SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE SERGIPE
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

NATHALIA MYLENA FARIAS SANTOS

ADMINISTRAÇÃO PÚBLICA 4.0: O DEVER DE PROTEÇÃO DE DADOS PESSOAIS INTERLIGADO AOS DEVERES DE ACESSO À INFORMAÇÃO, PUBLICIDADE E CIBERTRANSPARÊNCIA

São Cristóvão
2023

NATHALIA MYLENA FARIAS SANTOS

ADMINISTRAÇÃO PÚBLICA 4.0: O DEVER DE PROTEÇÃO DE DADOS PESSOAIS INTERLIGADO AOS DEVERES DE ACESSO À INFORMAÇÃO, PUBLICIDADE E CIBERTRANSPARÊNCIA

Dissertação apresentada ao Curso de Pós-Graduação *stricto sensu* em Direito da Universidade Federal de Sergipe, exigida como requisito para a obtenção do grau de Mestre em Direito. Área de concentração: Constitucionalização do Direito. Linha de Pesquisa: Eficácia dos direitos fundamentais e seus reflexos nas relações sociais e empresariais.

Orientador (a): Profª Drª Clara Angélica Gonçalves Cavalcanti Dias.

São Cristóvão

2023

NATHALIA MYLENA FARIAS SANTOS

ADMINISTRAÇÃO PÚBLICA 4.0: O DEVER DE PROTEÇÃO DE DADOS PESSOAIS INTERLIGADO AOS DEVERES DE ACESSO À INFORMAÇÃO, PUBLICIDADE E CIBERTRANSPARÊNCIA

Dissertação apresentada ao Programa de Pós-Graduação em Direito (PRODIR) da Universidade Federal de Sergipe, como parte dos requisitos para a obtenção do título de Mestre em Direito.
Essa Dissertação foi julgada e assinada pela comissão abaixo:

Aprovada em _____ de _____ de 2023.

BANCA EXAMINADORA

_____

Universidade Federal de Sergipe

_____

Universidade Federal de Sergipe

_____

Universidade Federal de Sergipe

São Cristóvão

2023

À Deus.
À minha mãe, Sueli Farias.
À minha avó, Ivone Farias.

AGRADECIMENTOS

Inauguro esta seção agradecendo a Deus, o Senhor, cujo amparo e proteção permitiram-me e permitem, a concretização de meus sonhos. Ressalto, inclusive, passagem na Bíblia em Mateus 21:22, "*E tudo o que pedirdes na oração, crendo, o recebereis*".

Desde a Graduação, cursada na Universidade Tiradentes (UNIT/SE), desenvolvi uma paixão pela área da pesquisa, ao longo dos períodos participei de grupos de pesquisa e apresentei trabalhos científicos.

De lá para cá, o sonho de fazer um Mestrado restou adormecido em virtude da dedicação a outros projetos pessoais, outras especializações. No ano de 2020, resolvi participar da seleção de Mestrado da Universidade Federal de Sergipe, após concluir uma de minhas especializações. Foi a primeira e única tentativa de participar do processo seletivo pois, para a honra e glória do Senhor, obtive êxito.

Recordo-me de vibrar a cada etapa ao longo processo seletivo, a alegria ao ver meu nome etapa após etapa, até a publicação do resultado final. Passado o êxtase da aprovação, novos desafios tiveram de ser enfrentados, com a Pandemia da COVID-19, todo o processo seletivo e a maior parte das aulas tiveram de ser realizadas de forma síncrona.

Em que pese os desafios, o Mestrado em Direito na UFS proporcionou muito mais alegrias, a ampliação e difusão do conhecimento, conhecimento este, adquirido através das aulas com a apresentação dos temas pelos colegas, cada um dedicado à sua linha de pesquisa.

Desta feita, ratifico meu agradecimento a Deus, que sempre segurou a minha mão e não permitiu que eu sucumbisse perante tais desafios. Agradeço a minha família, meu alicerce, minha rede de apoio, especialmente minha mãe, Sueli Farias, por todo o apoio incondicional, a minha avó Ivone, minhas tias Cristiane, Solange e Jaqueline, por sempre demonstrarem orgulho com minhas conquistas e aos meus primos que tenho como irmãos, Ariany Mylena e João Miguel, saibam que busco o melhor em mim para vocês a cada dia.

Agradeço também ao Programa de Pós-Graduação em Direito da Universidade Federal de Sergipe (PRODIR/UFS), à Nayara, competentíssima Secretária, sempre disposta a orientar a todos que a procuram; aos professores: Pedro Durão, Ubirajara Coelho, Flávia Pessoa, Henrique Cardoso, Tanize Zago, Lucas Gonçalves e Carlos Augusto Machado, os quais contribuíram sobremaneira para o desenvolvimento da minha Dissertação e, mais ainda, no meu desenvolvimento pessoal.

À minha orientadora, exemplo de ser humano e profissional, ética e compromissada, gentil e atenciosa, Clara Angélica Gonçalves Cavalcanti Dias. Impressionante como Deus nos guia à

presença de pessoas tão especiais. Antes mesmo de ingressar no Mestrado da UFS já havia decidido quem seria a minha orientadora, sua reputação ilibada e o carinho que as pessoas nutrem por Clara ultrapassam em muito, as barreiras físicas da UFS. Grata por todo o aprendizado, pelas oportunidades, inclusive o estágio docência e, sobretudo, por toda atenção e carinho.

Aos meus colegas do PRODIR/UFS sou grata pelo tempo que passamos juntos, por se fazerem presentes mesmo durante as aulas síncronas, assim como agradeço os conselhos, as trocas de conhecimento e o apoio no decorrer da nossa trajetória.

Por fim, agradeço aos membros da minha banca examinadora de Mestrado, à minha orientadora, Presidente da banca, Prof.ª Dr ª Clara Angélica Gonçalves Cavalcanti Dias e aos titulares Prof. ª Dr ª Tanize Zago Thomasi, a Prof.ª Dr ª Rita de Cássia Barros de Menezes e o Prof. º Dr. Diogo de Calasans Melo Andrade pelo respeito à integridade de meu trabalho, à gentileza nas recomendações e o carinho que demonstraram por mim e pela minha trajetória na área acadêmica.

Não se deve encarar os regimes referentes à proteção de dados pessoais de forma diversa caso seja o Estado ou então entes privados que realizem o tratamento de dados pessoais. Eventuais diferenças de tratamento somente serão justificadas caso tenham como objetivo a obtenção de um patamar idêntico de proteção para a pessoa.

Danilo Doneda (in memoriam)

RESUMO

Hodiernamente, a sociedade vivencia a intitulada Quarta Revolução Industrial ou Revolução 4.0 onde as novas tecnologias disruptivas ganham relevante destaque. Nessa conjuntura, destaca-se o papel da Administração Pública com a prestação digital de serviços públicos e a necessidade de assegurar os direitos e garantias fundamentais dos cidadãos bem como os deveres constitucionais administrativos. Ante o exposto, visa o presente trabalho demonstrar os impactos da atuação estatal no ciberespaço, isto é, a Administração Pública 4.0, correlacionando-se o direito fundamental à proteção de dados pessoais e os deveres de acesso público à informação, da publicidade e da cibertransparência. Assim, a contribuição da presente pesquisa revela a necessidade de adoção de mecanismos de Governança, da Governança de Dados, das boas práticas e do *compliance* com vistas a assegurar o devido respeito aos deveres constitucionais outrora citados. Ademais, ressalta-se também instrumentos que viabilizam esses mecanismos, tais como as técnicas 5W+1H+SHOW ME, abordagem *lean*, *benchmarking* e ciclo PDCA. Para tanto, o tipo de pesquisa empregado foi a pesquisa exploratória, com o objetivo de investigar conteúdo referente ao tema proposto. Quanto à abordagem, utilizou-se a metodologia qualitativa pois, buscou-se a análise de aspectos qualitativos sobre o tema, como instrumentos normativos e entendimentos doutrinários e jurisprudenciais. No que pertine à técnica utilizada como instrumento para conduzir aos objetivos da pesquisa, cita-se a pesquisa bibliográfica, em razão da utilização de materiais já publicados como livros, artigos e periódicos, bem como a utilização de legislação correlata ao tema.

Palavras-chave: Administração Pública 4.0; proteção de dados pessoais; acesso à informação; publicidade; cibertransparência.

ABSTRACT

Nowadays, society is experiencing the so-called Fourth Industrial Revolution or Revolution 4.0 where new disruptive technologies gain relevant prominence. In this context, the role of Public Administration stands out with the digital provision of public services and the need to ensure the fundamental rights and guarantees of citizens, as well as administrative constitutional duties. In view of the above, the present work aims to demonstrate the impacts of state action in cyberspace, that is, Public Administration 4.0, correlating the fundamental right to the protection of personal data and the duties of public access to information, publicity and cybertransparency. Thus, the contribution of this research reveals the need to adopt mechanisms of Governance, Data Governance, good practices and compliance with a view to ensuring due respect for the aforementioned constitutional duties. Furthermore, instruments that enable these mechanisms are also highlighted, such as the 5W+1H+SHOW ME techniques, lean approach, benchmarking and PDCA cycle. Therefore, the type of research employed was exploratory research, with the objective of investigating content related to the proposed theme. As for the approach, the qualitative methodology was used, since the analysis of qualitative aspects on the subject was sought, such as normative instruments and doctrinal and jurisprudential understandings. With regard to the technique used as an instrument to conduct the research objectives, bibliographical research is cited, due to the use of already published materials such as books, articles and periodicals, as well as the use of legislation related to the theme.

Keywords: Public Administration 4.0; personal data protection; access to information; publicity; cybertransparency.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

ADI – Ação Direta de Inconstitucionalidade

ANPD – Autoridade Nacional de Proteção de Dados

CDC – Código de Defesa do Consumidor

CF – Constituição Federal

CGU – Controladoria Geral da União

CNJ – Conselho Nacional de Justiça

CNPD – Conselho Nacional de Proteção de Dados e da Privacidade

EC – Emenda Constitucional

GDPR – *General Data Protection Regulation*

IA – Inteligência Artificial

IOT – *Internet of Things* (Internet das Coisas)

ISO – *International Organization for Standardization*

LAI – Lei de Acesso à Informação

LGPD – Lei Geral de Proteção de Dados

LINDB – Lei de Introdução às Normas do Direito Brasileiro

LRF – Lei de Responsabilidade Fiscal

MCI – Marco Civil da Internet

MP – Medida Provisória

OCDE – Organização para a Cooperação e Desenvolvimento Econômico

OEA – Organização dos Estados Americanos

ONU – Organização das Nações Unidas

PL – Projeto de Lei

PNSI – Política Nacional de Segurança da Informação

RE – Recurso Extraordinário

RESP – Recurso Especial

RGPD – Regulamento Geral de Proteção de Dados

SGSI – Sistema de Gestão em Segurança da Informação

STF– Supremo Tribunal Federal

STJ – Superior Tribunal de Justiça

TCU – Tribunal de Contas da União

TIC – Tecnologia de Informação e Comunicação

TJRS – Tribunal de Justiça do Rio Grande do Sul

SUMÁRIO

INTRODUÇÃO

A sociedade passou por diversas mudanças que impactaram as relações sociais, culturais, econômicas e ambientais, as Revoluções Industriais são claros exemplos dessas transformações. A Quarta Revolução Industrial, em especial, ganha novos contornos, pois enseja debates acerca da necessidade de releitura de direitos fundamentais e até mesmo, da necessidade de reconhecimento de novos direitos.

A Quarta Revolução Industrial pode ser denominada também de Revolução 4.0 ou, Revolução Digital. Trata-se do desenvolvimento e da inserção de novas tecnologias disruptivas na sociedade informacional.

Nessa conjuntura, destaca-se o papel da Administração Pública com a prestação digital de serviços públicos e a necessidade de assegurar os direitos e garantias fundamentais dos cidadãos bem como os deveres constitucionais administrativos.

Em particular, o presente trabalho pretende responder ao seguinte questionamento: Quais os limites de atuação da Administração Pública com vistas a assegurar o direito fundamental à proteção de dados pessoais sem prejuízo da observância dos deveres de acesso à informação, publicidade e cibertransparência, haja vista a esfera estatal não se encontrar imune a possíveis incidentes de segurança?

No que pertine ao objetivo geral, o presente trabalho visa demonstrar a necessidade de adoção de mecanismos assecuratórios à implementação da Lei Geral de Proteção de Dados (LGPD) nas Organizações Públicas em consonância com os deveres outrora citados.

Quanto aos objetivos específicos, propõe-se, compreender o fenômeno da Revolução 4.0 e como esta se relaciona com a Administração Pública; discutir aspectos da LGPD, em especial as hipóteses de tratamento de dados pessoais; bem como identificar os mecanismos que podem contribuir para a promoção do direito fundamental à proteção de dados pessoais dos titulares alinhado aos deveres de acesso à informação, publicidade e cibertransparência.

Para tanto, inicia-se o estudo da Administração Pública 4.0 mediante o uso de novas tecnologias aliadas a gestão governamental, apresentando-se o contexto histórico e as características da Revolução Digital, assim como as normas pertinentes à prestação digital de serviços públicos, como a Lei que instituiu o Governo Digital e a necessidade de inclusão digital enquanto pressuposto para o aumento da eficiência pública, do controle social e da *accountability*.

Em seguida, o estudo será a respeito do direito fundamental à proteção de dados pessoais e dos deveres de acesso à informação, da publicidade e da cibertransparência. Para tanto, discorrer-se-á, inicialmente, sobre a estrutura normativa da proteção de dados pessoais no ordenamento jurídico brasileiro. Então, passa-se ao estudo da proteção de dados no cenário internacional, passando-se ao estudo do tema do dever de acesso público à informação no contexto interno e externo vinculando-o aos princípios da publicidade e da cibertransparência.

Posteriormente, avança-se ao estudo do tratamento de dados pessoais pela Administração Pública sob a égide da Lei Geral de Proteção de Dados (LGPD), aludindo-se, primeiramente, a aspectos da referida lei e, seguidamente, ao tratamento de dados pessoais para, então, adentrar ao tema específico do tratamento de dados pessoais realizado pelo Poder Público.

No último capítulo, o presente trabalho concluirá sobre medidas assecuratórias para a proteção de dados pessoais na Administração Pública 4.0. Na ocasião reportar-se à ao papel da Governança e da Governança de Dados, bem como ao papel da segurança, das boas práticas e do *compliance*, finalizando o estudo com a necessária distinção entre os dados abertos, regulamentados pelo Poder Público, e os dados pessoais, com definição na LGPD, para a efetivação do direito fundamental à proteção de dados pessoais, sem prejuízo da efetivação dos deveres de acesso público à informação, da publicidade e da cibertransparência.

1 ADMINISTRAÇÃO PÚBLICA 4.0: PROTEÇÃO DE DADOS PESSOAIS E A PROMOÇÃO DE UM GOVERNO DIGITAL

Hodiernamente, vivenciamos a intitulada Revolução 4.0 com escopo na 4ª Revolução Industrial, decorrente das transformações oriundas da criação da internet, repercutindo nas searas social, econômica, cultural e ambiental.

A era *ciber* desencadeia um novo cenário sem o qual não se cogita sua ausência, com a criação e o constante aprimoramento de novas tecnologias tidas como disruptivas, ocasionando quebra de paradigmas.

Esse novo cenário pode ser verificado mediante o uso da Inteligência Artificial[1] (IA) e de *softwares*, seja na iniciativa privada seja no setor público, com a criação de *bots* (robôs)*; chatbots* (robôs de conversação)*;* Internet das Coisas (IoT em inglês); bancos digitais; prestação digital de serviços públicos; prestação de serviços *online,* tais como a oferta de cursos de Graduação, Pós-Graduação e de curta duração e de compra e venda; processo eletrônico, dentre outros.

Em decorrência disso, emergem novos paradigmas, com destaque para a cibertransparência, a ciberdemocracia, a advocacia 4.0 e a Administração Pública 4.0. Esses novos paradigmas resultantes da Revolução Digital precisam resguardar os direitos e garantias fundamentais, sobretudo, em razão da latente vulnerabilidade que se perfaz no ambiente virtual ante os incidentes de segurança, caracterizados pelo vazamento de dados pessoais, ciberataques, cibercrimes e acessos não autorizados.

Por diversas vezes, o interesse particular e o interesse público são colocados em xeque, com isso, na análise do caso concreto, esses interesses são sopesados e o interesse público é priorizado sob o fundamento do princípio da supremacia do interesse público sobre o interesse privado.

Ocorre que, quando se trata da preservação de dados pessoais, a dicotomia interesse público *versus* interesse privado toma contornos mais complexos. Não só pelo fato de a proteção dos dados pessoais consistir em um dever de todos que realizam sua coleta, armazenamento, uso e tratamento, mas também pelo fato de que a Administração Pública, além desse dever, possui outros, como o dever de acesso à informação, de transparência e publicidade nas suas ações.

A discussão sobre os dados pessoais deriva do desenvolvimento de novas tecnologias, o qual Klaus Schwab intitula quarta revolução industrial, baseada na revolução digital e "caracterizada por uma internet mais ubíqua e móvel, por sensores menores e mais poderosos que se tornaram mais baratos e pela inteligência artificial e aprendizagem automática (ou aprendizado de máquina)" (SCHWAB, 2016, p. 19).

Nesse sentido, afirma:

> A tecnologia não é uma força externa, sobre a qual não temos nenhum controle. Não estamos limitados por uma escolha binária entre "aceitar e viver com ela" ou

1 Segundo Martha Gabriel Inteligência Artificial (IA) "é a área da Ciência da Computação que lida com o desenvolvimento de máquinas/computadores com capacidade de imitar a inteligência humana" (GABRIEL, 2019).

> "rejeitar e viver sem ela". Na verdade, tomamos a dramática mudança tecnológica como um convite para refletirmos sobre quem somos e como vemos o mundo. Quanto mais pensamos sobre como aproveitar a revolução tecnológica, mais analisamos a nós mesmos e os modelos sociais subjacentes que são incorporados e permitidos por essas tecnologias. E mais oportunidades teremos para moldar a revolução de uma forma que melhore o estado do mundo (SCHWAB, 2016, p. 16).

