo será formalizado por documentos de interoperabilidade cuja solicitação seguirá os critérios estabelecidos pelo Comitê Central de Governança de Dados, em observância:

I - aos dispositivos:

a) da Lei nº 13.709, de 2018 - Lei Geral de Proteção de Dados Pessoais;

b) da Lei nº 14.129, de 29 de março de 2021; e

c) da Lei nº 12.527, de 18 de novembro de 2011;

II - às orientações da Autoridade Nacional de Proteção de Dados; e

III - às normas correlatas.

§ 4º Nas solicitações de interoperabilidade que envolvam dados pessoais, serão explicitados, além do disposto no § 3º:

I - o propósito legítimo, específico e explícito;

II - a compatibilidade com a finalidade; e

III - o compartilhamento do mínimo necessário para atendimento da finalidade. [...]

Art. 16. [...] Parágrafo único. É vedado o uso do Cadastro Base do Cidadão, ou o cruzamento deste com outras bases, para a realização de tratamentos de dados que visem mapear ou explorar comportamentos individuais ou coletivos de cidadãos, sem o consentimento expresso, prévio e específico dos indivíduos afetados e sem a devida transparência da motivação e finalidade (BRASIL, 2022).

estranhos à LGPD e o distanciamento da Autoridade Nacional de Proteção de Dados, além da adoção de um sistema que não traz protagonismo ao cidadão, como será tratado em seguida.

4.3. DIÁLOGOS ENTRE PRIVACIDADE, PROTEÇÃO DE DADOS PESSOAIS E ADMINISTRAÇÃO PÚBLICA DIGITAL

A implementação da Administração Pública Digital, de acordo com o referido acima, se apresenta em desenvolvimento no governo brasileiro. Esse contexto, entretanto, exige total observância ao direito fundamental à proteção de dados pessoais e aos princípios que dele derivam, em destaque à autodeterminação informativa, expressamente prevista no art. 2º, inc. II, da Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018). O tema, da forma atualmente conduzida, gerou diversos debates acerca dos limites que devem ser impostos ao Poder Público, principalmente com a publicação do Decreto nº 10.046/2019, que veio a ser alterado posteriormente pelo Decreto nº 11.266/2022 (BRASIL, 2022). Apesar das alterações realizadas, a forma adotada pelo Poder Público ao Governo Digital e/ou *e*-administração ainda carece de melhores contornos e artifícios para garantir o direito fundamental à proteção de dados, sob pena de configurar um grande mecanismo de vigilância dos titulares.

Conforme Danilo Doneda (apud DE LUCA, 2019), o decreto mencionado vai na contramão dos avanços observados em países como Reino Unido, Austrália, Canadá e Finlândia, que implementaram sistemas de interoperabilidade pautados na transparência e, principalmente, no controle e acesso dos indivíduos aos seus próprios dados. O cidadão, nessa linha, deve ter conhecimento prévio do destino que será concedido às suas informações, adquirindo confiança junto à Administração Pública, como elucida Patrícia Baptista e Leonardo Antoun (2022, p. 29):

> Embora um dos principais ganhos representados pela política digital seja, nas palavras de Vanice do Valle, o "desenvolvimento de cultura de dados como ativo institucional", talvez um dos maiores desafios das Administrações locais em relação ao governo digital seja assegurar aos seus cidadãos tratamento e proteção adequados a esses dados. O processamento desses dados, porém, deve servir aos fins prévia e claramente determinados e informados à sociedade, respeitando o princípio da finalidade pública e o direito à privacidade. O sucesso da política de governo digital depende da construção de um ambiente de confiança: o cidadão não pode temer o que o Estado possa fazer com os dados que colhe nas suas plataformas digitais. Ele precisa saber de antemão o que o Estado fará com eles. A Administração Pública não é dona desses dados colhidos, apenas os custos para finalidades públicas previamente informadas e delimitadas. Como destaca Lucas Borges de Carvalho, implantadas sem as devidas salvaguardas técnicas e jurídicas, as políticas de governo digital "podem constituir um fator de produção de novos riscos e incertezas" (BAPTISTA; ANTOUN, 2022, p. 29).

A confiança mencionada pelo autor é um dos argumentos para a implementação do chamado “governo aberto”, que torna mais transparente os processos decisórios dentro do aparato estatal através da disponibilização dos dados utilizados para tal. O Decreto nº 10.046/2019 (art. 11) e a Lei do Governo Digital (arts. 3º, inc. XIV, 4º, inc. IV e 29, §2º, inc. XI), aliás, possuem previsões a esse respeito, em consonância com os dispositivos do Decreto 8.777/2016, que instituiu a Política de Dados Abertos do Poder Executivo Federal (BRASIL, 2016). Isso, contudo, não deve “extrapolar os limites da privacidade do cidadão ao expor dados pessoais de que tem acesso em razão da consecução de serviços públicos e análise de deveres civis” (CRISTOVÁM; HAHN, 2020, p. 08).

Em vista disso, faz-se necessário trazer à baila outras formas de concretização do Governo Digital, diferentes da interoperabilidade atualmente pretendida, que possibilita o acesso de diversos órgãos da Administração Pública Federal a dados que o titular sequer autorizou que fossem utilizados para tal fim. Salienta-se, nessa lógica, a necessidade de proteção de todos os dados dos cidadãos, que possuem, segundo a teoria do mosaico, o mesmo potencial lesivo, independente do seu grau de sigilo ou de confidencialidade.