Não se pode perder de vista o uso de novas tecnologias na seara pública com o objetivo de prestação do serviço público mais eficiente, menos burocrático e mais próximo ao cidadão. Á esse movimento do Poder Público face ao desenvolvimento das novas tecnologias dá-se o nome de Administração Pública 4.0 ou Administração Pública digital.

Esse movimento decorreu da criação da internet e, desde então, vem intensificando e modificando as relações socioculturais resultando na sua virtualização. Esse ambiente virtual também foi denominado, por Pierre Lévy, de ciberespaço:

> O ciberespaço (que também chamarei de "rede") é o novo meio de comunicação que surge da interconexão mundial dos computadores. O termo especifica não apenas a infra-estrutura material da comunicação digital, mas também o universo oceânico de informações que ela abriga, assim como os seres humanos que navegam e alimentam esse universo. Quanto ao neologismo "cibercultura", especifica aqui o conjunto de técnicas (materiais e intelectuais), de práticas, de atitudes, de modos de pensamento e de valores que se desenvolvem juntamente com o crescimento do ciberespaço (LÉVY, 1999, p. 17).

Para o autor, o ciberespaço nada mais é que o espaço virtual. Esse espaço encontra-se em ascensão com o intenso desenvolvimento das novas tecnologias que, por sua vez, encontram-se, cada vez mais, integradas ao cotidiano da população. Seja no ambiente familiar, seja no ambiente profissional, o ciberespaço é uma realidade na qual não se cogita – ou pouco cogita-se – sua desvinculação da realidade social.

Por conseguinte, torna-se mais imperioso a efetivação dos deveres constitucionais administrativos, destacadamente o acesso à informação, a publicidade e a transparência, bem como o dever de proteção de dados pessoais.

Na esfera pública, a Revolução Digital consagrou a Administração Pública 4.0, na qual a prestação se serviços públicos é assegurada no ciberespaço, isto é, a prestação digital de serviços públicos.

Assim, a inserção de novas tecnologias disruptivas no setor público visa assegurar a oferta de serviços públicos a população, mediante a desburocratização e o aumento da

eficiência, pugnando por uma gestão governamental que abranja as novas perspectivas decorrentes da Revolução 4.0 na Administração Pública.

Diante de tais considerações, o tópico que se segue explanará a respeito da intitulada Revolução 4.0, com vistas a demonstrar as repercussões desta nova era, ainda vivenciada, nos setores da sociedade, em especial na Administração Pública.

1.1 QUARTA REVOLUÇÃO INDUSTRIAL E A REVOLUÇÃO 4.0: A ERA *CIBER*

A sociedade passou por diversas transformações que repercutiram nas esferas social, econômica, ambiental e cultural, em escala global. Dentre essas transformações, destacam-se as Revoluções Industriais.

A primeira Revolução Industrial foi marcada pela mecanização dos processos produtivos, com a construção de ferrovias e invenção da máquina a vapor, entre os anos de 1760 e 1840. A segunda Revolução Industrial, por sua vez, teve início no final do século XIX e início do século XX e foi marcada pelo advento da eletricidade, das linhas de montagem, proporcionando a produção em larga escala. A terceira Revolução Industrial, também conhecida por Revolução Digital ou do computador, com início na década de 1960, apresentou semicondutores, computação em *mainframe*, computador pessoal e internet (SCHWAB, 2016, p. 18).

A quarta Revolução Industrial, Revolução Digital ou, até mesmo, Revolução 4.0, inaugura a era *ciber,* hodiernamente vivenciada. Com início na virada do século é caracterizada por uma internet mais ubíqua e móvel, sensores menores, mais eficientes e, cada vez mais, menos custosos (SCHWAB, 2016, p. 19). Emerge a Inteligência Artificial (IA) e com ela, o *machine learning* (método de aprendizagem da máquina).

Para além disso, emergem as novas tecnologias disruptivas, rompendo toda a estrutura social, econômica, ambiental e cultural. A Internet das Coisas (IOT em inglês), a Inteligência Artificial (IA) já citada, *smartphones, smartwatches, bitcoins, blockchains*, bancos digitais, *e-commerce*, *uber, airbnb, netflix*, *whatsapp*, são exemplos da hodierna era *ciber*.

Segundo Klaus Schwab:

> A quarta revolução industrial, no entanto, não diz respeito apenas a sistemas e máquinas inteligentes e conectadas. Seu escopo é muito mais amplo. Ondas de

> novas descobertas ocorrem simultaneamente em áreas que vão desde o sequenciamento genético até a nanotecnologia, das energias renováveis à computação quântica. O que torna a quarta revolução industrial fundamentalmente diferente das anteriores é a fusão dessas tecnologias e a interação entre os domínios físicos, digitais e biológicos (SCHWAB, 2016, p. 19).

Importa elucidar que as Revoluções de outrora não foram substituídas pelas subsequentes. Na verdade, houve uma incorporação mediante o aperfeiçoamento das descobertas de cada século, tal qual ocorre com a Revolução 4.0.

A diferença desta em relação às demais, reside no fato de que, as novas tecnologias disruptivas impactam todo o cenário, em escala global, incorporando suas características à própria condição do ser humano.

O método de aprendizagem da máquina (*machine learning*), por exemplo, permite que a inteligência artificial seja alimentada com comportamentos humanos. Ocorre uma espécie de alimentação do comportamento humano, uma transferência, de modo que, a inteligência artificial reproduza os padrões de comportamento transferidos pela pessoa.

Na visão de Martha Gabriel (2019):

> *Machine Learning* (ML), ou "aprendizagem de máquinas" em português, é um campo de IA que lida com algoritmos que permitem a um programa "aprender" – ou seja, os programadores humanos não precisam especificar um código que determina as ações ou previsões que o programa vai realizar em determinada situação. Em vez disso, o código reconhece padrões e similaridades das suas experiências anteriores e assume a ação apropriada baseado nesses dados.

Esse método de aprendizagem é bastante utilizado nos *chatbots* (robôs de conversação) que atuam como assistentes virtuais ofertando opções de atendimento ao cliente e viabilizando a celeridade e otimização do próprio atendimento.

Também é utilizado para contratação de funcionários nas empresas com a filtragem de informações necessárias e pertinentes em relação ao perfil profissional almejado para o cargo em questão.

O uso de algoritmos também possui extrema relevância enquanto tecnologia disruptiva atuando através da coleta de dados pessoais, com a consequente formação do *profiling* (perfil) comportamental do indivíduo.

A par disso, o perfil comportamental permite que as empresas realizem o *marketing* direcionado, isto é, direcionar produtos e serviços para seus clientes com base nos gostos

pessoais de cada um. A intenção é fornecer produtos e serviços selecionados ao perfil do cliente, personalizado.

De outra banda, assevera Martha Gabriel (2019):

> Além de tecnologias *wearables* e *insideables*, outras tecnologias da nossa era têm poderes de transformar radicalmente a humanidade, como, por exemplo, a manipulação genética. O avanço no mapeamento e manipulação de DNA tem o potencial de permitir que reconfiguremos o nosso programa biológico (*software* humano) de inúmeras maneiras, de forma a acelerarmos artificialmente a evolução, saltando diversas transformações biológicas que aconteceriam apenas por meio de várias etapas da evolução natural, mais lentamente. Outra possibilidade dessas tecnologias é ir além da evolução natural do ser humano e introduzir características em nossos genes que talvez nunca ocorressem por meio da evolução natural.

Resta claro que a era *ciber*, com a inserção das novas tecnologias disruptivas, tem o condão de interferir na própria condição humana, tal qual o exposto acima e como ocorre nas pesquisas para cura de doenças com auxílio da biotecnologia.

Em contrapartida, surgem problemáticas decorrentes da má utilização das tecnologias. Reportando-se aos exemplos outrora mencionados, o *machine learning* pode ser utilizado com vistas à práticas discriminatórias em razão de origem, cor, raça, gênero, entre outros, inclusive na etapa de seleção de perfil para preenchimento de vaga em cargos de determinada empresa.

O uso de algoritmos, por sua vez, além da sua má utilização para promoção de discriminação, a exemplo do racismo algorítmico, pode inviabilizar o exercício da democracia no ciberespaço, a ciberdemocracia.

Fato que se verifica através do perfil comportamental do indivíduo, o qual passa a ter acesso somente as informações que se coadunem com seu perfil, claro exemplo é o do perfil político. Desse modo, o usuário não consegue obter posicionamentos plurais, divergentes do seu, como preconiza o Estado Democrático de Direito.

O *marketing* direcionado, utilizado com fins discriminatórios, ocasiona a exclusão de grupos que não se enquadrem no perfil de clientes de determinada empresa.

Não se pode perder de vista que o *marketing* direcionado é resultado da obtenção de dados pessoais dos clientes e pretensos clientes da empresa.

Através da obtenção de tais dados e, com a posterior formação do perfil comportamental, as empresas possuem informações preciosas, como o Cadastro de Pessoas Físicas (CPF), a renda, a profissão, grau de escolaridade e limite de crédito.

Assim, as empresas “descartam” pessoas pelo simples fato de não se enquadrarem nos requisitos impostos por elas mesmas para assumir a condição de clientes.

Em tais casos, ocorre a discriminação dessas pessoas mediante a oferta de produtos e serviços com condições diferenciadas e, até mesmo, mediante a não oferta de produtos e serviços.

Denota-se que as novas tecnologias disruptivas, oriundas da quarta Revolução Industrial, da Revolução Digital ou Revolução 4.0, impactam sobremaneira a realidade social, econômica, ambiental e cultural de nações, seja de maneira positiva, seja de maneira negativa, com práticas discriminatórias.

No entanto, é preciso combater tais situações e promover a inclusão digital dos cidadãos ante a compreensão e reconhecimento de um direito fundamental à inclusão digital, em razão da inevitabilidade dos impactos da era *ciber* no cenário global, era que veio para ficar.

Ademais, passa-se ao estudo do governo digital que tem por objetivo a desburocratização e o aumento da eficiência no setor público na promoção da prestação digital de serviços públicos para a coletividade.

1.2 GOVERNO DIGITAL E NORMAS CORRELATAS PARA A PRESTAÇÃO DIGITAL DE SERVIÇOS PÚBLICOS

Não é só nas relações entre particulares que se verifica o desenvolvimento do ciberespaço. Na seara pública é perceptível o uso de novas tecnologias com vistas a prestação de serviço público mais eficiente, menos burocrático e mais próximo ao cidadão.

Esse movimento do Poder Público face ao desenvolvimento das novas tecnologias foi intitulado de Administração Pública 4.0 ou Administração Pública digital.

Antes de adentrar no tema Administração Pública 4.0 imperioso apresentar a definição de Administração Pública. Nesse viés, colaciona-se sua definição através das lições de Maria Sylvia Zanella Di Pietro (2020):

> Em seu sentido objetivo, a Administração Pública abrange as atividades exercidas pelas pessoas jurídicas, órgãos e agentes incumbidos de atender concretamente às necessidades coletivas; corresponde à função administrativa, atribuída preferencialmente aos órgãos do Poder Executivo. Nesse sentido, a Administração Pública abrange o fomento, a polícia administrativa e o serviço público.

> Assim, a Administração Pública pode ser definida como a atividade concreta e imediata que o Estado desenvolve, sob regime jurídico total ou parcialmente público, para a consecução dos interesses coletivos.

Por sua vez, Augustinho Paludo (2022, p. 76) esclarece que:

> A Administração Pública abrange a ciência, a disciplina, as normas, a estrutura e as técnicas administrativas aplicadas ao meio público. A Administração compreende todo o aparato existente (estrutura e recursos; órgãos e agentes; serviços e atividades) à disposição dos governos para a concretização dos objetivos fundamentais da República Federativa do Brasil; para a realização de seus objetivos políticos, para a prestação de serviços públicos, e para o alcance do objetivo maior e primordial do Estado: a promoção do bem comum da coletividade.
> A função administrativa é típica do Poder Executivo, mas ela também é exercida nos poderes Legislativo e Judiciário para atender as suas necessidades internas.

No que pertine a Administração Pública 4.0 esta se encontra associada ao *New Public Management*, traduzido Nova Gestão Pública ou ainda, Nova Administração Pública Gerencial, que "utiliza tecnologias e modelos de mercado para melhorar a produtividade e a qualidade dos serviços públicos e melhor atender o cidadão consumidor" (PALUDO, 2022, p. 144).

Essa nova modalidade de gestão teve como potenciais impulsionadores a democracia e o fenômeno da globalização. Assevera Augustinho Paludo (2022, p. 142) que "a democracia cobra eficiência, participação nas decisões e *accountability* governamental, e a globalização traz as tecnologias da informação e comunicação, e a competitividade".

Diante de tal cenário, criou-se um importante instrumento de efetivação dos deveres pela Administração Pública no ambiente virtual, o Portal da Transparência:

> Lançado pela Controladoria-Geral da União (CGU), em 2004, o Portal da Transparência do Governo Federal é um site de acesso livre, no qual o cidadão pode encontrar informações sobre como o dinheiro público é utilizado, além de se informar sobre assuntos relacionados à gestão pública do Brasil. Desde a criação, a ferramenta ganhou novos recursos, aumentou a oferta de dados ano após ano e consolidou-se como importante instrumento de controle social, com reconhecimento dentro e fora do país (BRASIL, 2021).

Mais tarde, o portal passou por algumas modificações buscando avançar, ainda mais, na efetivação de suas obrigações, como se denota em trecho do texto extraído do seu *site:*

> A fim de atender de forma mais eficiente a crescente demanda e as obrigações de transparência, a CGU iniciou projeto para a restruturação do Portal. Como resultado do trabalho, o Governo Federal lançou, em 2018, o novo Portal da Transparência.

> Entre as novidades, estão: formas diversas de apresentação dos dados, mecanismo de busca integrado e intuitivo, melhor usabilidade, mais recursos gráficos, integração com redes sociais, maior e melhor oferta de dados abertos, adequação a plataformas móveis, maior interatividade (BRASIL, 2021).

A criação desse modelo permite ao cidadão o acesso, em tempo real, de informações pertinentes a atuação do poder público, tais como receitas estimadas, despesas previstas, informações a respeito de licitações públicas e sanções. Ressalta-se que o modelo preza pela acessibilidade do usuário portador de necessidades especiais, apresentando, ainda, linguagem simples, clara e concisa.

O Portal da Transparência, de origem federal, passou a ser adotado não só por outros estados, mas também pelos municípios brasileiros, consagrando-se como modelo de referência na accountability, no controle social e no combate à corrupção.

Assim, o que se propõe o Portal da Transparência é potencializar o acesso à informação, promovendo a transparência e a publicidade das ações governamentais. Frisa-se que essa é apenas uma das medidas adotadas com o enfoque no ciberespaço. A partir daí, novas medidas forma apresentadas com o objetivo de regulamentar o trato com a coisa pública no ambiente virtual.

Face a nova realidade consagrada pela utilização massiva das novas tecnologias, repercute a atuação do poder público enquanto garantidor de direitos individuais e coletivos, com destaque à proteção de dados pessoais, na consecução do interesse público, posto que os dados pessoais que se encontram sob o domínio da Administração Pública devem ser resguardados a fim de evitar seu uso indevido, seja por invasão aos sistemas, seja por dolo ou culpa na atuação do agente público. Diversos são os prejuízos decorrentes da violação ao dever de proteção dos dados pessoais, culminando no vazamento destes.

Trata-se da efetivação dos princípios constitucionais de observância pelo poder público, sobretudo a publicidade, a transparência e a eficiência[2]. Desse forma, assegura-se o efetivo cumprimento dos deveres constitucionais administrativos, com destaque para o controle social e a *accountability.*

Desenvolve-se, então, um novo conceito de transparência na gestão pública, a intitulada cibertransparência. O termo foi criado por Limberger (2016, p. 45) e designa “as

2 Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte […].

novas relações que se travam na rede, denominadas *ciber*, aglutinadas à ideia de transparência. O fenômeno tecnológico pode servir para potencializar a informação pública".

É o que se propõe o Portal da Transparência, potencializar o acesso à informação, promovendo a transparência e a publicidade das ações governamentais. Ressalte-se que essa é apenas uma das medidas adotadas com o enfoque do ciberespaço. A partir daí, novas medidas forma apresentadas com o objetivo de regulamentar o trato com a coisa pública no ambiente virtual.

Para além disso, a Administração Pública promove a inclusão e a cidadania, visto que a população passa a ter acesso não só as informações públicas como orçamento, receitas e despesas, mas também, acesso as informações de cunho pessoal, exercendo, assim, seu direito fundamental de acesso à informação.

Através da disponibilização de aplicativos, de canais virtuais de atendimento e canais de denúncia em *sites* próprios, os órgãos públicos aproximam a relação entre o cidadão e o poder executivo, especialmente no que toca aos seus interesses privados, tal qual para a obtenção de um benefício governamental.

Nesse viés, foram editados Decretos, com o intuito de regulamentar a prestação de serviço público digital. Destaca-se, inicialmente, o Decreto nº 8.777, de 11 de maio de 2016, que instituiu a política de dados abertos do poder executivo Federal.

O Decreto nº 8.777, de 11 de maio de 2016, instituiu a Política de Dados Abertos, cuja definição encontra respaldo no inciso III do art. 2º. Assim, são dados abertos: "dados acessíveis ao público, representados em meio digital, estruturados em formato aberto, processáveis por máquina, referenciados na internet e disponibilizados sob licença aberta que permita sua livre utilização, consumo ou cruzamento, limitando-se a creditar a autoria ou a fonte" (BRASIL, 2016).

Mencionado Decreto prevê, entre seus objetivos constantes no art. 1º, o aprimoramento da cultura de transparência pública (II) e o fomento do controle social e do desenvolvimento de novas tecnologias destinadas à construção de ambiente de gestão pública participativa e democrática e da melhor oferta de serviços públicos para o cidadão (V).