Para tal, na contramão do atual modelo adotado pelo Governo Federal, poderia se falar em “Sistemas de Recomendação voltados a Governo Eletrônico com o uso do Cadastro Base do Cidadão” (MOISINHO et al, 2021). Conforme proposto pelos autores, o sistema de recomendação contribuiria para a oferta de serviços de interesse do usuário, a partir da sua própria manifestação, senão vejamos:

> Dessa forma, utilizar um sistema de recomendação que integre a noção de auto perfil ao Cadastro Base do Cidadão (CBC) para serviços de governo eletrônico pode ser uma solução para oferecer serviços personalizados aos cidadãos, garantindo proteção à privacidade de dados e livre expressão da identidade pessoal em meio virtual. O objetivo é que o sistema de recomendação descarte os serviços irrelevantes dos resultados de busca, apresentando apenas resultados relevantes de interesse do usuário e de acordo com a construção do seu auto perfil no portal do governo. (MOISINHO et al, 2021, p. 02).

A criação de um "auto perfil" do usuário, segundo a pesquisa, tornaria possível a construção de uma identidade virtual do cidadão, que poderia escolher como prefere ser “visto” pela plataforma e pelo Governo. O titular de dados, nessa linha, teria maior controle sobre quais das suas informações seriam utilizadas na formação do seu perfil (MOISINHO, 2021), “escolhendo” compartilhar determinadas informações somente com as bases de dados que realmente lhe interessam. O modelo, assim, inverte a ideia atualmente empregada ao Cadastro Base do Cidadão, permitindo que o titular de dados tenha maior autonomia na

escolha das informações que pretende disponibilizar à Administração Pública, sendo uma importante evolução no que concerne à autodeterminação informativa.

Mais além da sugestão apresentada, há também que se garantir que os cidadãos tenham controle sobre a Administração Pública, no que tange ao exercício de atribuições que envolvam a massiva coleta e tratamento de dados. Dessa forma, evita-se que tais informações sejam utilizadas para outros fins que não os previstos pela legislação e autorizados (mesmo que não expressamente) pelos indivíduos, inclusive pelo fortalecimento e aproximação da Autoridade Nacional de Proteção de Dados, para servir como contrapoder e/ou contrapeso também em relação aos abusos no tratamento de dados pessoais pelo Poder Público. Nesse sentido:

> Por outro lado, a privacidade entendida como além do direito de ser deixado só pode ser transformada em ferramenta social no jogo de poderes da sociedade em rede, quando consegue limitar e controlar diretamente os sujeitos públicos e privados que coletam e tratam os dados pessoais. Se as informações pessoais são o ouro mais importante do novo século, a exigência de um direito à privacidade positivo, regulado, explícito e sancionador pode contribuir para equilibrar os interesses, de forma que, sendo um contrapeso nessa balança, pode representar um exercício de democracia. [...] . O Efeito Orwell deve ser ao revés, possibilitando que os sujeitos vigiem o Grande Irmão, sob todos os lados e esferas, num Estado de vidro, já que o ente estatal, caracterizado pelo público, deve estar ao controle da multidão. (PESSOA, 2020, p. 101).

O exercício da contravigilância, dessa maneira, serve como um impulsionador para que o Estado, como detentor de dados pessoais dos cidadãos para a execução dos mais diversos serviços, atue dentro das normas previstas para tal. A transparência atualmente desempenhada pelo governo brasileiro, através dos dados abertos e da Lei de Acesso à Informação, forma um importante arcabouço para esse controle. O decreto responsável pela criação do Cadastro Base do Cidadão, dentro dessa perspectiva, aponta para o catalogamento junto ao Portal Brasileiro de Dados Abertos do compartilhamento amplo de dados, na forma do seu artigo 11 (BRASIL, 2019b).

Tal determinação, entretanto, não engloba os dados descritos no diploma como de compartilhamento restrito ou específico[20], situação que, apesar de inevitável (pois não há

[20] Art. 4º O compartilhamento de dados entre os órgãos e as entidades de que trata o art. 1º é categorizado em três níveis, de acordo com sua confidencialidade:
I - compartilhamento amplo, quando se tratar de dados públicos que não estão sujeitos a nenhuma restrição de acesso, cuja divulgação deve ser pública e garantida a qualquer interessado, na forma da legislação;
II - compartilhamento restrito, quando se tratar de dados protegidos por sigilo, nos termos da legislação, com concessão de acesso a todos os órgãos e entidades de que trata o art. 1º para a execução de políticas públicas, cujo mecanismo de compartilhamento e regras sejam simplificados e estabelecidos pelo Comitê Central de Governança de Dados; e
III - compartilhamento específico, quando se tratar de dados protegidos por sigilo, nos termos da legislação, com concessão de acesso a órgãos e entidades específicos, nas hipóteses e para os fins previstos em lei, cujo compartilhamento e regras sejam definidos pelo gestor de dados (BRASIL, 2019b).

como publicar tais informações), torna dificultoso o controle do próprio titular no que concerne aos dados que disponibiliza ao ente público. Portanto, há de se conceder a cada indivíduo o poder de vigiar os seus próprios dados, a exemplo do que ocorre em países como a Estônia, onde os cidadãos sabem exatamente quem acessou o seu cadastro junto ao governo, além de poder limitar o acesso a algumas das informações ali presentes (CARPANEZ, 2018).

Dentro dos novos contornos da atual sociedade, não há outra alternativa aos cidadãos que não o controle da circulação das informações, sendo "possível utilizar-se das tecnologias de informação e comunicação para vigiar o Estado e as grandes corporações causando um incômodo público para que sejam cada vez mais públicas, transparentes, cristalinas" (PESSOA, 2020, p. 102).

A privacidade e a proteção de dados, assim, são partes essenciais no desenvolvimento do Governo Digital, tendo em vista a necessidade de uma relação de confiança entre a Administração Pública e os cidadãos. Não se desconhece da importância do tratamento de dados pelo Poder Público para execução de políticas públicas, mas as bases legais para coleta de informações devem ser pautadas na privacidade, na proteção de dados pessoais, na autodeterminação informativa dos titulares, mas, principalmente, na transparência pública, o que, caso contrário, levaria ao recrudescimento de um Estado de vigilância, especialmente quando as normativas criam mecanismos obscuros de compartilhamento amplo sem as salvaguardas necessárias para os cidadãos.

Deve-se afastar a ideia de que o cidadão honesto não possui nada a esconder ou a temer a partir da coleta das informações pessoais, num totalitarismo estatal chancelado pela metáfora do "homem de vidro", mas reivindicar que a vigilância seja direcionada contra o ente estatal, agora, sim, num "Estado de vidro", em ampla transparência do exercício das suas funções públicas. Para tal, os titulares devem ser entendidos como protagonistas da transformação buscada, a fim de que a autodeterminação informativa e a proteção de dados pessoais seja garantida a todos.

5. CONCLUSÃO

Como se viu, a atual conjuntura social, em que os dados tornaram-se um dos grandes ativos em disputa, exige uma proteção maior aos cidadãos frente a eventuais danos que possam advir do uso indevido de suas informações. Vive-se, na verdade, em uma sociedade em que a vigilância adotou novos rumos, sendo desenvolvida por um controle executado de forma horizontal pelos próprios indivíduos, muita influenciada pelas novas tecnologias de informação e comunicação. As informações angariadas dos indivíduos, e muitas vezes por eles disponibilizadas, servem, portanto, como matéria-prima do desenvolvimento do capitalismo de vigilância, que utiliza dos dados obtidos para prever e conduzir o comportamento humano.

Dentro desse contexto, há também um constante desenvolvimento de sistemas de vigilância estatais, muitas vezes justificados para fins de segurança pública e combate ao terrorismo, como o Sistema Echelon a nível internaconal e o Córtex no Brasil. Tais programas, contudo, possuem pouca transparência junto à sociedade, servindo, muitas vezes, para fins escusos e, além disso, representam grande perigo se usados para execução de vigilância indevida sobre os cidadãos. Mais recentemente, todavia, desenvolveu-se uma ampla discussão acerca do direito à proteção de dados pessoais, que passou a receber maior respaldo e garantias através de diversos diplomas. Dentre eles, destaca-se a publicação, em 2016, do Regulamento Geral de Proteção de Dados Pessoais com foco na União Europeia e, a nível nacional, da Lei Geral de Proteção de Dados Pessoais em 2018.

Além disso, o desenvolvimento tecnológico também serviu para proporcionar um aumento de eficiência na oferta de serviços pelo Estado. No Brasil, a fim de se criar uma Administração Pública mais digital, o governo vem adotando medidas que contribuam para a execução desse novo modelo, que pressupõe maior interoperabilidade entre os órgãos públicos, em destaque pelo compartilhamento de dados e informações acerca dos cidadãos, bem como sua unificação. Nesse sentido, o Decreto nº 10.046/2019, alterado pelo Decreto nº 11.266/2022, buscou regulamentar essa questão, estabelecendo diretrizes para esse propósito e criando um Cadastro Base do Cidadão, com objetivo de reunir os mais diversos serviços e dados em posse do Poder Público.

O presente trabalho, dessa forma, buscou questionar em que medida a atual forma de desenvolvimento da Administração Pública Digital no Brasil, que pressupõe o compartilhamento e unificação de dados dos cidadãos em posse do Poder Público, é compatível com a Lei Geral de Proteção de Dados Pessoais (LGPD), alicerçada na

privacidade e no direito fundamental à proteção de dados pessoais, considerando o atual contexto da vigilância exercida pelo Estado.

Em um primeiro momento, concluiu-se que, tendo em vista o atual modelo de vigilância exercida na sociedade, com a instauração de um "superpanóptico", os indivíduos necessitam de maior proteção aos seus dados pessoais, em destaque pela sua utilização como ativo digital e, portanto, mercadoria. Nessa linha, há de se conceder ao cidadão o maior controle possível sobre suas informações, garantindo a sua autodeterminação informativa, um dos princípios oriundos do direito à proteção de dados pessoais.

Na sequência, percebeu-se que o desenvolvimento da Administração Pública Digital no país, apesar de necessária, apresenta contornos que causam indagações a seu respeito. A principal delas, relativa ao compartilhamento de dados no âmbito público, se dá em razão dos perigos que podem advir do uso indevido de informações. A esse respeito, o Decreto nº 10.046/2019, alterado pelo Decreto nº 11.266/2022, apresenta incompatibilidades com a Lei Geral de Proteção de Dados Pessoais, principalmente pelo uso de conceitos até então estranhos às suas previsões.

Nessa perspectiva, a referência a dados biográficos e biométricos não são verificáveis na legislação mencionada. Junto disso, o rol apresentado no decreto não é taxativo, permitindo amplas opções para a obtenção de dados pelos mais diversos agentes. Da mesma forma, o aparente distanciamento da ANPD e a emissão de regulações a partir de um "gestor de dados" - nova terminologia que também diverge da LGPD, cujos dispositivos tratam de controlador, operador e encarregado -, proporciona risco à proteção de dados dos cidadãos brasileiros.

Por outro lado, concluiu-se também que os novos rumos da Administração Pública no país não prestigiam o titular de dados. Como já dito, a melhor garantia da sua autodeterminação informativa deve se dar a partir da sua atuação direta junto aos serviços disponibilizados. Nessa lógica, ao indivíduo deve ser oportunizada a escolha de quais dados pretende disponibilizar e para quais serviços e/ou órgãos. Da mesma forma, faz-se necessário que se tenha melhor controle de acesso às informações disponibilizadas, o que não se mostra como foco inicial do Governo Digital no Brasil, que busca a promoção de transparência a partir da abertura de dados, forma que, apesar de importante, não garante total publicidade ao indivíduo visto de forma isolada.

Isto posto, foi verificado que, a fim de garantir seu direito à proteção de dados e evitar que seus direitos sejam violados por eventuais sistemas de vigilância que se utilizem das informações disponibilizadas e unificadas em determinados serviços, ao cidadão deve ser

oportunizado o exercício da contravigilância, detendo controle sobre a Administração Pública e, principalmente, sobre seus próprios dados. Dessa forma, sugeriu-se a adoção de um sistema de serviços oferecidos a partir de um auto perfil do cidadão, o que difere do sistema atual, onde as informações fornecidas aos serviços unificados englobam todos eles, não sendo oportunizada qualquer escolha nesse sentido.