Traz, ainda, a definição de dados abertos, conforme disposto no art. 2º, inciso III, que seriam: "dados acessíveis ao público, representados em meio digital, estruturados em formato aberto, processáveis por máquina, referenciados na internet e disponibilizados sob licença

aberta que permita sua livre utilização, consumo ou cruzamento, limitando-se a creditar a autoria ou a fonte" (BRASIL, 2016).

No que pertine a gestão da Política de Dados Abertos do poder executivo federal, atribuiu-se a Controladoria Geral da União (CGU), por meio da Infraestrutura Nacional de Dados Abertos (INDA), segundo o art. 5º do supradito Decreto.

Destaca-se ainda, o Decreto nº 8.936, de 19 de dezembro de 2016, a qual instituiu a plataforma de cidadania digital gov.br. Logo em seu art. 1º, dispõe sobre suas finalidades, exemplificam-se a possibilidade de solicitação e de acompanhamento dos serviços públicos sem a necessidade de atendimento presencial (I), bem como a implementação e difusão do uso dos serviços públicos digitais, inclusive por meio de dispositivos móveis (II).

A definição de serviço público digital encontra amparo em seu art. 2º, inciso II, *in verbis*: "serviço público cuja prestação ocorra por meio eletrônico, sem a necessidade de atendimento presencial" (BRASIL, 2016).

Já o Plano de Dados Abertos consiste no: "documento orientador para as ações de implementação e promoção de abertura de dados de cada órgão ou entidade da administração pública federal, obedecidos os padrões mínimos de qualidade, de forma a facilitar o entendimento e a reutilização das informações" (BRASIL, 2016).

Assim, os dados abertos são dados facilmente obtidos e passíveis de utilização na rede, na consecução de execução das políticas públicas cuja importância se reverte na promoção do direito de acesso à informação, publicidade, transparência, *accountability*, controle social e combate à corrupção.

Eventos mais recentes seguiram o caminho na busca da prestação de um serviço público mais eficiente no ciberespaço. Exemplo disso é o Decreto nº 9. 319 de 2018, que instituiu o Sistema Nacional para a Transformação Digital – SinDigital e estabeleceu uma estrutura de governança para a implantação da Estratégia Brasileira para a Transformação Digital – E-Digital.

Sua importância reside no fato ser um dispositivo normativo que elenca objetivos agrupados em eixos temáticos para o desenvolvimento da prestação do serviço público no ambiente digital, como o eixo da cidadania e transformação digital do governo, assim definido: "o propósito da transformação digital no governo é torná-lo mais dinâmico e próximo da população, de forma a utilizar as tecnologias digitais para catalisar forças sociais e dinâmicas produtivas, para benefício da sociedade. O Estado deve se inserir de maneira eficaz

no ambiente digital, com atendimento eficiente ao cidadão, integração de serviços e políticas públicas e transparência" (BRASIL, 2018).

Dentre os objetivos da E-Digital, constantes no anexo I, verifica-se a:

> Cidadania e Transformação Digital do Governo
>
> O propósito da transformação digital no governo é torná-lo mais dinâmico e próximo da população, de forma a utilizar as tecnologias digitais para catalisar forças sociais e dinâmicas produtivas, para benefício da sociedade. O Estado deve se inserir de maneira eficaz no ambiente digital, com atendimento eficiente ao cidadão, integração de serviços e políticas públicas e transparência (BRASIL, 2018).

Instituindo a Política Nacional de Segurança da Informação (PNSI), o Decreto nº 9.637, de 26 de dezembro de 2018, alude ao respeito e promoção dos direitos humanos e das garantias fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a proteção da privacidade e o acesso à informação; ao *need to know* para o acesso à informação sigilosa, nos termos da legislação; e a integração e cooperação entre o Poder Público, o setor empresarial, a sociedade e as instituições acadêmicas, previstas, respectivamente, nos incisos II, XII, XV do art. 3º.

Em seu art. 6º, traz a adoção de uma Estratégia Nacional de Segurança da Informação, dividida nos seguintes módulos: (i) segurança cibernética; (ii) defesa cibernética; (iii) segurança das infraestruturas críticas; (iv) segurança da informação sigilosa; e (v) proteção contra vazamento de dados (BRASIL, 2018).

Insere ainda, no referido contexto, o Decreto nº 9.756, de 11 de abril de 2019, que instituiu o portal gov.br., com vistas à centralização na disponibilização de informações institucionais, notícias e serviços públicos prestados pelo governo federal.

Referido Decreto faz menção aos prazos para integração dos serviços públicos digitais em toda a rede federal, passo importante para a oferta simplificada e desburocratizada de tais serviços para a sociedade. Percebe-se que a data final para unificação foi 31 de dezembro de 2020, segundo o § 2º do art. 4º, *in verbis*: "até 31 de dezembro de 2020, os órgãos e as entidades da administração pública federal a que se refere o art. 1º deverão: (i) migrar os conteúdos de seus portais na internet para o portal único, registrado sob o domínio 'gov.br'; e (ii) desativar os endereços de sítios eletrônicos existentes do Governo federal ou

redirecionar o acesso para o portal único, registrado sob o domínio 'gov.br'" (BRASIL, 2019).

Outro importante passo para a regulamentação do Governo Digital foi a edição do Decreto de nº 9.854, de 25 de junho de 2019, sobre Internet das Coisas (IoT). De acordo com o Decreto, conceitua-se internet das coisas como a "infraestrutura que integra a prestação de serviços de valor adicionado com capacidades de conexão física ou virtual de coisas com dispositivos baseados em tecnologias da informação e comunicação existentes e nas suas evoluções, com interoperabilidade" (BRASIL, 2019). Leitura extraída no inciso I do seu art. 2º.

O Decreto estabelece também, no art. 5º, temas que integram o plano de ação para viabilizar o Plano Nacional de Internet das Coisas, a saber: "(i) ciência, tecnologia e inovação; (ii) inserção internacional; (iii) educação e capacitação profissional; (iv) infraestrutura de conectividade e interoperabilidade; (v) regulação, segurança e privacidade; e (vi) viabilidade econômica" (BRASIL, 2019).

Para tanto, o parágrafo único do supradito artigo aduz pela necessidade do alinhamento do plano de ação sobre Internet das Coisas com as ações estratégicas definidas na Estratégia Brasileira para a Transformação Digital (E-Digital).

De outra banda, o Decreto nº 10.046, de 09 de outubro de 2019, "estabelece as normas e as diretrizes para o compartilhamento de dados entre os órgãos e as entidades da administração pública federal direta, autárquica e fundacional e os demais Poderes da União[3]" (BRASIL, 2019).

Esse dispositivo normativo diferencia atributos biográficos dos atributos biométricos, conceitua e exemplifica dados cadastrais, traz o conceito de governança de dados, previsto no inciso XV do art. 2º, que corresponde ao "exercício de autoridade e controle que permite o gerenciamento de dados sob as perspectivas do compartilhamento, da arquitetura, da segurança, da qualidade, da operação e de outros aspectos tecnológicos" (BRASIL, 2019).

Salienta-se a estruturação de compartilhamento de dados nos níveis amplo, restrito e específico. Compartilhamento amplo refere-se aos dados públicos que não estão sujeitos a nenhuma restrição de acesso, cuja divulgação deve ser pública e garantida a qualquer interessado; compartilhamento restrito refere-se aos dados protegidos por sigilo, com concessão de acesso a todos os órgãos e as entidades da administração pública federal direta,

3 É o que consta no art. 1º.

autárquica e fundacional e os demais Poderes da União para a execução de políticas públicas, cujo mecanismo de compartilhamento e regras sejam simplificados e estabelecidos pelo Comitê de Governança de Dados; por sua vez, o compartilhamento específico refere-se aos dados protegidos por sigilo, 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, conforme previsto no art. 4º, incisos I, II e III, respectivamente.

Destarte, o Decreto nº 10.160, de 9 de dezembro de 2019, proclamou o Governo Aberto. Essa norma visa ampliar o acesso à informações de caráter público para a sociedade, fortalecendo a transparência e a *accountability*. Seus arts. 2º e 3º dispõem o seguinte:

> Art. 2º São diretrizes da Política Nacional de Governo Aberto:
> I - aumento da disponibilidade de informações sobre as atividades governamentais, incluídos os dados sobre os gastos e o desempenho das ações e dos programas do Governo federal;
> II - fomento à participação social nos processos decisórios;
> III - estímulo ao uso de novas tecnologias que fomentem a inovação, o fortalecimento da governança pública e o aumento da transparência e da participação social na gestão e na prestação de serviços públicos; e
> IV - aumento dos processos de transparência, de acesso a informação e da utilização de tecnologias que subsidiem esses processos.
>
> Art. 3º Os planos de ação nacionais sobre governo aberto contemplarão iniciativas, ações, projetos, programas e políticas públicas destinadas:
> I - ao aumento da transparência;
> II - ao aprimoramento da governança pública;
> III - ao acesso às informações públicas;
> IV - à prevenção e ao combate à corrupção;
> V - à melhoria da prestação de serviços públicos;
> VI - à eficiência administrativa; e
> VII - ao fortalecimento da integridade pública (BRASIL, 2019).

De modo mais específico, o Decreto nº 10.332, de 28 de abril de 2020, instituiu a Estratégia de Governo Digital para o período de 2020 a 2022 na Administração Pública Federal. Aduz que "a Estratégia de Governo Digital para o período de 2020 a 2022 está organizada em princípios, objetivos e iniciativas que nortearão a transformação do governo por meio do uso de tecnologias digitais, com a promoção da efetividade das políticas e da qualidade dos serviços públicos e com o objetivo final de reconquistar a confiança dos brasileiros" (BRASIL, 2020).

Por meio de tal Decreto, os objetivos da E-Digital foram reformulados tendo em vista o período considerado de 2020 a 2022. Passou a vigorar com a seguinte redação:

> - oferecer serviços públicos digitais simples e intuitivos, consolidados em plataforma única e com avaliação de satisfação disponível; - conceder acesso amplo à informação e aos dados abertos governamentais, para possibilitar o exercício da cidadania e a inovação em tecnologias digitais; - promover a integração e a interoperabilidade das bases de dados governamentais; - promover políticas públicas baseadas em dados e evidências e em serviços preditivos e personalizados, com utilização de tecnologias emergentes; - implementar a Lei Geral de Proteção de Dados, no âmbito do Governo federal, e garantir a segurança das plataformas de governo digital; - disponibilizar a identificação digital ao cidadão; - adotar tecnologia de processos e serviços governamentais em nuvem como parte da estrutura tecnológica dos serviços e setores da administração pública federal; - otimizar as infraestruturas de tecnologia da informação e comunicação; e - formar equipes de governo com competências digitais (BRASIL, 2020).

Apresenta como objetivos, a oferta de serviços públicos digitais; a avaliação de satisfação nos serviços digitais; canais e serviços digitais simples e intuitivos; acesso digital único aos serviços públicos; plataformas e ferramentas compartilhadas; serviços públicos integrados; políticas públicas baseadas em dados e evidências; serviços públicos do futuro e tecnologias emergentes; serviços preditivos e personalizados ao cidadão; implementação da LGPD no âmbito do Governo federal; garantia da segurança das plataformas de governo digital e de missão crítica; identidade digital ao cidadão; reformulação dos canais de transparência e dados abertos; participação do cidadão na elaboração de políticas públicas; governo como plataforma para novos negócios; otimização das infraestruturas de tecnologia da informação; o digital como fonte de recursos para políticas públicas essenciais e equipes de governo com competências digitais (BRASIL, 2020).

Inobstante a edição dos supracitados Decretos, em 29 de março de 2021, foi sancionada a lei nº 14.129, conhecida por dispor a respeito do Governo digital. No art. 14 assevera que “a prestação digital dos serviços públicos deverá ocorrer por meio de tecnologias de amplo acesso pela população, inclusive pela de baixa renda ou residente em áreas rurais e isoladas, sem prejuízo do direito do cidadão a atendimento presencial” (BRASIL, 2021).

O parágrafo único assevera, ainda, que o acesso a tais serviços será realizado, preferencialmente, mediante o autosserviço (BRASIL, 2021). O autosserviço é conceituado no inciso II do art. 4º, e consiste no “acesso pelo cidadão a serviço público prestado por meio digital, sem necessidade de mediação humana” (BRASIL, 2021).

A lei assegura direitos aos usuários da prestação digital de serviços públicos, tais como gratuidade no acesso às plataformas digitais; atendimento; padronização de

procedimentos; recebimento de protocolo; indicação de canal preferencial de comunicação, nos termos do art. 27. (BRASIL, 2021).

Em relação aos seus princípios e diretrizes constantes no art. 3º, citam-se:

> I – a desburocratização, a modernização, o fortalecimento e a simplificação da relação do poder público com a sociedade, mediante serviços digitais, acessíveis inclusive por dispositivos móveis;
> II – a disponibilização em plataforma única do acesso às informações e aos serviços públicos, observadas as restrições legalmente previstas e sem prejuízo, quando indispensável, da prestação de caráter presencial;
> III – a possibilidade aos cidadãos, às pessoas jurídicas e aos outros entes públicos de demandar e de acessar serviços públicos por meio digital, sem necessidade de solicitação presencial;
> IV – a transparência na execução dos serviços públicos e o monitoramento da qualidade desses serviços;
> V – o incentivo à participação social no controle e na fiscalização da administração pública […] (BRASIL, 2021).

Não se pode perder de vista que todas essas estratégias para a transformação digital, inclusive na Administração Pública, derivam do que hodiernamente se trata por Sociedade da Informação. Sobre o tema preleciona BIONI (2019):

> Em cada época, existiu um elemento central para o seu desenvolvimento, sendo o modo pelo qual ele se estruturou o fator determinante para se estabelecer os seus respectivos marcos históricos.
> (...)
> Por isso, a informação avoca um papel central e adjetivante da sociedade: *sociedade da informação*. A informação é o (novo) elemento estruturante que (re)organiza a sociedade, tal como o fizeram a terra, as máquinas a vapor e a eletricidade, bem como os serviços, respectivamente, nas sociedades agrícola, industrial e pós-industrial. (grifo original).

A promoção e difusão de um espaço público virtual ou Governo Digital implica, se bem aproveitado, na prestação de um serviço público mais eficiente. Em decorrência, visualiza-se a efetivação dos deveres administrativos e o exercício dos direitos do cidadão no ciberespaço.

Em 2020, pesquisa realizada sobre Governo Eletrônico pela Organização das Nações Unidas (ONU), “classificou o Brasil como 20º (vigésimo), entre 193 países, com melhor oferta de serviços públicos digitais” (BRASIL, 2020).

Por conseguinte:

> O Índice de Serviços Online mede o uso de tecnologia da informação e comunicações (TIC) pelos governos para a prestação de serviços públicos em nível nacional, incluindo dados abertos, participação eletrônica, prestação de serviços multicanais, serviços móveis, nível de utilização pelo cidadão, bem como parcerias inovadoras por meio do uso de TICs […]
> Desde janeiro de 2019, mais de 800 serviços públicos de interesse da sociedade, antes acessados somente presencialmente, já foram transformados em digitais, permitindo que o cidadão os acesse de casa, pelo computador ou celular, evitando deslocamentos agora desnecessários (BRASIL, 2020).

À vista disso, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), no mesmo ano, classificou o Brasil na 16ª posição, de 33 países, no que pertine a transformação digital dos serviços públicos. Essa pesquisa leva em consideração o desempenho dos países "em seis dimensões: orientado pelo usuário, orientado por dados, aberto por padrão, digital por design, proatividade, e governo como plataforma" (BRASIL, 2020).

A regulamentação no uso das tecnologias acarreta segurança jurídica nas relações entre o poder público e o cidadão, além de propiciar a otimização na prestação dos serviços públicos, impulsionando sua eficiência. Nota-se que, por meio dos instrumentos normativos ora citados, exige-se que a difusão do acesso à informação no ambiente virtual ocorra, primordialmente, para aqueles considerados hipossuficientes[4].

Nessa toada, informa LIMBERGER (2016, p. 91):

> A informação pública disponibilizada pelos sítios estatais é uma das manifestações da Administração eletrônica. Existe, porém, uma conexão entre a administração eletrônica e a democracia eletrônica, uma vez que, estando as informações em rede e efetuando o cidadão este acesso, há um fortalecimento desta, pois permite uma apropriação de informação, que servirá para melhor deliberação democrática. Outra consequência, que daí pode advir, é, a partir da informação pública, disponibilizada em rede, a organização cidadã para criação de fóruns de discussão virtual, a respeito dos assuntos públicos.

A prestação do serviço público digital promove a democracia no sentido de que, as informações ali prestadas fomentam a transparência e a publicidade, fornecendo mecanismos para o controle social e a *accountability*.

Insere-se aqui, a cidadania eletrônica ou cibercidadania, pois o exercício da cidadania no ambiente digital dever ser resguardado e até mesmo incentivado pelo poder público.

4 O termo hipossuficiente remete ao sentido de acesso às novas tecnologias, bem como às dificuldades apresentadas em seu manuseio.

Relevante inovação trazida pela Lei do Governo Digital, é a possibilidade de criação de laboratórios de inovação, com respaldo no art. 44, cuja redação traz a abertura para a sociedade na participação e colaboração com métodos, conceitos e ferramentas inovadoras para a gestão pública, para a prestação de serviços públicos, tratamento de dados, bem como para a participação do cidadão no controle da Administração Pública (BRASIL, 2021).

Assim, é perceptível o uso da tecnologia enquanto aliada na prestação do serviço público, contribuindo significativamente na efetividade dos princípios constitucionais do acesso à informação, da publicidade e da transparência, assim como na prestação de um serviço público cada vez mais eficiente. No entanto, a adesão as novas tecnologias devem estar acompanhadas de medidas que incluam a população mais vulnerável.

Para além disso, a prestação digital de serviços públicos tem o condão de promover o controle social e a *accountability* de forma mais transparente e democrática, haja vista a facilidade na obtenção das informações postas a disposição em rede.

1.3 INCLUSÃO DIGITAL COMO PRESSUPOSTO DO AUMENTO DA EFICIÊNCIA PÚBLICA, DO CONTROLE SOCIAL E DA *ACCOUNTABILITY*

A Lei nº 14.129, de 29 de março de 2021, conhecida como Lei do Governo Digital, estatui condições para a implementação de um Governo atento as mudanças ocasionadas pela Revolução Digital prezando também pelo aumento da eficiência pública.