A Autoridade Nacional de Proteção de Dados, por derradeiro, possui papel central nesse contexto, sendo necessário que suas atribuições ultrapassem somente a emissão de orientações e diretrizes. A supervisão e controle, em nome da população, é essencial, pelo que a instituição deve ser fortalecida e com atuação mais presente quanto ao compartilhamento de dados no âmbito do Poder Público.

Ademais, destaca-se que o presente trabalho foi construído em meio à publicação das recentes alterações sobre o tema, principalmente no que concerne ao julgamento da ADPF 695/DF e ADI 6649/DF e a edição do Decreto nº 11.266/2022, o que limitou o tempo de análise e possível adoção de outras perspectivas. Por tal, a percepção acerca dos possíveis efeitos advindos de tais inovações poderão ser analisados em uma pesquisa futura.

REFERÊNCIAS

AFFONSO, Elaine Parra. **A insciência do usuário na fase de coleta de dados:** privacidade em foco. 2018. Tese (Doutorado em Ciência da Informação) – Programa de Pós-Graduação em Ciência da Informação da Faculdade de Filosofia e Ciências, da Universidade Estadual Paulista, Marília, 2018.

AZEVEDO, Cynthia Picolo Gonzaga de; LIMA, Eliz Marina Bariviera de; SILVA, Felipe Rocha da; RODRIGUES, Gustavo Ramos; DUTRA, Luiza Corrêa de Magalhães; SANTARÉM, Paulo Rená da Silva; VIEIRA, Victor Barbieri Rodrigues. **Nota técnica:** análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022. Instituto de Referência em Internet e Sociedade (IRIS) e Laboratório de Políticas Públicas e Internet (LAPIN), novembro de 2022. Disponível em: https://irisbh.com.br/wp-content/uploads/2022/11/Nota-tecnica-Analise-comparativa-entre-o-anteprojeto-de-LGPD-Penal-e-o-PL-1515-2022.pdf. Acesso em: 20 nov. 2022.

BAPTISTA, Patrícia; ANTOUN, Leonardo. Governo Digital: política pública, normas e arranjos institucionais no regime federativo brasileiro: a edição da Lei Federal N. º 14.129/2021 e o desenvolvimento da Política Nacional de Governo Digital. In: **RFD-Revista da Faculdade de Direito da UERJ**, v. 13, n. 41, p. 1-34, 2022. Disponível em: https://www.e-publicacoes.uerj.br/index.php/rfduerj/article/view/70724/43746. Acesso em: 05 nov. 2022.

BAUMAN, Zygmunt. **Vigilância líquida:** diálogos com David Lyon. Rio de Janeiro: Jorge Zahar, 2013.

BENTHAM, Jeremy. **O panóptico.** Belo Horizonte, MG: Grupo Autêntica, 2019.

BRANDEIS, Louis. WARREN, Samuel. **The right to privacy.** Harvard Law Review, v. IV, n. 5, dez. 1890. Disponível em: http://faculty.uml.edu/sgallagher/brandeisprivacy.htm. Acesso em 03 dez. 2022.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília: Presidência da República, [2022]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 30 nov. 2022.

BRASIL. **Decreto nº 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. Brasília: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 03 dez. 2022.

BRASIL. **Decreto nº 11.266, de 25 de novembro de 2022**. Altera o Decreto nº 10.046, de 9 de outubro de 2019, que 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. Brasília: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/decreto/D11266.htm. Acesso em 30 nov. 2022.

BRASIL. Gabinete de Segurança Institucional. Acesso à informação. Institucional. **A ABIN**. Disponível em: https://www.gov.br/abin/pt-br/acesso-a-informacao/institucional/a-abin. Acesso em: 10 nov. 2022.

BRASIL. **Lei n° 12.414, 09 de junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 07 dez. 2022.

BRASIL. **Lei n° 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htmhttp://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.. Acesso em: 17 nov. 2022.

BRASIL. **Lei n° 13.979, de 06 de fevereiro de 2020**. Dispõe sobre as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019. Brasília: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l13979.htm#view. Acesso em: 10 dez. 2022.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em 07 dez. 2022.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 07 dez. 2022.

BRASIL. **Lei nº 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 nº 7.116, de 29 de agosto de 1983, a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), a Lei nº 12.682, de 9 de julho de 2012, e a Lei nº 13.460, de 26 de junho de 2017. Brasília: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm. Acesso em: 10 dez. 2022.

BRASIL. Lei nº 14.460, de 25 de outubro de 2022. **Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados; altera as Leis nºs 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e 13.844, de 18 de junho de 2019; e revoga dispositivos da Lei nº 13.853, de 8 de julho de 2019**. Brasília: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Lei/L14460.htm. Acesso em: 08 dez. 2022.

BRASIL. **Lei nº 7.232, de 29 de outubro de 1984.** Dispõe sobre a Política Nacional de Informática, e dá outras providências. Brasília: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/Leis/L7232.htm. Acesso em: 07 dez. 2022.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 07 dez. 2022.

BRASIL. **Lei nº 9.507, de 12 de novembro de 1997**. Regula o direito de acesso a informações e disciplina o rito processual do *habeas data*. Brasília: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9507.htm#:~:text=LEI%20N%C2%BA%209.507%2C%20DE%2012%20DE%20NOVEMBRO%20DE%201997.&text=Regula%20o%20direito%20de%20acesso,rito%20processual%20do%20habeas%20data. Acesso em: 07 dez. 2022.

BRASIL. **Lei nº 9.883, de 07 de dezembro de 1999**. Institui o Sistma Brasileiro de Inteligência, cria a Agência Brasil de Inteligência - ABIN, e dá outras providências. Brasília: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9883.htm. Acesso em: 22 nov. 2022.

BRASIL. **Medida Provisória nº 954, de 17 de abril de 2020**. Brasília: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm. Acesso em 05 dez. 2022.

BRASIL. Ministério da Economia. Governo Digital. Acesso à informação. **Modelo de Acessibilidade**. Disponível em: https://www.gov.br/governodigital/pt-br/acessibilidade-digital/modelo-de-acessibilidade. Acesso em: 05 nov. 2022.

BRASIL. Ministério da Economia. Governo Digital. Estratégia de governança digital. **Do Eletrônico ao Digital**. Disponível em: https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/do-eletronico-ao-digital. Acesso em: 08 dez. 2022.

BRASIL. Portal da Câmara dos Deputados. **O que é o Sivam?** 12 nov. 2004. Disponível em: https://www.camara.leg.br/noticias/55929-o-que-e-o-sivam/. Acesso em: 01 dez. 2022.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade n° 6649. Decreto 10.046/2019**. Requerente: Conselho Federal da Ordem dos Advogados do Brasil – CFOAB. Relator Ministro Gilmar Mendes, 18 de dezembro de 2020. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6079238. Acesso em 05 Dez. 2022.

BRASIL. Supremo Tribunal Federal. **Arguição de Descumprimento de Preceito Fundamental n° 695. Decreto 10.046/2019**. Requerente: Partido Socialista Brasileiro - PSB . Relator Ministro Gilmar Mendes, 15 de junho de 2020. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5938693. Acesso em 05 Dez. 2022.

BRASIL. Supremo Tribunal Federal. **STF suspende compartilhamento de dados de usuários de telefônicas com IBGE.** Disponível em:

https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442902&ori=1. Acesso em: 05 dez. 2022.

BRUNO, Fernanda. Mapas de crime: vigilância distribuída e participação na cibercultura. **Revista da Associação Nacional dos Programas de PósGraduação em Comunicação E-compós**, Brasília, DF, v. 12, n. 2, p. 1-16, 2009. Disponível em: https://e-compos.emnuvens.com.br/e-compos/article/view/409. Acesso em: 05 dez. 2022.

CANCELIER, Mikhail Vieira de Lorenzi . O direito à privacidade hoje: perspectiva histórica e o cenário brasileiro. In: **Sequência: Estudos Jurídicos e Políticos**, Florianópolis, v. 38, n. 76, p. 213-240, set. 2017. Disponível em: https://periodicos.ufsc.br/index.php/sequencia/article/view/2177-7055.2017v38n76p213. Acesso em: 27 nov. 2022.

CARAM, Bernardo. **BC comunica vazamento de dados pessoais de 160 mil chaves Pix.** Folha de S. Paulo, 21 jan. 2022. Disponível em: https://www1.folha.uol.com.br/mercado/2022/01/bc-comunica-vazamento-de-dados-pessoais-de-160-mil-chaves-pix.shtml. Acesso em: 10 dez. 2022.

CARDOSO, Jessica. **Entenda o que significa a extradição de Assange para os EUA**. Poder 360, 22 jun. 2022. Disponível em: https://www.poder360.com.br/internacional/entenda-o-que-significa-a-extradicao-de-assange-para-os-eua/. Acesso em 21 out. 2022.

CARIBÉ, João Carlos Rebello. Uma perspectiva histórica e sistêmica do capitalismo de vigilância. **Revista Inteligência Empresarial**, v. 41, p. 5-13, 2019. Disponível em: https://inteligenciaempresarial.emnuvens.com.br/rie/article/view/88. Acesso em 25 nov. 2022.

CARPANEZ, Juliana. **Votação via internet, identidade universal e histórico médico online: o que faz da Estônia um país digital.** Portal UOL, 25 fev. 2018. Disponível em: https://noticias.uol.com.br/internacional/ultimas-noticias/2018/02/25/estonia-como-e-a-sociedade-digital-sem-burocracia-prometida-ao-resto-do-planeta.htm. Acesso em: 11 dez. 2022.

CARPENTIERI, José Rafael. A Abin e o que restou da ditadura: O problema do controle das forças coercitivas do Estado brasileiro. In: **Dilemas-Revista de Estudos de Conflito e Controle Social**, v. 10, n. 2, p. 323-351, 2017.

CASIMIRO, Sofia de Vasconcelos. Novas guerras em novos campos de batalha: o RGPD Europeu e as gigantes tecnológicas norte-americanas. WACHOWICZ, Marcos (Org.). **Proteção de dados pessoais em perspectiva:** LGPD e RGPD na ótica do direito comparado. Curitiba: Gedai, UFPR, 2020. p. 104-125.

CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. **O CNMP e as boas práticas de combate à corrupção e de gestão e governança dos Ministérios Públicos**. Brasília, 2. ed., 2021. Disponível em: https://www.cnmp.mp.br/portal/images/Publicacoes/documentos/2021/CARTILHA_BOAS_PRATICAS_WEB_final.pdf. Acesso em: 05 nov. 2022.

COSTA, Rogério da. Sociedade de controle. In: **São Paulo em perspectiva**, v. 18, p. 161-167, 2004. Disponível em:

https://www.scielo.br/j/spp/a/ZrkVhBTNkzkJr9jVw6TygVC/?format=html. Acesso em: 05 nov. 2022.

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**, [S.l.], v. 6, n. 1, p. 1-24, jan.-jun. 2020.

DE LUCA, Cristina. **Decreto de Bolsonaro aproxima uso de nossos dados a países como China**. Portal UOL. Disponível em: https://porta23.blogosfera.uol.com.br/2019/10/13/governo-tem-nossos-dados-mas-nao-deve-trata-los-como-se-fosse-o-dono-deles/?cm. Acesso em: 10 dez. 2022.