Nessa perspectiva, constituem pilares para sua implementação a desburocratização, a inovação, a transformação digital e a participação do cidadão.

A desburocratização visa a ruptura de barreiras burocráticas levando-se em consideração que esses aspectos inviabilizam o acesso à informação e a tutela de direitos dos cidadãos. Deste modo, o acesso simplificado, mediante linguagem clara, simples e de fácil compreensão, bem como a presença de instruções de acesso aos *sites* e aplicativos do Governo, privilegiam a inclusão digital.

A inovação, por sua vez, pode ser associada as novas tecnologias disruptivas, vez que o caráter disruptivo se apresenta como uma inovação, uma quebra de paradigmas capaz de repercutir em toda a sociedade, a exemplo do uso da Inteligência Artificial (IA) nos mais diversos setores, inclusive no Poder Judiciário.

A transformação digital, conforme analisado no tópico anterior, possui amparo no Decreto nº 9.319, de 21 de março de 2018 e tem por objetivo "aproveitar o potencial das tecnologias digitais para promover o desenvolvimento econômico e social sustentável e inclusivo, com inovação, aumento de competitividade, de produtividade e dos níveis de emprego e renda no País" (BRASIL, 2018). Trata-se da aderência da Administração Pública às novas tecnologias na consecução de suas finalidades precípuas, apresentando como resultado a Administração Pública Digital ou 4.0.

A participação do cidadão é medida que se impõe na promoção dos objetivos do Estado democrático de Direito. A participação popular viabiliza o controle social dos cidadãos nos atos de gestão, sobretudo por meio da instituição de ouvidorias com canais de denúncias, inclusive anônimas e sugestões, seja referente a críticas ou elogios.

Para além disso, a participação popular deve ser assegurada e incentivada pelo Poder Público, não sendo suficiente a criação de canal de denúncias, por exemplo. Assim, é necessário a adoção de mecanismos de respostas efetivas aos cidadãos, isto é, prestação de contas do Estado aos cidadãos.

A prestação de contas relaciona-se com o princípio da *accountability*. Alguns autores defendem que ambas as expressões não são sinônimas, a exemplo de José Matias Pereira, ao compreender que

> O termo *accountability* pode ser considerado o conjunto de mecanismos e procedimentos que levam os decisores governamentais a prestarem contas dos resultados de suas ações, garantindo-se maior transparência e a exposição das políticas públicas. Quanto maior a possibilidade de os cidadãos poderem discernir se os governantes estão agindo em função do interesse da coletividade e sancioná-los apropriadamente, mais *accountable* é um governo. O conceito de *accountable* está relacionado estreitamente ao universo político-administrativo anglo-saxão.
> (…)
> O exercício da *accountability* é determinado pela qualidade das relações entre governo e cidadãos, entre burocracia e clientelas (PEREIRA, 2014, p. 85).

De acordo com referido autor a *accountability* vai além da prestação de contas, engloba os mecanismos estatais assegurados na prestação do serviço público eficaz, primando pelo constante diálogo entre Estado e cidadãos ante a convergência de seus interesses, isto é, o interesse público.

O próprio conceito de prestação de contas abrange uma série de condutas por parte do Administrador. É o que preleciona Hely Lopes Meirelles (2016, p.119):

> O dever de prestar contas é decorrência natural da administração como encargo de gestão de bens e interesses alheios. (…) No caso do administrador público, esse dever ainda mais se alteia, porque a gestão se refere aos bens e interesses da coletividade e assume o caráter de um *múnus público*, isto é, de um encargo para com a comunidade.
> A prestação de contas não se refere apenas aos dinheiros públicos, à gestão financeira, mas a todos os atos de governo e de administração (Grifo original).

No que toca ao termo *accountability*, Augustinho Paludo (2022, p. 245) informa que este se desenvolveu a partir da terceira onda de democratização dos anos 1980-1990 e que um de seus objetivos consiste em aumentar a responsabilização dos governantes. Trata-se, então, de uma conquista da democracia.

Importa esclarecer que "*accountability* inclui a obrigação de prestar contas, a utilização de boas práticas de gestão e a responsabilização pelos atos e resultados decorrentes da utilização de recursos públicos" (PALUDO, 2022, p. 246).

No ciberespaço a participação popular também deve ser resguardada. De nada adianta o investimento em transformação digital na Administração Pública, se este não prever mecanismos que garantam a tutela dos direitos e liberdades fundamentais dos cidadãos.

Conforme outrora explicitado, denotam-se diversas normas regulamentando a atuação estatal no ciberespaço, com destaque para a prestação digital dos serviços públicos, assegurada pela Lei do Governo Digital.

A par disso, surgem deveres correlatos da Administração Pública, sejam novos deveres, decorrentes da própria necessidade do universo digital, como o dever fundamental de inclusão digital e o direito de acesso à internet, cujos debates se intensificaram em decorrência da pandemia da COVID-19, seja a partir de uma releitura dos direitos já assegurados, a exemplo do direito à privacidade e à liberdade de expressão.

Nessa seara, surgem nomenclaturas que associam direitos e deveres ao universo *ciber*. A cibertransparência, a ciberdemocracia e a cibercidadania.

No que pertine ao termo cibercidadania, Pérez Luño (2004, apud Limberger, 2016) esclarece que esta é "expressão que traduz uma nova forma de a Administração Pública disponibilizar a informação em rede aos cidadãos, que pode não ser somente a utilização da ferramenta tecnológica, mas uma nova forma de gerenciamento público e das relações democráticas com a sociedade que daí advenham".

Portanto, a inclusão digital dos cidadãos, sobretudo dos que se encontram em situação de maior vulnerabilidade, é imprescindível para que se efetive o Estado democrático

de Direito, o que pode ser realizado mediante ações educativas para a população com a explicação sobre como baixar aplicativos, acessar sites, incluir dados pessoais, como solicitar informações dos órgãos, sem prejuízo da possibilidade de acesso presencial ao órgão para eventuais esclarecimentos e demandas.

A inclusão digital encontra amparo no princípio da dignidade da pessoa humana. Até porque:

> O princípio da dignidade da pessoa humana se presta também ao papel de parâmetro para controle de atos estatais – normativos, administrativos e jurisdicionais – e mesmo de atos particulares, como os contratos e negócios jurídicos em geral.
> (…)
> Outro papel relevante do princípio da dignidade da pessoa humana se relaciona à identificação de direitos fundamentais. A dignidade é essencial, em primeiro lugar, para o reconhecimento da fundamentalidade de direitos que não estejam inseridos no catálogo constitucional de direitos e garantias fundamentais (SARMENTO, 2016, p. 84).

Em sua obra *A Galáxia da Internet: Reflexões sobre a internet, os negócios e a sociedade*, adverte Manuel Castells (2003):

> A centralidade da Internet em muitas áreas da atividade social, econômica e política equivale a marginalidade para aqueles que não têm acesso a ela, ou têm apenas um acesso limitado, bem como para os que são incapazes de usá-la eficazmente. Assim, não surpreende que a proclamação do potencial da Internet como um meio de liberdade, produtividade e comunicação venha de par com a denúncia da "divisão digital" gerada pela desigualdade a ela associada. A diferenciação entre os que têm e os que não têm Internet acrescenta uma divisão essencial às fontes já existentes de desigualdade e exclusão social, numa interação complexa que parece aumentar a disparidade entre a promessa da Era da Informação e sua sombria realidade para muitos em todo o mundo.
> (…)
> Em seu significado usual, "a divisão digital" diz respeito à desigualdade de acesso à Internet. (…) o acesso por si só não resolve o problema, mas é um pré-requisito para a superação da desigualdade numa sociedade cujas funções e grupos sociais dominantes organizam-se cada vez mais em torno da Internet.

Não se pode perder de vista que a criação da internet propiciou o desenvolvimento do ambiente virtual. A prestação digital de serviços públicos é possível, tão somente em razão do acesso à internet, situação que se aplica aos demais setores insertos no ciberespaço, desde compra e vendas *online* até o acesso à educação.

Ademais, a inclusão digital está intrinsecamente associada ao exercício da cibercidadania, da ciberdemocracia, do controle social e da *accountability*, todos eles são pilares do Estado democrático de Direito na Administração Pública 4.0.

Vislumbram-se, dessa forma, inúmeras vantagens proporcionadas pelo ciberespaço na prestação dos serviços públicos, haja vista o alcance em massa, a praticidade e a disponibilização da informação em tempo real. No entanto, necessária a conjugação da prestação de serviço público em rede com a elaboração de políticas públicas que alcancem a população mais vulnerável.

Ante o que foi exposto, o tópico seguinte abordará o tema da proteção de dados pessoais enquanto um direito fundamental interligado aos deveres de acesso à informação, publicidade e cibertransparência, trazendo decisões jurisprudenciais que sopesaram tais deveres, ocasião na qual ainda não havia sido promulgada a LGPD e os debates sobre o tema eram incipientes.

1.4 O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS E OS DEVERES DE ACESSO À INFORMAÇÃO, PUBLICIDADE E CIBERTRANSPARÊNCIA

Diante de um cenário no qual o acesso à informação deve ser assegurado em sua acepção mais ampla, junto aos princípios da publicidade e da transparência, com a exigência de certos requisitos para efetivação de tais deveres, surge também o dever de zelo com os dados extraídos das informações disponíveis e disponibilizadas pelo Poder Público, o dever de proteção de dados pessoais.

Nesse diapasão esclarecem (FLÔRES; SILVA, 2020, p. 13-14):

> O acesso à informação se tornou indispensável, tanto para cumprir as exigências sociais de uma sociedade que quer ser informada sobre os atos que envolvem direitos e manutenção de deveres relativos à Administração Pública, quanto para a próprio Poder Público, que realiza a coleta dos mais diversos dados sobre os quais tem interesse para a gestão pública. A informação está presente na relação democrática entre os indivíduos e entre estes e o Estado, o que é incrementado pelo uso crescente de tecnologias, que permitem a produção, distribuição e acesso a essas informações de forma cada vez mais célere. Resta saber se todo esse aparato tecnológico, bem como o recolhimento e o controle dos dados pessoais contribuem para fortalecer a democracia ou, ao revés, fragilizam os direitos fundamentais e a dignidade humana dos titulares, supedâneos dessa mesma democracia.

No mesmo sentido, (CARVALHO; PEIXOTO; CARVALHO, 2020, p. 61-62) informam que “até mesmo as informações públicas, que isoladamente não teriam potencialidade lesiva, quando combinadas entre si ou com dados privados, podem dar ensejo a formas de violações que atingem valores democráticos elementares”.

A Lei de Acesso à Informação destaca, em seu inciso I do art. 6º, dentre suas finalidades, a gestão transparente da informação, com amplo acesso e divulgação (BRASIL, 2011). Assim, para que o dever de acesso à informação seja assegurado de forma efetiva, necessário que esta seja repassada do modo mais transparente quanto possível, envolvendo os atributos da clareza, da precisão e da compreensibilidade.

Até porque "numa democracia, a transparência e o livre fluxo da informação é a regra, ao passo que o sigilo é medida excepcional, somente justificável em circunstâncias taxativas e detalhadamente explicitadas na lei, relacionadas com um interesse público devidamente caracterizado e proporcional a defesa dos direitos fundamentais. Contudo, a grande questão está em, ter assegurados esses direitos, sem que sejam também suprimidos os direitos de outros (…)" (CUNHA, 2016, p. 92-93).

A Lei de Acesso à Informação destaca, em seu inciso I do art. 6º, dentre suas finalidades, a gestão transparente da informação, com amplo acesso e divulgação (BRASIL, 2011). Assim, para que o dever de acesso à informação seja assegurado de forma efetiva, necessário que esta seja repassada do modo mais transparente quanto possível, envolvendo os atributos da clareza, da precisão e da compreensibilidade.

Até porque "numa democracia, a transparência e o livre fluxo da informação é a regra, ao passo que o sigilo é medida excepcional, somente justificável em circunstâncias taxativas e detalhadamente explicitadas na lei, relacionadas com um interesse público devidamente caracterizado e proporcional a defesa dos direitos fundamentais. Contudo, a grande questão está em, ter assegurados esses direitos, sem que sejam também suprimidos os direitos de outros (…)" (CUNHA, 2016, p. 92-93).

Em diversas ocasiões o Supremo Tribunal Federal adotou o posicionamento de prevalência do interesse público nas demandas nas quais se discutiam a possibilidade de divulgação de dados dos servidores pela Administração Pública.

Destaca-se a Ação Originária nº 2.367 proposta pela Associação dos Juízes Federais do Rio de Janeiro e Espírito Santo (AJUFERJES) com o objetivo de afastar a aplicabilidade da Resolução n° 151/2012 e da Resolução n° 215/2015, ambas do Conselho Nacional de Justiça (CNJ) no tocante a divulgação dos vencimentos dos magistrados. Ocasião na qual se entendeu que:

> 1. Não há violação à intimidade ou à vida privada na divulgação nominal e pormenorizada da remuneração de magistrados, pois os dados são de interesse público e a transparência se impõe. Precedentes.

> 2. A jurisprudência do STF entende prevalecer, no caso, o princípio da publicidade administrativa, que concretiza a República como forma de governo.
> (…)
> (BRASIL, 2018).

Destaca-se, ainda, o entendimento do Relator, nos seguintes termos:

> Os atos do Conselho Nacional de Justiça não apenas densificam a interpretação constitucional conferida pelo Supremo Tribunal Federal, como promovem a transparência. Como venho afirmando nesta Corte, a transparência se impõe porque decorre (i) do princípio democrático (CF/1988, art. 1º, caput), (ii) do sistema representativo (CF/1988, art. 1º, parágrafo único), (iii) do regime republicano (CF/1988, art. 1º,caput), e (iv) do princípio da publicidade (CF/1988, art 37, caput). Ao especificar o conteúdo desses princípios no exercício de suas competências constitucionais, o ato do CNJ não exorbita do poder regulamentar, mas antes confere efetividade ao disposto na Constituição Federal (BRASIL, 2018).

Destarte no caso em apreço, o que se verifica é o embate entre o interesse público (prevalente) e o interesse privado, no qual se entende que o servidor, ao exercer uma função pública, assume o ônus de ter suas informações pessoais publicizadas com o fito de concretizar os deveres de acesso à informação, publicidade e transparência nos atos da gestão pública.

A respeito da supremacia do interesse público, princípio implícito à atuação estatal, aduz Irene Patrícia Nohara (2019):

> Supremacia do interesse público é postulado que alicerça todas as disciplinas do direito público, que partem de uma relação vertical do Estado em relação aos cidadãos. Já no direito privado, as relações jurídicas são analisadas na perspectiva da horizontalidade, isto é, da igualdade entre sujeitos e interesses particulares.
> As relações do Estado são exorbitantes do direito comum, pois visam ao interesse geral.
> A supremacia do interesse público deve orientar o legislador e o aplicador da lei. O legislador, quando da discussão de projetos de lei ao medir as restrições que os interesses sofrerão em nome de benefícios coletivos; e o aplicador da lei – juiz ou administrador –, na aplicação do direito público.

Em que pese o embate entre o direito fundamental à proteção de dados pessoais e a atuação estatal com vistas a divulgação das informações pessoais para a promoção da publicidade e da transparência, destaca-se que o entendimento jurisprudencial hodierno pugna pela divulgação das informações estritamente necessárias ao exercício dos direitos tutelados, a exemplo da possibilidade de divulgação de nomes, setores e remuneração, vedando-se a divulgação de Cadastro de Pessoas Físicas (CPF) e endereço do servidor.

Conclui Celso Antônio Bandeira de Melo (2015, p. 73):

> Fácil é ver-se que as prerrogativas inerentes à supremacia do interesse público sobre o interesse privado só podem ser manejadas legitimamente para o alcance de interesses públicos; não para satisfazer apenas interesses ou conveniências tão só do aparelho estatal, e muito menos dos agentes governamentais.

Sob outra perspectiva, não se pode perder de vista que a proteção ao sigilo dos dados pessoais consiste em um direito fundamental subjetivo, pois, a partir deles é possível obter uma representação do indivíduo, refletindo em uma parcela relevante de sua personalidade (ASSAD; LEITE, 2018, p. 196).

Através dos dados pessoais e com a consequente representação de sua personalidade, as pessoas são conhecidas nos relacionamentos, de uma forma indireta, resultando, assim, em uma relação cada mais íntima entre os dados pessoais, a própria identidade do indivíduo e sua personalidade (DONEDA, 2011, p. 106).

O princípio da publicidade, por seu turno, está previsto no art. 5º, incisos XIV, XXXIII e LX da Constituição Federal de 1988, este último dispondo que "a lei só poderá restringir a publicidade dos atos processuais quando a defesa da intimidade ou o interesse social o exigirem" (BRASIL, 1988), consagrando o princípio da publicidade como regra, no ordenamento jurídico pátrio.

Também encontra previsão em seu art. 37, no capítulo referente a Administração Pública, consoante informado anteriormente. Demonstrando, assim, a importância da publicidade na gestão da informação como condição, inclusive, de eficácia dos atos.

Não obstante o amparo constitucional, o princípio da publicidade também encontra previsão em outros dispositivos normativos, os quais serão explicitados a seguir.

O Decreto-Lei nº 4.657, de 04 de setembro de 1942, conhecida como Lei de Introdução às Normas do Direito Brasileiro (LINDB) traz, em seu bojo, a publicidade como condição de vigência das leis, é o que se extrai do art. 1º, *in verbis*: "Salvo disposição contrária, a lei começa a vigorar em todo o país quarenta e cinco dias depois de oficialmente publicada" (BRASIL, 1942).

O normativo ainda prevê tal condição aplicada no ordenamento estrangeiro, em seu § 1º, assim dispondo: "nos Estados, estrangeiros, a obrigatoriedade da lei brasileira, quando admitida, se inicia três meses depois de oficialmente publicada" (BRASIL, 1942).