DATA PRIVACY BRASIL. Comissão Mista Da Medida Provisória nº 869, de 2018, segunda audiência pública. **Tratamento de dados pela Administração Pública e Proteção de dados relativos à defesa e segurança pública** .Disponível em: https://legis.senado.leg.br/sdleg-getter/documento/download/6f7ee87d-306b-4e9f-978a-51bbcd61fbcb. Acesso em: 15 dez. 2022.

DELEUZE, Gilles. **Conversações**: 1972-1990. São Paulo: 34, 1992.

DIAS, Tatiana; MARTINS, Rafael Moro. **Documentos vazados mostram que ABIN pediu ao SERPRO dados e fotos de todas as CNHs do país.** The Intercept Brasil. 06 jun. 2020. Disponível: https://theintercept.com/2020/06/06/abin-carteira-motorista-serpro-vigilancia/. Acesso em: 23 nov. 2022.

DIFERENÇA entre Machine learning e Deep learning. **PUCRS Online**. Porto Alegre, 20 out. 2020. Disponível em: https://online.pucrs.br/blog/public/diferenca-entre-machine-learning-e-deep-learning. Acesso em: 26 out. 2022.

DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. In: **Espaço Jurídico**, Joaçaba, v. 12, n. 2, pp. 91-108, jul./dez. 2011.. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 11 nov. 2022.

DONEDA, Danilo. Privacidade, vida privada e intimidade no ordenamento jurídico brasileiro. Da emergência de uma revisão conceitual e da tutela de dados pessoais. In: **Âmbito Jurídico**, Rio Grande, v. XI, n. 51, mar. 2008. Disponível em: http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=2460. Acesso em: 25 nov. 2022.

EUA grampearam Dilma, ex-ministros e avião presidencial, revela WikiLeaks. **Portal G1.** Brasília, 07 jul. 2015 Disponível em: https://g1.globo.com/politica/noticia/2015/07/lista-revela-29-integrantes-do-governo-dilma-espionados-pelos-eua.html Acesso em: 22 out. 2022.

FAUS, Joan. **Libertada Chelsea Manning, soldado que revelou segredos ao Wikileaks**. El País, 17 mai. 2017. Disponível em: https://brasil.elpais.com/brasil/2017/05/17/internacional/1494976665_612495.html. Acesso em: 25 out. 2022.

FIGUEIREDO, Lucas. **O Grande Irmão: Abin tem megabanco de dados sobre movimentos sociais**. The Intercept Brasil, 05 dez. 2016. Disponível em: https://theintercept.com/2016/12/05/abin-tem-megabanco-de-dados-sobre-movimentos-sociais/. Acesso em: 16 nov. 2022.

FIORETTI, Julia. **Agência espiã britânica coletou imagens de chats com webcam do Yahoo!, diz The Guardian.** Portal UOL. Disponível em: https://noticias.uol.com.br/ultimas-noticias/reuters/2014/02/27/agencia-espia-britanica-coletou-imagens-de-chats-com-webcam-do-yahoo-diz-the-guardian.htm. Acesso em: 22 out. 2022.

FOUCAULT, Michel. **Em defesa da sociedade:** curso no Collège de France (1975-1976). 4. ed. São Paulo: Martins Fontes, 2005.

FOUCAULT, Michel. **Vigiar e punir:** nascimento da prisão; tradução de Raquel Ramalhete. 42 ed. Petrópolis, RJ: Vozes, 2014.

FRANCISCO, Pedro Augusto P.; VENTURINI, Jamila. **Privacidade, Vigilância e Inteligência no Brasil:** O marco legal e suas lacunas. 2017. Disponível em: https://bibliotecadigital.fgv.br/dspace/handle/10438/20410. Acesso em: 12 nov. 2022.

FRAZÃO, Pedro Henrique Oliveira et al. **Um big brother global?** os programas de vigilância da NSA à luz da securitização dos espaços sociotecnológicos. 2016. Dissertação (Mestrado em Relações Internacionais) - Programa de Pós-Graduação em Relações Internacionais da Universidade Estadual da Paraíba, 2016. Disponível em: https://pos-graduacao.uepb.edu.br/ppgri/files/2012/02/Pedro-Fraz%C3%A3o.pdf. Acesso em 22/10/2022.

GOOGLE. Ajuda no Google Ads. Central de Ajuda. Começar a anunciar. Glossário. **Cookie:** definição. Disponível em: https://support.google.com/google-ads/answer/2407785?hl=pt-BR#:~:text=Um%20pequeno%20arquivo%20que%20%C3%A9,da%20Web%20que%20elas%20visitamF. Acesso em: 30 nov. 2022.

GREENWALD, Gleen. **Sem lugar para se esconder:** Edward Snowden, a NSA e a espionagem do governo americano. Rio de Janeiro: Sextante, 2014.

GULARTE, Jeniffer. **Conheça o Córtex, plataforma criada pelo governo para vigiar os cidadãos.** Crusoé. Disponível em: https://crusoe.uol.com.br/edicoes/195/big-brother-federal/. Acesso em: 10 nov. 2022.

LOURENÇÃO, Humberto José. O "Echelon System" no processo de contratação do Sistema De Vigilância Da Amazônia (SIVAM). In: **Perspectivas em Ciências Tecnológicas**, v. 2, n. 2, Mar. 2013, p. 75-96. Disponível em: https://fatece.edu.br/arquivos/arquivos-revistas/perspectiva/volume2/5.pdf. Acesso em: 06 nov. 2022.

LYON, David. Cultura da vigilância: envolvimento, exposição e ética na modernidade digital. In: BRUNO, Fernanda; CARDOSO, Bruno; KANASHIRO, Marta; GUILHON, Luciana; MELGAÇO, Lucas (Org.). **Tecnopolíticas da vigilância:** perspectivas da margem. São Paulo: Boitempo, 2018, p. 153-181.

MAIOR, Suetoni Souto. **Saiba o que é Pandora, o sistema criado e usado pelo Gaeco e outros órgãos para desvendar crimes na Paraíba.** Suetoni Souto Maior, 23 abr. 2022. Disponível em: https://suetonisoutomaior.com.br/saiba-o-que-e-pandora-o-sistema-criado-e-usado-pelo-gaeco-e-outros-orgaos-para-desvendar-crimes-na-paraiba/. Acesso em: 10 nov. 2022.

MOISINHO, Aline M. et al. Modelo Conceitual para Sistemas de Recomendação voltados a Governo Eletrônico com o uso do Cadastro Base do Cidadão. In: **Anais do IX Workshop de Computação Aplicada em Governo Eletrônico**. SBC, 2021. p. 215-226.

MORENO, Ana Carolina; MORONI, Alyohha. **Além da Saúde, CGU, PRF e IFPR também confirmaram invasão por grupo hacker.** Portal G1, 14 dez. 2021. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/12/14/alem-da-saude-cgu-prf-e-ifpr-tambem-confirmaram-invasao-por-grupo-hacker.ghtml. Acesso em 07 dez. 2022.

NORTON-TAYLOR, Richard. ***Not so secret:*** *deal at the heart of UK-US intelligence*. The Guardian, 25 jun. 2010. Disponível em: https://www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released. Acesso em: 20 nov. 2022.

NOVA falha do Ministério da Saúde expõe dados de 243 milhões de brasileiros na internet, diz jornal. **Portal G1.** Rio de Janeiro, 02 dez. 2020. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2020/12/02/nova-falha-do-ministerio-da-saude-expoe-dados-de-243-milhoes-de-brasileiros-na-internet-diz-jornal.ghtml. Acesso em: 05 dez. 2022.

PARAÍBA. Ministério Público do Estado da Paraíba. **MPVirtual, Pandora e Thoth:** sistemas do MPPB ganham destaque em cartilha do CNMP. Portal MPPB, 21 mai. 2021. Disponível em: https://www.mppb.mp.br/index.php/38-noticias/procuradoria-geral/23337-tres-sistemas-criados-pelo-mppb-ganham-destaque-nacional-em-cartilha-sobre-boas-praticas-sobre-gestao-governanca-e-combate-a-corrupcao. Acesso em: 14 nov. 2022.

PESSOA, João Pedro Seefeldt. **O efeito Orwell na sociedade em rede:** cibersegurança, regime global de vigilância social e direito à privacidade no século XXI. Porto Alegre: Editora Fi, 2020.

PESSOA, João Pedro Seefeldt. **Verás que um filho teu não foge à luta:** a contravigilância na sociedade em rede e a nova ação conectiva dos movimentos sociais do século XXI. Porto Alegre: Editora Fi, 2021.

REBELLO, Aiuri. **Conheça o Córtex, sistema de vigilância do governo que integra de placa de carro a dados de emprego**. The Intercept Brasil, 21 set. 2020. Disponível em: https://theintercept.com/2020/09/21/governo-vigilancia-cortex/. Acesso em: 15 nov. 2022.

REINO UNIDO começa a julgar extradição de Assange. **Portal G1**. Disponível em: https://g1.globo.com/mundo/noticia/2020/02/24/reino-unido-comeca-a-julgar-extradicao-de-assange.ghtml. Acesso em 21 out. 2022.

RIO DE JANEIRO. Ministério Público do Estado do Rio de Janeiro. Elaboração de parecer sobre a legalidade dos Decretos nº 10.046/2019 e nº 10.047/2019 em face das normas que disciplinam os direitos fundamentais à proteção de dados e à privacidade no ordenamento jurídico brasileiro. In: **Revista do Ministério Público do Estado do Rio de Janeiro,** v. 75, jan./mar. 2020. Disponível em: https://www.mprj.mp.br/documents/20184/1606722/Lucia_Maria_Teixeira_Ferreira.pdf. Acesso em: 12 dez. 2022.

RIO GRANDE DO SUL. Tribunal de Justiça do Estado do Rio Grande do Sul. Sistema de Consultas Integradas. **Manual do Usuário**. PROCERGS, jan. 2004. Disponível em: https://www.tjrs.jus.br/novo/download/?arquivo_id=23493. Acesso em: 27 nov. 2022.

RODOTÁ, Stefano. **A vida na sociedade de vigilância:** a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RUARO, Regina Linden. Algumas reflexões em torno do RGPD, em especial quanto ao consentimento, com alusões à lgpd (um exercício interpretativo). In: **Direitos Fundamentais & Justiça**, Belo Horizonte, ano 14, n. 42, 2020, p. 219-249.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. O direito à proteção dos dados pessoais: uma leitura do sistema europeu e a necessária tutela dos dados sensíveis como paradigma para um sistema jurídico brasileiro. In: **Direitos Fundamentais & Justiça**. Programa de Pós-Graduação Mestrado e Doutorado em Direito da PUCRS. Porto Alegre, ano 4, n. 11, p. 162-180, abr./jun. 2010.

SANTANNA, Gustavo da Silva. **Do Patrimonialismo à sociedade da informação:** proposições para a implantação da administração pública eletrônica (e-administração) no Brasil. Tese (Doutorado em direito) - Universidade do Vale do Rio dos Sinos. Programa de Pós-graduação em direito. São Leopoldo, RS, 2019.

SÃO PAULO faz parceria com operadoras de telefonia para monitorar quarentena. **CNN Brasil**, São Paulo, 09 abr. 2020. Disponível em: https://www.cnnbrasil.com.br/nacional/sao-paulo-faz-parceria-com-operadoras-de-telefonia-para-monitorar-quarentena/. Acesso em: 05 dez. 2022.

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. Direitos Fundamentais & Justiça, Belo Horizonte, ano 14, n. 42, 2020, p. 189-218.