Já em seu § 3º aduz que, "se, antes de entrar a lei em vigor, ocorrer nova publicação de seu texto, destinada a correção, o prazo deste artigo e dos parágrafos anteriores começará a correr da nova publicação" (BRASIL, 1942).

Depreende-se, a partir da leitura da lei, que a publicidade atua como marco temporal na contagem dos prazos para início da vigência da lei.

No âmbito da atuação da Administração Pública destacam-se algumas leis, dentre elas, a Lei nº 8.666, de 21 de junho de 1993, Lei de Licitações que "estabelece normas gerais sobre licitações e contratos administrativos pertinentes a obras, serviços, inclusive de publicidade, compras, alienações e locações no âmbito dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios" (BRASIL, 1993), conforme aduz seu art. 1º.

Precisamente, no § 1º do art. 61, informa que:

> A publicação resumida do instrumento de contrato ou de seus aditamentos na imprensa oficial, que é condição indispensável para sua eficácia, será providenciada pela Administração até o quinto dia útil do mês seguinte ao de sua assinatura, para ocorrer no prazo de vinte dias daquela data, qualquer que seja o seu valor, ainda que sem ônus, ressalvado o disposto no art. 26 desta Lei (BRASIL, 1993).

Dessa forma, a publicidade dos atos serve como instrumento para garantir sua eficácia.

Outro importante normativo é a Lei nº 9.784, de 29 de janeiro de 1999, que tem por finalidade regular o processo administrativo no âmbito da Administração Pública Federal, o qual previu, em seu parágrafo único, inciso V, do art. 2º, dentre os critérios a serem observados, a "divulgação oficial dos atos administrativos, ressalvadas as hipóteses de sigilo previstas na Constituição" (BRASIL, 1999).

De outra banda, a Lei Complementar nº 101, de 04 de maio de 2000, conhecida como Lei de Responsabilidade Fiscal (LRF) traz, dentre suas hipóteses para efetivação da transparência, especificamente no art. 48, § 1º, II, a "liberação ao pleno conhecimento e acompanhamento da sociedade, em tempo real, de informações pormenorizadas sobre a execução orçamentária e financeira, em meios eletrônicos de acesso público" (BRASIL, 2000).

Traz, ainda, no seu § 2º que "a União, os Estados, o Distrito Federal e os Municípios disponibilizarão suas informações e dados contábeis, orçamentários e fiscais conforme periodicidade, formato e sistema estabelecidos pelo órgão central de contabilidade da União,

os quais deverão ser divulgados em meio eletrônico de amplo acesso público" (BRASIL, 2000).

Assim, referido dispositivo legal, esclarece que, para uma gestão fiscal transparente, é imprescindível que se dê publicidade as informações relativas a execução orçamentária e financeira.

Para além disso, a Lei 12.527, de 18 de novembro de 2011, com o objetivo de regular o acesso à informações, aloca, entre suas diretrizes a necessidade de "observância da publicidade como preceito geral e do sigilo como exceção" (BRASIL, 2011).

Ademais, o Supremo Tribunal Federal, também se posicionou acerca da publicidade nos atos de gestão. Através do Recurso Extraordinário nº 71.652, no qual se consagrou o entendimento de que "o ato administrativo somente começa a produzir seus efeitos depois de publicado, e no respectivo órgão oficial" (BRASIL, 1971).

Ante o exposto, denota-se o necessário comprometimento da Administração Pública em efetivar o direito fundamental à proteção de dados pessoais, sem prejuízo ao direito fundamental de acesso público à informação e à publicidade e à transparência, tarefa que não se apresenta de forma tão simples.

Para tanto, necessário elucidar a estrutura normativa da proteção de dados pessoais no Brasil, de forma gradativa, partindo de um estudo na Constituição Federal de 1988, passando pelas leis setoriais, culminando no estudo da LGPD e novamente, da CF/88 por meio da Emenda Constitucional nº 115 de 2022.

1.5 ESTRUTURA NORMATIVA DA PROTEÇÃO DE DADOS PESSOAIS NO ORDENAMENTO JURÍDICO BRASILEIRO

A trajetória da proteção de dados pessoais no ordenamento jurídico brasileiro foi marcada por decisões conflitantes mas que, ao mesmo tempo, contribuíram para uma sedimentação do tema nos diversos dispositivos normativos até então previstos desde a entrada em vigor da LGPD.

A ênfase e a urgência na elaboração de mecanismos de supervisão e de controle desses dados, citados como fundamentos na impugnação de determinadas situações, se traduzem na vulnerabilidade dos dados pessoais, especialmente no ambiente virtual e quando armazenados em quantidades significativas, ante as inúmeras possibilidades de seu uso

indevido, a exemplo de vazamentos, prática de crimes cibernéticos e de golpes, até mesmo a venda dos dados pode gerar um prejuízo imensurável na vida dos cidadãos, além de pôr em xeque a credibilidade daqueles que detém o poder de guarda.

Nessa senda, o que se pleiteia é a autonomia do titular no gerenciamento de seus próprios dados, ou seja, que ele detenha o poder de decidir sobre: como (meio de tratamento), por quê (motivo), para que (finalidade) e até quando (duração), seus dados estarão em poder de terceiros e poderão ser divulgados. Com essa compreensão não se busca a consagração de um direito absoluto no ordenamento pátrio, mas sim, uma garantia em razão de um direito assegurado, ainda que implicitamente, o direito a proteção de dados.

Inobstante a vigência da LGPD, sabe-se que os desafios que permeiam a proteção e o tratamento dos dados persistirão em decorrência da visão abrangente suscitada pela própria norma, onde se busca uma mudança de postura das partes envolvidas, sobretudo, na sua forma de "pensar" e agir frente a complexidade do sistema envolto a temática.

Assim, a análise dos dispositivos normativos pertinentes a proteção de dados pessoais faz-se necessária ante o impacto que as novas tecnologias exercem na sociedade informacional, seja na seara de direito público seja na seara de direito privado.

Para tanto, passa-se ao estudo da evolução normativa da proteção de dados pessoais no Brasil com a análise da Constituição Federal de 1988, do Código de Defesa do Consumidor conjuntamente a Lei do Cadastro Positivo, perpassando pela análise da Lei de Acesso à Informação, do Marco Civil da Internet até a Lei Geral de Proteção de Dados.

A constitucionalização do direito no Brasil representou importante avanço no cenário social e jurídico, haja vista que esse fenômeno alçou a Constituição Federal de 1988 ao patamar de centro do sistema jurídico. Assim, qualquer ato infraconstitucional deve guardar pertinência, não só formal, mas também material, com as normas constitucionais.

É o que acontece com a proteção de dados pessoais, cuja vigência integral da lei que dispõe sobre o tema, a Lei Geral de Proteção de Dados (LGPD), se deu no ano de 2020. Em que pese as discussões sobre o direito fundamental à proteção de dados tenham se intensificado após sua vigência, relevantes questionamentos já perduravam no ordenamento jurídico pátrio, sobretudo com base na Constituição Federal de 1988.

Malgrado as discussões nem sempre tenham tido como objeto principal a proteção de dados pessoais, importante destacá-las haja vista que suas contribuições no decorrer dos anos

fomentaram a compreensão pela necessidade de tutela específica do tema frente aos perigos ocasionados pela ausência de proteção efetiva na proteção dos dados pessoais.

O fenômeno da constitucionalização do direito no Brasil teve como marco primordial, a Constituição Federal de 1988, com a redemocratização do país. Esse importante documento normativo é caracterizado pela doutrina majoritária como constituição analítica, decorrente do exacerbado conteúdo abarcado por ela.

Segundo (BARROSO, 2005, p. 20) todos os principais ramos do direito são abordados na Constituição Federal de 1988. Reportando-se ao seu art. 5º, que dispõe sobre os direitos e garantias fundamentais, denota-se a presença de temas que envolvem o direito penal, o direito processual penal e o direito trabalhista, por exemplo.

Mais adiante, em seu art. 37, apresentam-se os princípios constitucionais do direito administrativo. Por conseguinte, nossa atual constituição também dispõe sobre a ordem econômica e financeira bem como dispõe sobre a ordem social.

Com esse fenômeno, "a Constituição passou a desfrutar já não apenas da supremacia formal que sempre teve, mas também de uma supremacia material, axiológica, potencializada pela abertura do sistema jurídico e pela normatividade de seus princípios" (BARROSO, 2005, p. 21).

Dessa forma, qualquer ato infraconstitucional deve ser lido e interpretado com supedâneo nas normas constitucionais, a fim de torná-las efetivas. Não se pode perder de vista que a constitucionalização do direito traz uma carga de protagonismo judicial, sobretudo ao Supremo Tribunal Federal, o qual compete zelar pela Constituição.

A Constituição Federal de 1988 é considerada uma Constituição Cidadã por prever diversos direitos e garantias aos seus destinatários. Além do mais, possui diversos princípios que possibilitam uma margem de abrangência em sua interpretação por parte do legislador e do Judiciário, haja vista que "com a influência do Constitucionalismo hodierno, os direitos fundamentais ganham proporções incomensuráveis e de forte relevância no contexto pátrio, sobretudo buscando-se garantir a dignidade da pessoa humana" (DIAS; SILVA, 2020, p.03).

Nessa perspectiva, dentre os direitos e as garantias fundamentais ali previstos, destaca-se o inciso XII, do art. 5º, *in verbis*: É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (BRASIL, 1988).

Trata-se de uma importante garantia prevista constitucionalmente. No entanto, com base no supracitado dispositivo constitucional, o Supremo Tribunal Federal foi instado a se manifestar em algumas ocasiões, o que gerou importantes discussões a respeito da proteção de dados pessoais, ainda que de forma incipiente.

Posto que "a Constituição deve conter – e juízes e tribunais devem implementar – direitos fundamentais, princípios e fins públicos que realizem os grandes valores de uma sociedade democrática: justiça, liberdade e igualdade" (BARROSO, 2010).

Nessa seara, passa-se ao estudo de alguns julgados da Corte Superior que fomentaram o estudo acerca de um direito fundamental à proteção de dados pessoais.

O primeiro julgado a ser destacado é o Mandado de Segurança nº 21.729/DF, cuja decisão pontuou que o âmbito de proteção contido no inciso XII, do art. 5º da Constituição Federal de 1988 refere-se à comunicação de dados, e não dos dados em si (BRASIL, 1995).

O Mandado de Segurança foi impetrado pelo Banco do Brasil S/A em face do Ministério Público Federal em razão da solicitação de informações sobre concessão de empréstimos, subsidiados pelo Tesouro Nacional, com base em plano de governo, a empresas do setor sucroalcooleiro[5].

O fundamento aduzido pelo Banco foi o sigilo bancário. Entretanto, restou denegada a concessão da segurança, sob os seguintes fundamentos:

> a) as informações reclamadas são indispensáveis à instrução de procedimento administrativo no âmbito do Ministério Público Federal para investigar a concessão de empréstimos de 1 bilhão e 100 milhões de dólares pelo Governo Federal, por intermédio do Impetrante, a empresas do setor sucroalcooleiro em que pese a existência de débito para com a instituição bancária e também para com a Previdência Social;
> b) o sigilo bancário apenas obstaculiza o fornecimento de informações a terceiros;
> (…)
> d) a proteção de dados de que cogita o inciso XII do artigo 5º da constituição federal não alcança a hipótese;
> e) no caso, a requisição de dados diz respeito a financiamentos específicos concedidos a pessoas jurídicas, não se podendo cogitar da inviolabilidade da vida privada;
> (…).

Nesse sentido, importa mencionar trecho do voto do Ministro Francisco Rezek, *in verbis*:

5 É o que consta na ementa do MS nº 21. 729-4 DF de 05/10/1995.

> Do inciso XII, por seu turno, é de ciência corrente, que ele se refere ao terreno das comunicações: a correspondência comum, as mensagens telegráficas, a comunicação de dados, e a comunicação telefônica. Sobre o disparate que resultaria do entendimento de que fora do domínio das comunicações, os dados em geral – e a seu reboque o cadastro bancário – são invioláveis, não há o que dizer. O funcionamento mesmo do Estado e do setor privado enfrentaria um bloqueio. A imprensa, destacadamente, perderia sua razão de existir (BRASIL, 1995).

Em contraponto, destaca-se trecho do voto do Ministro Relator Marco Aurélio informando que:

> O direito à preservação da intimidade mostra-se de forma alargada, valendo notar que o inciso seguinte, o XII, prevê o sigilo quanto a dados e comunicações telefônicas, isto sem considerar-se o trecho inicial do dispositivo, no que preserva a correspondência e as comunicações telegráficas (BRASIL, 1995).

Vislumbra-se o debate acerca do inciso XII do artigo 5º da Constituição enquanto norma garantidora do sigilo de dados ou da comunicação de dados.

Ademais, o voto do relator seguiu o entendimento a favor da concessão em caráter liminar da segurança e com o entendimento de que a norma constitucional previa o sigilo de dados. Todavia, seu voto restou vencido junto aos votos dos Ministros Maurício Corrêa, Celso de Mello, Ilmar Galvão e Carlos Velloso.

O que se extrai do mencionado julgado é a compreensão de que a norma constitucional prevista no inciso XII do artigo 5º da Constituição Federal de 1988 assegura o sigilo da comunicação dos dados e não dos dados em si.

Posicionamento ratificado quando do julgamento do Recurso Extraordinário nº 418.416 no qual se impugnava ato judicial que deferiu medida de busca e apreensão nas empresas do paciente, inclusive de computadores e disquetes para decodificação dos dados ali inseridos e autorizava o compartilhamento de tais informações entre a Receita Federal e a fiscalização do Instituto Nacional de Seguridade Social, o INSS, para eventual instauração de procedimentos de natureza administrativa e fiscal.

Em razão da importância dos debates sobre os dados pessoais no RE nº 418.416, extrai-se trechos do posicionamento do Ministro Ricardo Lewandowski:

> É justamente o fato de os dados apreendidos terem sido compartilhados com a Receita Federal e a fiscalização do INSS. Penso ter havido um extravasamento indevido dos dados de um processo penal que possuía um objeto específico.
> (…)

> Estamos definindo, aqui, um "*leading case*" muito importante. Se deixarmos consignado que os dados de um determinado processo podem extravasar o âmbito do processo para autoridades administrativas sem qualquer restrição, isso poderá representar um precedente gravíssimo (BRASIL, 2006).

Ressalta-se que a proposta do Ministro Ricardo Lewandowski de restringir a utilização de dados da investigação criminal em curso foi acolhida pelos Ministros Marco Aurélio e Celso de Mello. No entanto, o Tribunal, por maioria, a rejeitou[6].

Dessa forma, restou decidido que não houve quebra do sigilo das comunicações de dados, com menção ao posicionamento proferido no MS 21.729/DF anteriormente discutido, com adoção da tese de Tércio Sampaio Ferraz Júnior, ressaltando, nos termos do Ministro Sepúlveda Pertence que: "a proteção a que se refere o art. 5º, XII, é da comunicação de dados e não os dados" (BRASIL, 2006).

Outro importante caso envolvendo a proteção de dados pessoais refere-se a Ação Penal nº 307-3 DF, que debateu a validade de prova obtida por meio de decodificação de dados armazenados em microcomputador apreendido. No caso, foi reconhecida a ilegalidade da prova em virtude de ser decorrente da apreensão de computador realizada sem mandado de busca e apreensão (BRASIL, 1997).

Para fins de elucidação colaciona-se trecho do voto do Ministro Moreira Alves:

> Ainda que se pretendesse que a apreensão do micro-computador fosse lícita, dando margem posteriormente à declaração de perdimento dele em favor do Estado, nem por isso poderia a Polícia Federal apoderar-se dos dados contidos nesse micro-computador, mandando decodificá-los para deles utilizar-se como prova em processo penal.
> Com efeito, também com relação aos dados em geral, - e, consequentemente, os constantes de computador que pode armazenar as mais sigilosas informações de seu proprietário –, eles estão cobertos pela garantia do disposto no inciso XII do artigo 5º da atual Constituição (BRASIL, 1997).

Acrescenta o Ministro Ilmar Galvão

> (…) a invasão da memória dos computadores implica fatalmente a quebra do sigilo não apenas de dados em geral, desde os relativos a simples agenda até os relacionados a fórmulas e cálculos, mas também de toda a correspondência, epistolar e telegráfica, em relação aos quais o manto constitucional é de natureza absoluta, já que não deixou espaço reservado ao trabalho normativo do legislador ordinário, como se fez com as comunicações telefônicas (BRASIL, 1997).

6 Informação contida no extrato de ata do RE nº 418.416-8 de 10/05/2006.

A respeito do tema importante a lição de (SARLET, 2018, p. 411-412) ao dispor sobre as reservas legais simples e qualificadas. As reservas legais simples são aquelas nas quais não há expressa previsão constitucional acerca dos parâmetros a serem observados pelo legislador, ou seja, as restrições serão previstas em lei, norma infraconstitucional, geralmente marcadas pela expressão 'salvo nas hipóteses previstas em lei'.

Por outro lado, as normas qualificadas já trazem em seu bojo constitucional os pressupostos a serem observados na aplicação de seu dispositivo, a exemplo do inciso XII do artigo 5º da Constituição, ora mencionado, quanto ao sigilo das comunicações telefônicas (SARLET, 2018, p. 411-412).

A importância do julgado se dá pela compreensão de que a obtenção da prova ocorreu sem a observância do princípio do contraditório e incorreu em violação a privacidade alheia, bem como em violação ao domicílio e violação à garantia da inviolabilidade da intimidade das pessoas[7].

Em seguida, analisa-se a proteção de dados pessoais com ênfase nas relações de consumo.

Nessa perspectiva, a Lei nº 8.078 de 1990 dispõe sobre a proteção ao consumidor, e, no tocante à proteção de dados, regula o acesso as informações constantes em bancos de dados mantidos pelas Instituições, sejam de caráter público ou privados.

Destaca-se o §2º, do art. 43 do referido diploma legal, *in verbis*:

> O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
> A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele (BRASIL, 1990).

Assim, extrai-se do comando legal a observância ao dever constitucional de acesso à informação, bem como a necessidade de comunicação expressa ao consumidor quando da abertura de qualquer meio que armazene os dados pessoais.

Importante discussão jurisprudencial se deu na Apelação Cível nº 70069420503 do Tribunal de Justiça do Rio Grande do Sul (TJRS) na qual foi ajuizada pelo Ministério Público, Ação Coletiva, em face da Confederação Nacional de Dirigentes Lojistas, (SPC BRASIL), em

7 Conforme disposto na ementa da Ação Penal nº 307-3 DF de 13/12/94.

razão da venda de dados e de informações pessoais de consumidores sem a prévia anuência destes, para utilização na prospecção de futuros clientes (RIO GRANDE DO SUL, 2016).

Com essa decisão, restou consignada a possibilidade de comercialização dos dados pessoais dos consumidores, sob um fundamento de que estes não estariam abarcados por uma proteção legal quanto ao sigilo ou pendência de prévia autorização para sua utilização.

Por conseguinte, o Tribunal também entendeu que existe uma diferenciação entre dados de identificação e dados sensíveis. Assim, os dados de identificação poderiam ser comercializados em contraponto aos dados sensíveis. Na ocasião decidiu-se que os dados em questão eram de identificação, por sua vez, não sigilosos, tratando-se de informação fornecida nas relações negociais cotidianas.

De outro modo, apresenta-se o julgado no REsp nº 1.419.697 que avaliou a natureza do sistema *scoring* e a possibilidade de violação a princípios e regras do CDC e com isso gerar um direito a indenização por dano moral (BRASIL, 2014).

Na ocasião, a tese adotada pelo Superior Tribunal de Justiça foi a de que:

> 1) O sistema "credit scoring" é um método desenvolvido para avaliação do risco de concessão de crédito, a partir de modelos estatísticos, considerando diversas variáveis, com atribuição de uma pontuação ao consumidor avaliado (nota do risco de crédito).
> 2) Essa prática comercial é lícita, estando autorizada pelo art. 5º, IV, e pelo art. 7º, I, da Lei n. 12.414/2011 (lei do cadastro positivo).
> 3) Na avaliação do risco de crédito, devem ser respeitados os limites estabelecidos pelo sistema de proteção do consumidor no sentido da tutela da privacidade e da máxima transparência nas relações negociais, conforme previsão do CDC e da Lei n. 12.414/2011.
> 4) Apesar de desnecessário o consentimento do consumidor consultado, devem ser a ele fornecidos esclarecimentos, caso solicitados, acerca das fontes dos dados considerados (histórico de crédito), bem como as informações pessoais valoradas.
> 5) O desrespeito aos limites legais na utilização do sistema "credit scoring", configurando abuso no exercício desse direito (art. 187 do CC), pode ensejar a responsabilidade objetiva e solidária do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consulente (art. 16 da Lei n. 12.414/2011) pela ocorrência de danos morais nas hipóteses de utilização de informações excessivas ou sensíveis (art. 3º, § 3º, I e II, da Lei n. 12.414/2011), bem como nos casos de comprovada recusa indevida de crédito pelo uso de dados incorretos ou desatualizados (BRASIL, 2014).

Assim, o STJ entendeu que a natureza do sistema *scoring* constitui uma metodologia de cálculo do risco de crédito e não um banco de dados de consumidores, o qual se utiliza de modelos estatísticos e dos dados existentes no mercado, acessíveis na internet não se exigindo o prévio e expresso consentimento do consumidor.

O que não se pode perder de vista é a natureza dos dados utilizados e os potenciais prejuízos do uso indevido a esses consumidores. Para todo aquele que, de alguma forma, lida com dados de terceiros, exige-se dever de diligência em seu tratamento. Ademais, o fato de os dados encontrarem-se em domínio público, na internet, não retira seu caráter indisponível, tampouco a proteção assegurada.

Por sua vez, a Lei nº 12.527 de 2011, Lei da Acesso à Informação (LAI) tem por objetivo regular o acesso à informação com vistas à efetivação dos princípios da publicidade e da transparência pela Administração Pública.

Em que pese sua atuação ser voltada para a seara pública, razoável compreender a razão de tal normativo dispor sobre o tratamento de informações pessoais pelos agentes públicos, tendo em vista que a Administração Pública também dispõe de banco de dados, os quais concentram inúmeros dados da população brasileira.

Nesse sentido, a LAI dispõe de uma seção específica tratando sobre as informações pessoais, a seção V, prevista no art. 31[8] que alude aos direitos da personalidade previstos no Código Civil. Observa-se que tais direitos são considerados limitativos à atuação da Administração Pública no tratamento das informações pessoais.

São os direitos relativos à imagem, honra, intimidade, vida privada das pessoas, sem prejuízo às liberdades e garantias individuais.

No mesmo viés, o supracitado artigo informa sobre a restrição ao acesso das informações pessoais, pelo prazo máximo de cem anos. Além disso, a norma traz dois legitimados para acessar tais dados, o titular e o agente público legalmente autorizado.

8 Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais. § 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem: I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem. § 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido. § 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias: I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico; II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem; III - ao cumprimento de ordem judicial; IV - à defesa de direitos humanos; ou V - à proteção do interesse público e geral preponderante. § 4º A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância. § 5º Regulamento disporá sobre os procedimentos para tratamento de informação pessoal.

Percebe-se a limitação no espectro de legitimados por parte do legislador no tratamento das informações pessoais, evitando, de certo modo, a concentração das informações em questão, que, por sua vez, são armazenadas em grande quantidade, em verdadeiros bancos de dados, nas mãos de quaisquer agentes públicos.

Importa destacar que a divulgação ou o acesso as informações de caráter pessoal somente poderão ser divulgadas ou acessadas por terceiros mediante previsão legal ou consentimento expresso do titular. Sendo desnecessário o consentimento nas hipóteses expressamente previstas na lei, a exemplo do cumprimento de ordem judicial e as relativas à defesa de direitos humanos.

Importa destacar também a expressa menção da norma a responsabilização do agente que utilizar indevidamente as informações pessoais.

A Lei nº 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet (MCI) "estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria" (BRASIL, 2014), conforme dispõe seu art. 1º.

Consoante (BIONI, 2019) sua proeminência consolidou-se com o episódio do escândalo de espionagem revelado pelo ex-analista Edward Snowden, da Agência Nacional de Segurança dos Estados Unidos.

Nesse sentido, o MCI trouxe, em seu arcabouço, a proteção de dados pessoais com enfoque anteriormente não visto no ordenamento jurídico brasileiro.

Destaca-se o desenvolvimento da personalidade, como um de seus fundamentos e, dentre seus princípios, a proteção de dados pessoais. A norma legal, ao dispor expressamente sobre o tema, demonstra necessária preocupação com os impactos dos dados pessoais na internet.

Outro importante aspecto constante no MCI diz respeito aos direitos e garantias dos usuários os quais distinguem-se o direito de não fornecimento de dados pessoais por seu titular, a terceiros (art. 7º, VII), com a ressalva de seu consentimento livre, expresso e informado ou de outras hipóteses previstas em lei; o acesso a informações claras e completas no que concerne ao uso, coletas, armazenamento, tratamento e proteção de seus dados pessoais que, por sua vez, só poderão ser utilizados para finalidades que: justifiquem sua coleta, que não sejam vedadas pela legislação, e que estejam especificadas nos contratos de

prestação de serviços ou em termos de uso de aplicações de internet (art. 7º, VIII) (BRASIL, 2014).

Ademais, imperativo que haja o consentimento expresso do titular sobre a coleta, o uso, o armazenamento e o tratamento de seus dados pessoais, com destaque das demais cláusulas contratuais (art. 7º, IX) (BRASIL, 2014).

Salienta-se também a possibilidade de exclusão definitiva dos dados pessoais através de requerimento de seu titular, cuja ressalva decorre das hipóteses na qual se exige sua guarda obrigatória (art. 7º, X) (BRASIL, 2014).

Sob outro enfoque, o presente normativo busca, além da proteção aos dados pessoais, o respeito aos demais direitos da personalidade, conforme alude seu art. 10, senão vejamos: "a guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas" (BRASIL, 2014).

Nessa seara, o MCI realizou uma distinção entre a proteção de dados e os demais direitos da personalidade, como a honra, a imagem, a intimidade e a vida privada, enfatizando que não se trata, necessariamente, de uma extensão de outros direitos, mas sim, um direito autônomo.

Preleciona (BIONI, 2019):

> Pela combinatória de tais dispositivos, verifica-se ser a autodeterminação informacional o parâmetro normativo eleito pelo MCI para a proteção de dados pessoais. Todas as normas desembocam na figura do cidadão-usuário para que ele, uma vez cientificado a respeito do fluxo de seus dados pessoais, possa controlá-lo por meio do consentimento. Essa perspectiva de controle perpassa desde a fase de coleta e compartilhamento dos dados com terceiros até o direito de deletá-los junto ao prestador de serviços e produtos de Internet ao término da relação.

Portanto, o Marco Civil da Internet se apresenta como um instrumento normativo que, além de demonstrar uma preocupação com a proteção dos dados pessoais, insculpido como um de seus princípios que regem o uso da internet no país, pauta-se também, na compreensão da autodeterminação informativa com vistas a efetivação da proteção de dados pessoais.

Por outro prisma, a Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados (LGPD), entrou em vigor no ano de 2020. Trata-se da primeira lei brasileira que tutela, de forma específica, a proteção de dados pessoais.

A LGPD sofreu forte influência do Regulamento Geral de Proteção de Dados (RGPD) que substituiu a Diretiva 95/46/CE, da União Europeia. Essa influência é tão significativa ao ponto de a LGPD consagrar uma mudança na cultura organizacional com foco na postura ativa de todos aqueles que a ela encontram-se submetidas.

Inicialmente, cumpre destacar a teoria da Autorregulação Regulada. A partir dela, compreende-se que a norma traz parâmetros mínimos a serem seguidos por todos aqueles a submetidos à sua observância. Assim, a norma concede uma margem de liberdade para que esses utilizem os melhores mecanismos à sua disposição para sua adequação a LGPD.

Trata-se da criação de um programa de governança em privacidade pelas Organizações (IRAMINA, 2020, p. 93).

Destaca-se, nesse cenário o Projeto de Lei nº 6212 de 2019 de autoria do Senador Antonio Anastasia (PSDB/MG) cujo objetivo é alterar a LGPD para dispor sobre corregulação ou autorregulação regulada. Referido Projeto de Lei estabelece alguns requisitos para a produção de atos normativos de corregulação a exemplo da necessidade de identificação de autoria, acompanhada de exposição de motivos e da avaliação de impacto regulatório; fases de consulta e audiência públicas; dentre outros requisitos, conforme se extrai do art. 51-B (BRASIL, 2019).

No próprio Projeto de Lei explica-se, de forma sucinta o que se entenderia por corregulação. Cuida-se da "possibilidade de que os próprios controladores ou operadores de dados pessoais elaborem, individualmente ou por meio de associações, regras de boas práticas e de governança sobre os dados pessoais, as quais, conforme parágrafo terceiro, podem ser reconhecidas pela Autoridade Nacional de Proteção de Dados" (BRASIL, 2019).

Destarte, a teoria da autorregulação regulada ou corregulação, está relacionada às boas práticas e de governança da LGPD, aduzindo que

> Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (BRASIL, 2018).

Segundo Iramina (2020, p. 108):

> A governança nodal, por sua vez, incentiva a participação efetiva de indivíduos e instituições variadas, principalmente do setor privado, que possuem um conjunto de tecnologias, conhecimentos e modos de pensar variados, para buscar contornar o déficit de capacidade regulatória de alguns dos países, desonerando a estrutura estatal do ônus de implementar todas as medidas de incentivo à conformidade normativa do regulado.

O que se busca, então, é a participação ativa e colaborativa das Organizações na implementação de mecanismos voltados à sua adequação à LGPD, desonerando o Estado da responsabilidade única de promoção desses meios e, por conseguinte, diminuindo o ônus estatal. Afinal, quem melhor do que os regulados para compreender seus próprios déficits e, sobretudo, os meios de que dispõem, inclusive financeiros, para promover sua adequação à norma geral?

No que concerne a abordagem regulatória, sua "característica fundamental está na necessidade de que os próprios regulados exercitem, em maior grau, habilidades colaborativas e assumam responsabilidades por seus atos" (IRAMINA, 2020, p. 105).

Assim, os regulados devem dispor de uma política interna, composta por princípios, diretrizes, mecanismos de supervisão e controle, consagrando as boas práticas de gestão e de governança que viabilize o *compliance* e a *accountability* constantemente.

Sua finalidade consiste no incentivo à voluntariedade dos regulados na aderência da norma, sempre buscando uma cooperação entre as partes, apenas aplicando-se as sanções em *ultima ratio,* ou seja, quando restar verificado a obstaculização por parte dos regulados.

No tocante ao direito à autodeterminação informativa, importa elucidar que encontra amparo no inciso II do art. 2º, da LGPD, que a consagrou como um dos fundamentos da proteção de dados pessoais.

Cuida-se de uma construção jurisprudencial do Tribunal Constitucional alemão cujo ponto fulcral se deu na sentença do recenseamento, entre os anos de 1982 e 1983.

Segundo (MENDES, 2020, p. 11) o objeto do litígio refere-se ao processamento eletrônico de dados, inovação tecnológica à época, que incorreu em um número significativo no armazenamento e transmissão desses dados.

Nessa seara, ainda consoante (MENDES, 2020, p. 11), compreendeu o Tribunal, que o processamento massivo de dados pessoais "ameaçaria o poder do indivíduo de decidir por si mesmo se e como ele desejaria fornecer a terceiros os seus dados pessoais", haja vista a possibilidade de perfilização de tais indivíduos e, consequentemente sua identificação.

Nesse sentido, Laura Schertel Mendes afirma:

> Por conseguinte, da dimensão objetiva do direito à autodeterminação informativa decorre não apenas um dever de proteção contra o conhecimento não autorizado por terceiros, mas também um dever de proteção contra o consentimento meramente aparente (ou fictício) quanto ao tratamento de dados. Dos deveres de proteção decorrentes do direito à autodeterminação informativa resulta, assim, um controle judicial específico também de contratos que regulam o tratamento de dados (MENDES, 2020, p. 15).

No Brasil, salienta-se a edição da Medida Provisória nº 954 de 2020, com previsão de compartilhamento de dados por empresas de telecomunicações prestadoras de serviço em telefonia fixa e móvel com a Fundação Instituto Brasileiro de Geografia e Estatística (IBGE) com a finalidade de subsidiar a "Pesquisa Nacional por Amostra de Domicílios Contínua (PNAD Contínua), que consiste na maior operação estatística domiciliar empreendida regularmente pelo IBGE, com mais de 200 mil domicílios pesquisados a cada trimestre[9]" (BRASIL, 2020).

Na ocasião, ADIs foram impetradas em face da referia MP, dentre as quais, destaca-se a ADI nº 6.387 de autoria da Associação *Data Privacy* Brasil de Pesquisa, que requereu sua intervenção no feito na qualidade de *Amicus Curiae*, a qual foi deferida.

Pugnou-se pela inconstitucionalidade formal, sob o fundamento da ausência de preenchimento dos requisitos de urgência e relevância, imprescindíveis na edição de uma MP, bem como, pela inconstitucionalidade material, alegando violação a dignidade humana, a intimidade, a vida privada, a honra e a imagem das pessoas, além da comunicação dos dados. Pugnou-se também pelo reconhecimento do direito fundamental à autodeterminação informativa.

Ressalta-se que "o vício da MPV 954/2020 não é em si a previsão do compartilhamento de dados para o IBGE, mas a insuficiência das salvaguardas nela previstas que se conformasse ao princípio do devido processo legal" (BRASIL, 2020, p. 21).

A MP não dispunha de mecanismos de supervisão, controle e prevenção contra o uso indevido dos dados que seriam compartilhados, o que ocasionaria uma vulnerabilidade significativa para os cidadãos ante a possibilidade de vazamento, perfilização, dentre outros riscos.

Nesse diapasão, dita MP teve sua eficácia suspensa pelo STF, inicialmente em sede liminar, posteriormente referendada pela Corte Constitucional, cujo prazo de validade se deu em 03 de agosto de 2020 (BRASIL, 2020).

9 Conforme consta na exposição de motivos.

Vislumbra-se a autodeterminação informacional em uma relação intrínseca com os princípios da dignidade humana e do livre desenvolvimento da personalidade do indivíduo, mas não necessariamente, extensão destes, em verdade, consiste em um direito autônomo cuja tutela diz respeito a forma como determinado indivíduo pretende se apresentar a sociedade onde a autonomia na gestão de seus próprios dados se mostra indispensável.

Por fim, aponta-se a Proposta de Emenda à Constituição nº 17 de 2019, que objetiva "alterar os artigos 5°, XII, e 22, XXX, da Constituição Federal para incluir o direito fundamental à proteção de dados pessoais, bem como estabelecer a competência privativa da União para legislar sobre o tema" (DONEDA, 2020).

A proposta foi aprovada e incorporada no ordenamento brasileiro por meio Emenda Constitucional nº 115 de 2022. A partir de então, a proteção de dados pessoais constitui um direito fundamental assegurado expressamente na Constituição Federal de 1988.

Analisados os instrumentos normativos que dispõem sobre dados pessoais no cenário nacional, a seguir, analisam-se documentos internacionais a respeito do tema.

1.6 BREVES CONSIDERAÇÕES SOBRE A PROTEÇÃO DE DADOS PESSOAIS NO CENÁRIO INTERNACIONAL

Na perspectiva internacional, a proteção de dados pessoais possui significativa relevância com a promulgação de inúmeros instrumentos sobre o tema.

Inicialmente, destacam-se as *Diretrizes e Recomendações da Organização para a Cooperação e Desenvolvimento Econômico (OCDE)*. Trata-se de Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais, em vigor no ano de 1980. Essas Diretrizes já apontavam importantes definições para a temática da proteção de dados pessoais, como os conceitos de controlador de dados, dado pessoal e fluxos transfronteiriços de dados pessoais.