SECRETARIA-GERAL IBERO-AMERICANA. **XIII Cimeira Ibero-Americana de Chefes de Estado e de Governo. Declaração de Santa Cruz de La Sierra de 14 e 15 de novembro de 2003**. Disponível em: https://www.segib.org/wp-content/uploads/DECLARASAO-STA-CRUZ-SIERRA.pdf. Acesso em 14 dez. 2022.

SILVEIRA, Alessandra; MARQUES, João. Do direito a estar só ao direito ao esquecimento. Considerações sobre a proteção de dados pessoais informatizados no Direito da União Europeia: sentido, evolução e reforma legislativa. In: **Revista da Faculdade de**

Direito da UFPR. Curitiba, v. 61, n. 3, pp. 91 - 118, 2016. Disponível em: https://revistas.ufpr.br/direito/article/view/48085/29828 . Acesso em: 30 nov. de 2022.

SISTEMA com dados sigilosos é acessado por 49 órgãos, diz secretário de Segurança do RS. **GauchaZH**, 06 set. 2010. Disponível em: https://gauchazh.clicrbs.com.br/geral/noticia/2010/09/sistema-com-dados-sigilosos-e-acessado-por-49-orgaos-diz-secretario-de-seguranca-do-rs-3030814.html. Acesso em: 05 dez. 2022.

TOLEDO, Diego. **Ataques cibernéticos a órgãos públicos alertam para riscos de vazamento de dados.** CNN Brasil, 20 dez. 2021. Disponível em: https://www.cnnbrasil.com.br/tecnologia/podcast-e-tem-mais-ataques-ciberneticos-a-orgaos-publicos-alertam-para-riscos-de-vazamento-de-dados/. Acesso: 07 dez. 2022.

UNIÃO EUROPEIA. Conselho da Europa. **Chart of signatures and ratifications of Treaty 108.** Disponível em: https://www.coe.int/en/web/portal/home. Acesso em 30 nov. 2022.

UNIÃO EUROPEIA. Corte Europeia de Direitos Humanos. ***Case of Big Brother Watch and Others v. The United Kingdom*** **(Applications nº. 58170/13, 62322/14 and 24960/15).** Recorrente: Big Brother Watch e Outros. Recorrido: Reino Unido. Presidente: Juiz Linos-Alexandre Sicilianos. Estrasburgo, França, 13 de setembro de 2018. Disponível em: http://hudoc.echr.coe.int/eng?i=001-186048. Acesso em: 16 abr. 2019

UNIÃO EUROPEIA. Parlamento Europeu. **Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016L0680. Acesso em 3 dez. 2022.

UNIÃO EUROPEIA. Parlamento Europeu. **Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas (Diretiva relativa à privacidade e às comunicações eletrônicas)**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32002L0058. Acesso em: 30 nov. 2022.

UNIÃO EUROPEIA. Parlamento Europeu. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados**. Disponível em: https://eur-lex.europa.eu/PT/legal-content/summary/protection-of-personal-data.html. Acesso em: 30 nov. 2022.

UNIÃO EUROPEIA. Parlamento Europeu. **Relatório de 11 de julho de 2001 sobre a existência de um sistema global de interceptação de comunicações privadas e econômicas (sistema de interceptação "ECHELON")**. Disponível em: https://www.europarl.europa.eu/doceo/document/A-5-2001-0264_PT.html?redirect. Acesso em: 05 dez. 2022.

UNIÃO EUROPEIA. Parlamento Europeu. **Tratado sobre o funcionamento da União Europeia (versão consolidada).** Jornal Oficial da União Europeia, v. 7, 2016. Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF. Acesso em 30 nov. 2022.

UNIÃO EUROPEIA. Tribunal de Justiça. **Acórdão (Grande Sessão) de 16 de julho de 2020: Data Protection Commissioner contra Facebook Ireland Ltd e Maximillian Schrems (processo C-311/18)**. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CJ0311&qid=1606742479317. Acesso em 30 nov. 2022.

VAIDHYANATHAN, Siva. **A Googlelização de tudo:** (e por que devemos nos preocupar) : a ameaça do controle total da informação por meio da maior e mais bem sucedida empresa do mundo virtual; tradução de Jeferson Luiz Camargo. São Paulo: Cultrix, 2011.

VALENÇA, Lucas. **Empresa de software espião Pegasus abandona licitação do governo**. Portal UOL, 25 mai. 2021. Disponível em: https://noticias.uol.com.br/politica/ultimas-noticias/2021/05/25/empresa-de-software-espiaopegasus-deixa-edital-que-e-rodeado-de-incertezas.htm. Acesso em: 27 nov. 2022.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação.** 2007. 297 p. Dissertação (Mestrado) - Universidade de Brasília, Faculdade de Direito, Programa de Pós Graduação em Direito, Estado e Sociedade, 2007. Disponível em: https://repositorio.unb.br/handle/10482/3358. Acesso em: 25 nov. 2022.

WEBER, Max. **Economia e sociedade**: fundamentos da sociologia compreensiva, vol. II. Brasília, DF: Editora Universidade de Brasília, 2004.

WIKILEAKS. **What is WikiLeaks.** Disponível em: https://wikileaks.org/What-is-Wikileaks.html. Acesso em: 15 nov. 2022.

ZANATTA, Rafael A. F. **O que sabemos sobre a Harpia Tech?** Data Privacy Brasil Research. 10 jun. 2022. Disponível em: https://www.dataprivacybr.org/o-que-sabemos-sobre-a-harpia-tech/. Acesso em: 15 nov. 2022.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância:** a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro, RJ: Intrínseca, 2021.

ZUBOFF, Shoshana. Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação. In: BRUNO, Fernanda; CARDOSO, Bruno; KANASHIRO, Marta; GUILHON, Luciana; MELGAÇO, Lucas (Org.). **Tecnopolíticas da vigilância:** perspectivas da margem. São Paulo: Boitempo, 2018, p. 17-68.