Para além disso, já previam princípios pertinentes ao tema, a saber: (i) princípio de limitação da coleta; (ii) princípio de qualidade dos dados; (iii) princípio de definição da finalidade; (iv) princípio de limitação de utilização; (v) princípio do *back-up* de segurança; (vi) princípio de abertura; (vii) princípio de participação do indivíduo e; (viii) princípio de responsabilização.

Apresenta-se também a *Convenção para a Proteção dos Indivíduos com relação ao Processamento de Dados Pessoais (Convenção 108*) do Conselho da Europa, promulgado no ano de 1981. Cuida-se do "primeiro instrumento internacional juridicamente vinculativo adotado no domínio da proteção de dados", o qual visa a garantia dos direitos e liberdades fundamentais dos indivíduos, em especial "o direito à vida privada, face ao tratamento automatizado dos dados de caráter pessoal" (CONSELHO DA EUROPA, 1981).

Atualmente, a Convenção conta com 27 (vinte e sete) assinaturas não seguidas de ratificações e 17 (dezessete) adesões com ratificações. Frisa-se que tal instrumento internacional é de extrema relevância, sobretudo, pelo caráter vinculante de seus preceitos, isto é, cada país signatário assume um compromisso de submissão aos preceitos nela estabelecidos, há uma força cogente na referida Convenção.

De grande relevância no contexto internacional cujos preceitos em muito foram adotados pela LGPD, é o *General Data Protection Regulation* (GDPR) da União Europeia, substituta da Diretiva 95/46 CE.

Em relação a esse documento normativo internacional, da leitura do seu tópico 2, no art. 1º do capítulo I, percebe-se o tratamento da proteção de dados pessoais como um direito fundamental, *in verbis*: "… O presente regulamento defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais" (UNIÃO EUROPEIA, 2016).

O GDPR traz, em seu capítulo I, art. 4º, importantes definições, a exemplo do conceito de dado pessoal, o qual se refere a "informação relativa a uma pessoa singular identificada ou identificável", e do conceito de tratamento, consistente na "operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registro, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição" (UNIÃO EUROPEIA, 2016).

O Regulamento Europeu de Proteção de Dados apresenta, ainda, as hipóteses de licitude do tratamento de dados que, em muito se assemelham as bases legais para o tratamento de dados pessoais insculpidos na LGPD, *in verbis*:

> O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:
>
> •a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;
>
> •b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;
>
> •c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;
>
> •d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
>
> •e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;
>
> •f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.
>
> O primeiro parágrafo, alínea f), não se aplica ao tratamento de dados efetuado por autoridades públicas na prossecução das suas atribuições por via eletrónica (UNIÃO EUROPEIA, 2016).

As hipóteses que justificam o tratamento de dados pessoais na LGPD serão objeto de análise detida no capítulo a seguir.

No que toca aos direitos fundamentais, importante a lição de Robert Alexy ao explanar sobre a teoria da colisão que se relaciona com a teoria dos princípios. Adverte o autor que, diante de uma colisão entre princípios, ou seja, quando a aplicação de um importar na inaplicabilidade do outro, com base na análise do caso concreto, não ocorre a invalidação ou a eliminação do princípio de seu ordenamento pátrio, o que ocorre, de fato, é um sopesamento entre estes, o qual o autor trata como relação de precedência condicionada entre princípios (ALEXY, 2008, p. 97).

Reconhece-se expressa menção a proteção de dados pessoais como um direito fundamental na *Declaração de Santa Cruz de La Sierra*, firmada pelo Governo Brasileiro em 15 de novembro de 2003 (DONEDA, 2011, p. 103). A previsão encontra-se em seu item 45, que assim dispõe:

> 45. Estamos também conscientes de que a protecção de dados pessoais é um direito fundamental das pessoas e destacamos a importância das iniciativas reguladoras ibero-americanas para proteger a privacidade dos cidadãos, contidas na Declaração de Antigua, pela qual se cria a Rede Ibero-Americana de Protecção de Dados, aberta a todos os países da nossa Comunidade (CÚPULA IBERO-AMERICANA DE CHEFES DE ESTADO E DE GOVERNO, 2003).

A *Carta dos Direitos Fundamentais da União Europeia*, traz expressamente, em seu capítulo II, que trata das liberdades, precisamente no art. 8º, a proteção de dados pessoais. Vejamos:

> 1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito.
> 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação
> 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente (PARLAMENTO EUROPEU, 2000).

O dispositivo prevê a necessidade de positivação de uma norma específica voltada à proteção de dados pessoais, bem como a criação de uma autoridade com o objetivo de fiscalização para o cumprimento das normas previstas, sem prejuízo do direito de acesso à informação e retificação da dados pelo seu titular. Hodiernamente, o Brasil conta com a LGPD e a ANPD enquanto instância administrativa de nível mais elevado na Administração Pública Federal referente ao tema.

Passadas as discussões a respeito da proteção de dados pessoais em âmbito nacional e internacional, segue-se com a análise do dever estatal de acesso público à informação, também nas perspectivas nacional e internacional, associando-o aos deveres de publicidade, transparência e cibertransparência.

1.7 O DEVER DE ACESSO PÚBLICO À INFORMAÇÃO NO CONTEXTO INTERNO E EXTERNO VINCULADO À PUBLICIDADE E À CIBERTRANSPARÊNCIA

O direito de acesso à informação foi consagrado na Constituição Federal de 1988, com previsão no art. 5º, XIV, *in verbis*: "é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional" (BRASIL, 1988).

Encontra previsão também no inciso XXXIII aduzindo que: "todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado" (BRASIL, 1988).

A garantia prevista para assegurar tal direito é o habeas data, insculpido no inciso LXXII do art. 5º, nos seguintes termos: "conceder-se-á habeas data a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo" (BRASIL, 1988).

Não obstante a previsão constitucional, a Lei nº 9.507, de 12 de novembro de 1997 ampliou as possibilidades para impetração com o respectivo remédio constitucional. A partir de então, é possível impetrar *habeas data* para assegurar o conhecimento sobre informações próprias, para retificação e para a complementação de informações, nos termos de seu art. 7º[10].

Por conseguinte, foi editada a Lei nº 12.527, de 18 de novembro de 2011, a Lei de Acesso à Informação (LAI) com o fito de privilegiar a publicidade e a transparência na esfera pública. Seu art. 3º deixa claro que o acesso à informação constitui um direito fundamental no qual devem ser observadas as seguintes diretrizes:

> I - observância da publicidade como preceito geral e do sigilo como exceção;
> II - divulgação de informações de interesse público, independentemente de solicitações;
> III - utilização de meios de comunicação viabilizados pela tecnologia da informação;
> IV - fomento ao desenvolvimento da cultura de transparência na administração pública;
> V - desenvolvimento do controle social da administração pública.

A Constituição Federal de 1988 estabeleceu expressamente como princípios gerais da Administração Pública a legalidade, a impessoalidade, a moralidade, a publicidade e a eficiência, este último assegurado por meio da Emenda Constitucional nº 19 de 1998.

Assim, o acesso à informação consiste em meio hábil à promoção da publicidade, da transparência, do controle social e da *accountability*, assim como à promoção da cidadania e da democracia, tal como se apresenta o Estado Democrático de Direito, previsto na Constituição Federal de 1988 em seu preâmbulo e no art. 1º.

10 Art. 7° Conceder-se-á *habeas data*: I – para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registro ou banco de dados de entidades governamentais ou de caráter público; II – para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo; III – para a anotação nos assentamentos do interessado, de contestação ou explicação sobre dado verdadeiro mas justificável e que esteja sob pendência judicial ou amigável.

Nas palavras de Eva Cecília Trindade Siqueira e Carlos Augusto Alcântara Machado:

> (…) a opinião pública pode ser construída ou modificada quando o cidadão tem acesso às informações públicas e à forma de utilização do patrimônio público pelos gestores. Desta forma, o cidadão pode interferir na Administração Pública através da formalização de denúncia aos órgãos fiscalizadores como Ministério Público e Tribunal de Contas (SIQUEIRA; MACHADO, 2020, p. 44).

Outrossim, a Lei de Acesso à Informação assegura não apenas o direito de acesso à informações de caráter público, mas pugna pela gestão transparente da informação com sua autenticidade e integridade. É a leitura do art. 6º, *in verbis*: "Cabe aos órgãos e entidades do poder público, observadas as normas e procedimentos específicos aplicáveis, assegurar a: (i) gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação; (ii) proteção da informação, garantindo-se sua disponibilidade, autenticidade e integridade; e (iii) proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso" (BRASIL, 2011).

Segundo o inciso III do art. 3º, a informação sigilosa é "aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado". Por sua vez, a informação pessoal é "aquela relacionada à pessoa natural identificada ou identificável", nos termos do inciso IV, também do art. 3º.

Denota-se que, mesmo para as informações consideradas sigilosas existe um lapso temporal a ser delimitado, ou seja, a informação pública não pode ser considerada sigilosa *ad eternum*.

Para tanto, os prazos máximos de duração do sigilo das informações encontram-se dispostos no §1º do art. 24. Para as informações classificadas no grau ultrassecreto, o prazo máximo de sigilo é de 25 (vinte e cinco) anos; para as secretas, o prazo máximo é de 15 (quinze) anos. Por fim, em relação as informações classificadas no grau de sigilo reservado, sua duração máxima é de 5 (cinco) anos.

Em âmbito internacional, o direito de acesso à informação encontra amparo na *Declaração Universal dos Direitos Humanos*, de 1948, prevendo em seu art. 19 que: "todo o indivíduo tem direito à liberdade de opinião e de expressão, o que implica o direito de não ser inquietado pelas suas opiniões e o de procurar, receber e difundir, sem consideração de fronteiras, informações e ideias por qualquer meio de expressão" (DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS, 1948).

Encontra amparo também no *Pacto Internacional dos Direitos Civis e Políticos*, em particular no seu art. 19, dispondo o seguinte:

> 1. Ninguém poderá ser molestado por suas opiniões.
> 2. Toda pessoa terá direito à liberdade de expressão; esse direito incluirá a liberdade de procurar, receber e difundir informações e idéias de qualquer natureza, independentemente de considerações de fronteiras, verbalmente ou por escrito, em forma impressa ou artística, ou por qualquer outro meio de sua escolha.
> 3. O exercício do direito previsto no parágrafo 2 do presente artigo implicará deveres e responsabilidades especiais. Conseqüentemente, poderá estar sujeito a certas restrições, que devem, entretanto, ser expressamente previstas em lei e que se façam necessárias para:
> a) assegurar o respeito dos direitos e da reputação das demais pessoas;
> b) proteger a segurança nacional, a ordem, a saúde ou a moral públicas (BRASIL, 1992).

Salienta-se também, a *Declaração Interamericana de Princípios de Liberdade de Expressão*, do ano 2000, cujo item 04 (quatro) aduz:

> O acesso à informação em poder do Estado é um direito fundamental do indivíduo. Os Estados estão obrigados a garantir o exercício desse direito. Este princípio só admite limitações excepcionais que devem estar previamente estabelecidas em lei para o caso de existência de perigo real e iminente que ameace a segurança nacional em sociedades democráticas (DECLARAÇÃO INTERAMERICANA DE PRINCÍPIOS DE LIBERDADE DE EXPRESSÃO, 2000).

A *Convenção das Nações Unidas contra a Corrupção*, promulgada em 2003, por seu turno, aponta em seu art. 10:

> Tendo em conta a necessidade de combater a corrupção, cada Estado Parte, em conformidade com os princípios fundamentais de sua legislação interna, adotará medidas que sejam necessárias para aumentar a transparência em sua administração pública, inclusive no relativo a sua organização, funcionamento e processos de adoção de decisões, quando proceder. Essas medidas poderão incluir, entre outras coisas:
> a) A instauração de procedimentos ou regulamentações que permitam ao público em geral obter, quando proceder, informação sobre a organização, o funcionamento e os processos de adoção de decisões de sua administração pública, com o devido respeito à proteção da intimidade e dos documentos pessoais, sobre as decisões e atos jurídicos que incumbam ao público;
> b) A simplificação dos procedimentos administrativos, quando proceder, a fim de facilitar o acesso do público às autoridades encarregadas da adoção de decisões; e
> c) A publicação de informação, o que poderá incluir informes periódicos sobre os riscos de corrupção na administração pública (BRASIL, 2006).

Levando-se em consideração a imprescindibilidade da participação social como mecanismo para coibir práticas de corrupção, referida Convenção também pontua a necessidade de adoção, por cada Estado Parte, de mecanismos que incentivem essa participação, tal como apresentam-se as seguintes medidas do art. 13: “a) Aumentar a transparência e promover a contribuição da cidadania aos processos de adoção de decisões; b) Garantir o acesso eficaz do público à informação; c) Realizar atividade de informação pública para fomentar a intransigência à corrupção, assim como programas de educação pública, incluídos programas escolares e universitários” (BRASIL, 2006).

No mesmo sentido, a Organização dos Estados Americanos (OEA) publicou a *Lei Modelo Interamericana 2.0 sobre Acesso à Informação Pública*. O documento está dividido em 8 (oito) capítulos, distribuídos da seguinte maneira: definições, alcance e direito de acesso e interpretação; medidas para promover a abertura; acesso à informação em poder das autoridades públicas; regime de exceções; apelações; órgão garante; medidas de promoção e cumprimento e medidas transitórias.

Sua importância reside no fato de que tal ferramenta

> Permite o aumento dos níveis de transparência e um combate efetivo à corrupção; promove concorrência aberta, investimento e crescimento econômico; fomenta a confiança pública nas instituições democráticas; e capacita os cidadãos, particularmente aqueles que estão em situação de vulnerabilidade, permitindo-lhes obter conhecimento adequado dos meios à sua disposição para melhorar seus padrões de vida e ter melhores oportunidades de colher os benefícios do crescimento econômico (ORGANIZAÇÃO DOS ESTADOS AMERICANOS, 2020, p. 09).

Não se pode perder de vista que a publicidade das informações públicas é a regra, inclusive enquanto promotora da cidadania e da democracia. Desse modo, as exceções abarcadas na Lei Modelo Interamericana são as informações reservadas e as confidenciais, assim definidas:

> a. informação reservada: compreende a informação pública que se exclui temporariamente do conhecimento das pessoas por existir um risco claro, provável e específico de dano a interesses públicos, conforme os requisitos contemplados nesta Lei;
> b. informação confidencial: compreende a informação privada em poder de sujeitos obrigados, cujo acesso público se proíbe por mandato constitucional ou legal, em razão de um interesse pessoal juridicamente protegido (ORGANIZAÇÃO DOS ESTADOS AMERICANOS, 2020, p. 45).

Por derradeiro, classificam-se como informação reservada, a informação que possa prejudicar a condução das negociações e relações internacionais; ponha em risco a vida, a dignidade humana, a segurança ou a saúde de qualquer pessoa e afete direitos do devido processo ou prejudique a condução dos expedientes judiciais ou dos procedimentos administrativos, até que se tornem definitivos. As informações confidenciais, por sua vez, afetam o direito à privacidade, inclusive aquela relacionada à vida, à saúde ou à segurança, bem como o direito à honra e à própria imagem; os dados pessoais e as patentes, os direitos de autor e os sigilos comerciais (ORGANIZAÇÃO DOS ESTADOS AMERICANOS, 2020, p. 49).

Em que pese estar situado na primeira dimensão dos direitos fundamentais, o direito de acesso à informações públicas, retratado pelo ideal de liberdade oriundo da Revolução Francesa, onde se exige uma postura absenteísta do Estado, pugna por medidas que viabilizem e incentivem as liberdades individuais, não bastando a não atuação estatal para sua efetividade.

Até porque, o acesso público à informação como um direito fundamental garante ao cidadão o conhecimento a respeito das receitas arrecadadas pelo Estado, as despesas previstas, prestação de serviços públicos, orçamentos, licitações e contratos, dentre tantas outras informações que repercutem no interesse da própria coletividade.

Nessa toada, pertinente a análise do Decreto nº 9.690 de 23 de janeiro de 2019 que permitia a delegação da competência de classificação das informações nos graus ultrassecretos e secretos para ocupantes de cargos em comissão, além de permitir a delegação da competência de classificação de informações no grau reservado a agentes públicos que exerciam funções de direção, comando ou chefia (BRASIL, 2019).

Em contrapartida, de autoria da Câmara dos Deputados, foi criado o Projeto de Decreto Legislativo nº 3 de 2019 cujo objetivo seria: “sustar a aplicação do Decreto nº 7.724, de 16 de maio de 2012, no que diz respeito à delegação da competência de classificação de informações públicas nos graus de sigilo ultrassecreto ou secreto” (BRASIL, 2019).

Mediante o Decreto nº 9.690/2019 buscou-se a modificação do Decreto nº 7.724/2012, que por sua vez, regulamenta a Lei de Acesso à Informação (LAI) no tocante a possibilidade de delegação da competência de classificação das informações nos graus ultrassecretos e secretos.

Entretanto, mencionado projeto foi arquivado em 27 de fevereiro do mesmo ano em decorrência da edição de novo Decreto, de nº 9.716, editado pelo governo federal que revogou parte do decreto anterior.

Pertinente também a análise da Medida Provisória nº 928 de 2020, a qual, dentre outras finalidades, suspendia: "os prazos de resposta a pedidos de acesso à informação nos órgãos ou nas entidades da administração pública cujos servidores estejam sujeitos a regime de quarentena, teletrabalho ou equivalentes e que, necessariamente, dependam de acesso presencial de agentes públicos encarregados da resposta; ou agente público ou setor prioritariamente envolvido com as medidas de enfrentamento da situação de emergência" (BRASIL. 2020).

Em face da aludida MP foram impetradas Ações Diretas de Inconstitucionalidade atinentes à mudança nas regras de solicitação de informações com fulcro na LAI.

Nesse diapasão, o Supremo Tribunal Federal suspendeu a eficácia dos dispositivos ora citados e, em 30 de abril de 2020, referendou a decisão liminar proferida pelo Ministro Alexandre de Morais, que na ocasião se pronunciou afirmando que: "as restrições instituídas por medida provisória são genéricas e abusivas e ofendem o princípio da publicidade e da transparência".

Têmis Limberger assevera que a transparência se apresenta como resultado da integração do princípio da publicidade com o direito de acesso à informação e o princípio democrático (LIMBERGER, 2016, p. 44). Assim, não há que se falar em respeito ao princípio da transparência, sem a promoção da publicidade dos atos governamentais e do direito de acesso à informação pública. Esse tripé, privilegia o Estado democrático de Direito.

Nas palavras da referida autora:

> A publicidade e a transparência são dois movimentos distintos, porém na mesma rota. A publicidade parte do conhecimento dos atos da administração para a coletividade, enquanto a transparência permite ao cidadão o acesso à informação pública. A transparência é uma composição decorrente do princípio da publicidade, do direito à informação, relacionada ao princípio democrático. É a administração agindo em conformidade com o seu dever de publicizar seus atos, o cidadão se informando dos atos praticados pela administração, tudo isto fortalece a cultura democrática (LIMBERGER, 2016, p. 45-46).

Para além disso, os princípios constitucionais administrativos outrora citados, necessitam ser assegurados também no ciberespaço. Hodiernamente, a informação pública se encontra disponibilizada em rede. Dessa maneira, a democracia e a transparência, em

particular, ganham novas identidades, denominando-se, assim, a ciberdemocracia e a cibertransparência, respectivamente.

Atesta Augustinho Paludo (2022, p. 281):

> O Governo Eletrônico não deve ser visto apenas como meio de disponibilização de serviços pela internet. O avanço das tecnologias de informação e comunicação tem possibilitado a interação entre governo e sociedade, e a disponibilização de uma vasta gama de informações eletrônicas que proporcionam mais transparência às ações dos governos.

E conclui que:

> A transparência viabilizada pela internet inclui a disponibilização de todo o tipo de informação sobre: o Governo, a Administração, a estrutura de governo e dos órgãos, o processo decisório, as políticas públicas, as contratações e compras públicas em geral, a prestação de contas dos recursos utilizados, legislação etc.
> A disponibilização da prestação de contas através da internet proporciona a transparência da gestão governamental no contexto democrático, e é uma forma de concretização do *accountability* governamental (PALUDO, 2022, p. 282).

Até porque o uso de novas tecnologias associadas à gestão governamental, inclusive com a prestação digital de serviços públicos deve assegurar o exercício dos direitos e liberdades fundamentais e, em hipótese alguma, ser utilizadas com propósitos antidemocráticos.

Portanto, o direito fundamental de acesso público à informação reflete a publicidade, a transparência, o controle social e *accountability*, isto é, reflete o grau de comprometimento do Estado com a cidadania e a democracia, pilares do Estado Democrático de Direito, devendo ser efetivados tanto no ambiente físico quanto no ambiente virtual.

2 TRATAMENTO DE DADOS PESSOAIS PELA ADMINISTRAÇÃO PÚBLICA SOB A ÉGIDE DA LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

Em sua obra *21 lições para o século 21*, Yuval Noah Harari afirma:

> Se quisermos evitar a concentração de toda a riqueza e de todo o poder nas mãos de uma pequena elite, a chave é regulamentar a propriedade dos dados (…) os dados vão suplantar tanto a terra quanto a maquinaria como o ativo mais importante, e a política será o esforço por controlar o fluxo de dados (HARARI, 2018).

Não atoa, diversas situações impactaram o cenário internacional e nacional relativas ao uso indevido de dados pessoais. No cenário internacional, o escândalo da *Cabridge*

Analytica nas eleições norte-americanas acendeu um alerta mundial acerca da fragilidade dos dados, sobretudo em razão da facilidade de coleta no ambiente digital e a possibilidade de formação de um perfil comportamental do indivíduo com base nos dados coletados, capaz de identificar, inclusive as preferências políticas de cada pessoa.

No cenário nacional, diversos foram os acontecimentos de vazamento de dados pessoais, ocasionando graves danos às vítimas, a exemplo de fraudes. No ano de 2021 foram tantos os dados pessoais vazados, que a situação em questão foi intitulada "megavazamento", onde o número de dados pessoais vazados superaram, em números, a população brasileira, ou seja, ocorreu vazamento de dados pessoais de pessoas já falecidas (G1, 2021).

Diante dessas fragilidades, países reforçaram os estudos e as pesquisas sobre o tema da proteção de dados pessoais, bem como promulgaram legislações específicas sobre o tema. Alguns países já previam também a necessidade de reconhecimento de um direito fundamental à proteção de dados pessoais. Assim, não bastava a existência de uma lei que reconhecesse um direito à proteção de dados, seria necessário o seu reconhecimento em caráter fundamental.

No Brasil, a Lei Geral de Proteção de Dados (LGPD) é a primeira lei específica sobre o tema, a qual traz requisitos específicos para o tratamento de dados pessoais, informando sobre as bases legais que justificam esse tratamento. Muito embora a Lei traga os requisitos, urge destacar que determinadas bases legais apresentam problemáticas em decorrência de seu alto grau de abstração, a exemplo do legítimo interesse, o que pode ocasionar danos aos titulares dos dados.

Ante essa perspectiva, o presente capítulo abordará o tratamento de dados pessoais pela Administração Pública sob a égide da Lei Geral de Proteção de Dados (LGPD). Para tanto, discorrer-se à, primeiramente, sobre aspectos gerais da supradita lei, a fim de introdução ao objetivo específico do capítulo. Em seguida, será abordado o tema do tratamento de dados pessoais de forma geral apresentando as bases legais que justificam seu tratamento. Por fim, explanar-se à o tratamento de dados pessoais pelo Poder Público, o qual apresenta tópico individualizado na norma ora estudada, também analisando as bases legais que justificam seu tratamento de dados.

Tudo isso com vistas a elucidar a problemática do presente trabalho no que pertine a identificação dos limites de atuação da Administração Pública com o objetivo de assegurar o

direito fundamental à proteção de dados pessoais sem prejuízo da observância dos deveres de acesso à informação, publicidade e cibertransparência.

2.1 ASPECTOS GERAIS DA LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

A Lei nº 13.709/2018, LGPD, assim como as demais normas vigentes no ordenamento jurídico brasileiro, possui estreita relação com a Constituição Federal de 1988, em razão do fenômeno da constitucionalização do direito, outrora abordado.

Os preceitos constantes na CF/88 encontram guarida na LGPD não apenas em caráter formal, mas também em caráter material, isto é, não bastam sua mera positivação ou reprodução nos textos legais, é imperativo que hajam mecanismos que efetivem os direitos tutelados.

Nas disposições preliminares informa a respeito da sua aplicabilidade e inaplicabilidade, seus fundamentos e definições importantes como as referentes a dado pessoal, dado pessoal sensível, dado anonimizado, controlador, operador e encarregado, dentre outros. Informa também sobre os princípios a serem observados no tratamento de dados pessoais, tais como a necessidade, a finalidade e a não discriminação.

Possui um capítulo destinado ao tratamento de dados pessoais, subdividido em requisitos para o tratamento de dados pessoais e para o tratamento de dados pessoais sensíveis; outro capítulo para o tratamento em relação a crianças e adolescentes; do término do tratamento de dados; apresenta os direitos do titular; regras para o tratamento de dados pessoais pelo poder público; da responsabilização em caso de violações aos seus preceitos; transferência internacional de dados; agentes de tratamento; da segurança e boas práticas; da fiscalização; o papel da Autoridade Nacional de Proteção de Dados (ANPD) e, por fim, apresenta as disposições finais e transitórias.

Logo em seu art. 1º, a lei informa que sua observância aplica-se, “inclusive nos meios digitais”, reforçando a ideia de que o tratamento de dados pessoais deve ser assegurado tanto no ambiente físico quanto no ambiente virtual.

Assim, aqueles que armazenam dados pessoais em cadernetas, agendas, papéis impressos, de modo geral, devem se submeter a referida lei, bem como aqueles que coletam e armazenam dados pessoais no ciberespaço, a exemplo das lojas *online* de vendas.

Destarte, possui como objetivo a proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, conforme se extrai do art. 1º.

Por conseguinte, os fundamentos da proteção de dados pessoais previstos no art. 2º são os seguintes: o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Nota-se que os fundamentos apresentados relacionam-se com as normas constitucionais. Dentre eles, o único fundamento que não está expressamente previsto na CF/88 é a autodeterminação informativa que, conforme já explanado, trata-se de uma construção jurisprudencial do Tribunal Constitucional alemão, reconhecido pelo Supremo Tribunal Federal (STF) na decisão referente a MP nº 954/2020.

A partir de então, com a vigência da LGPD, norma geral específica de tutela da proteção de dados no país, começa a ser delineado um caminho de busca pela adequação à norma pelos regulados.

Com tal objetivo o STF editou a Resolução nº 724, de 02 de março de 2021, instituindo um Comitê com competência para identificação e implementação das medidas necessárias para consecução desses objetivos (BRASIL, 2021).

Dentre as competências do Comitê Executivo de Proteção de Dados, previstas no art. 3º, identificam-se a formulação de princípios e diretrizes para a gestão de dados pessoais, bem como a proposição de sua regulamentação (II); a prestação de orientações sobre o tratamento e a proteção de dados de acordo com a LGPD (IV); realização de eventos, organização de cursos e apresentação de estudos para capacitação e orientação de Ministros, servidores, colaboradores, terceirizados e estagiários do órgão (VI).

A Autoridade Nacional de Proteção de Dados (ANPD), emitiu, no mês de maio de 2021, um *Guia Orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado*. Neste documento o que se busca é:

> Estabelecer diretrizes não vinculantes aos agentes de tratamento e explicar quem pode exercer a função do controlador, do operador e do encarregado; as definições

> legais; os respectivos regimes de responsabilidade; casos concretos que exemplificam as explicações da ANPD e as perguntas frequentes sobre o assunto (BRASIL, 2021).

Trata-se do primeiro documento emitido pelo órgão desde sua previsão na LGPD em meio a discussões quanto a mudança em sua estruturação, atualmente vinculada à Casa Civil da Presidência da República.

Ademais, o documento possibilita o envio de sugestões e contribuições pela sociedade civil através de um endereço de e-mail[11] como forma de viabilizar a participação social fortalecendo, assim, a ideia de voluntariedade e de constante diálogo entre regulador e regulados visando conformidade à LGPD.

Destarte, não se pode perder de vista que a LGPD busca a atuação dinâmica dos agentes envolvidos na consecução de suas finalidades, pautando-se na cooperação mútua, na voluntariedade dos regulados para o atingimento desses fins, com a promoção de medidas flexíveis que possibilitam ao regulado propor seus princípios, diretrizes, sua própria política interna, numa espécie de mudança de cultura organizacional, sem retirar, contudo, o caráter sancionador da ANPD.

2.2 DO TRATAMENTO DE DADOS PESSOAIS

O tratamento de dados pessoais encontra previsão na LGPD e constitui importante instrumento para a promoção de uma mudança na cultura organizacional. Para tanto, a lei prevê bases legais para o tratamento de dados pessoais que, por sua vez, abrange o ciclo de vida de dado pessoal, da coleta ao descarte, possuindo, ainda, caráter extrapatrimonial. Importa ressaltar a ausência de hierarquia entre as bases legais (FONSECA, 2021, p. 83-84).

Em seu art. 3º, a LGPD pontua que, tanto a pessoa natural quanto a pessoa jurídica, devem observar as respectivas normas para o tratamento de dados, desde que, observadas as seguintes hipóteses: (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 (BRASIL, 2018).

Nota-se que a lei reforça, a priori, o caráter territorial da aplicabilidade da lei, isto é, a lei se aplica ao tratamento de dados pessoais realizados no Brasil.

11 E-mail: normatizacao@anpd.gov.br.

O art. 4º, por seu turno, exemplifica as hipóteses de não incidência da LGPD. Senão Vejamos:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
> II - realizado para fins exclusivamente:
> a) jornalístico e artísticos; ou
>
> b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
>
> III - realizado para fins exclusivos de:
>
> a) segurança pública;
>
> b) defesa nacional;
>
> c) segurança do Estado; ou
>
> d) atividades de investigação e repressão de infrações penais; ou
>
> IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei (BRASIL, 2018).

Na realização do tratamento de dados pessoais, destacam-se três figuras importantes. A primeira é o controlador de dados pessoais, representado por pessoa natural ou jurídica, de direito público ou privado, com poder decisório referente ao tratamento de dados pessoais. O operador, que também pode ser pessoa natural ou jurídica, de direito público ou privado, é quem realiza o tratamento de dados pessoais em nome do controlador. A figura do encarregado apresente grande relevância, pois, é a pessoa indicada pelo controlador e pelo operador com vistas a atuar como interlocutor entre o controlador, os titulares de dados pessoais e a ANPD, conforme se extra do art. 5º, incisos VI, VII e VIII, respectivamente, da lei ora tratada (BRASIL, 2018).

O capítulo II, situado a partir do art. 7º, traz regras específicas para o tratamento de dados pessoais, representando as bases legais. A primeira base legal, ou seja, a primeira hipótese na qual se permite a realização do tratamento de dados pessoais é o consentimento. Importa destacar que o consentimento deve referir-se a finalidades determinadas e autorizações genéricas, adverte a lei em seu art. 8º,§ 4º, serão consideradas nulas (BRASIL, 2018).

Outra base legal é a necessidade de tratamento de dados pessoais com o fim de cumprimento de obrigação legal ou regulatória pelo controlador. Nessa hipótese, a exigência

deriva de um instrumento normativo ou regulatório e não de uma situação específica. Assim, quando a lei ou um regulamento exigir, realiza-se o tratamento de dados pessoais, independentemente do consentimento de seu titular (BRASIL, 2018).

A Administração Pública também realiza tratamento de dados pessoais e, desde que, atenda ao interesse público, mediante a execução de políticas públicas, não necessita do consentimento do titular dos dados (BRASIL, 2018).

Em estudos realizados por órgão de pesquisa, dispensa-se o consentimento do titular dos dados, primando-se, sempre que possível, pela anonimização[12] dos dados pessoais. Edson Pires da Fonseca (2021, p. 89) aduz que: "órgãos de pesquisa vinculados a pessoas jurídicas de direito privado com finalidade de lucro não poderão utilizar esta base legal para fundamentar o tratamento de dados pessoais". Nesses casos, exige-se o consentimento do titular, a primeira base legal tratada.

Para além disso, também constitui justificativa legal para o tratamento de dados pessoais, a execução de contratos. Frisa-se que o Direito Contratual, estatuído no Código Civil de 2002 nos arts. 421 ao 853, pugna pela liberdade contratual, bem como pelo princípio da intervenção mínima e pela excepcionalidade da revisão contratual. Nessa toada, os dados necessários e pertinentes ao desenvolvimento da relação contratual submetem-se a LGPD.

Destarte, o exercício regular de direito, reveste-se de importante base legal na promoção do devido processo legal e do contraditório e ampla defesa, princípios assegurados na Constituição Federal de 1988 e, necessários ao regular desenvolvimento em processo judicial, administrativo ou arbitral.

De outra banda, o inciso VII do art. 7º, tutela o tratamento de dados com vistas a proteção da vida e da incolumidade física do titular ou de terceiro. Trata-se de escusa de consentimento apto a assegurar um dos valores mais sensíveis do ser humano, o direito à vida (BRASIL, 2018).

A par disso, Fonseca (2021, p. 92) esclarece: "o GDPR, que serviu de base para a elaboração da LGPD, aclara em seu Considerando nº 46 situações nas quais esta base legal pode ser utilizada, destacando-se fins humanitários, incluindo a monitorização de epidemias e da sua propagação ou em situações de emergência humanitária, em especial em situações de catástrofes naturais e de origem humana[13]".

12 Segundo o art. 5º, inciso I da LGPD dado anonimizado é o "dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento".
13 GDPR, Considerando nº 46: "O tratamento de dados pessoais também deverá ser considerado lícito quando for necessário à proteção de um interesse essencial à vida do titular dos dados ou de qualquer outra pessoa

No mesmo sentido da proteção aos valores mais sensíveis do ser humano, apresenta-se a base legal relativa ao direito à saúde. A lei informa que para a utilização dessa base legal, é imperativo que o tratamento de dados pessoais seja desempenhado "exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária" (BRASIL, 2018). Pertine informar que os dados utilizados em procedimentos relativos ao direito à saúde correspondem a dados pessoais sensíveis[14], o que demanda maior cautela no seu tratamento.

A penúltima base legal para o tratamento de dados pessoais da LGPD é o legítimo interesse do controlador ou de terceiro, salvo nos casos de prevalência de direitos e liberdades fundamentais do titular (BRASIL, 2018). Tal base legal sofre severas críticas de autores em razão do seu alto grau de abstração sobre o que vem a ser o legítimo interesse. A LGPD não traz essa definição.

Assevera FONSECA (2021, p. 93): "o legítimo interesse é uma das bases legais mais polêmicas e deve ser utilizada com cautela para que não haja abusos ou justificativas elásticas, o que pode colocar o controlador em elevado risco jurídico".

Espera-se que a ANPD, no uso de sua atribuição regulamentadora, esclareça determinadas condutas aptas a resguardar a atuação do controlador de dados pessoais, sem prejuízo do respeito aos direitos do titular, sobretudo trazendo exemplos concretos no que pertine ao legítimo interesse do controlador, sob pena de se permitir o arbítrio na sua apuração, seja na esfera administrativa, seja na esfera judicial. Importa destacar que o legítimo interesse coaduna-se com os princípios da LGPD, em especial o princípio da boa-fé.

A última base legal é a proteção ao crédito (BRASIL, 2018). Possui estreita ligação com o Código de Defesa do Consumidor, o qual busca assegurar os direitos dos consumidores ante a compreensão de sua vulnerabilidade frente aos fornecedores/produtores. A importância desse inciso reporta ao tópico 2.1 outrora tratado sobre a estrutura normativa da proteção de

singular. Em princípio, o tratamento de dados pessoais com base no interesse vital de outra pessoa singular só pode ter lugar quando o tratamento não se puder basear manifestamente noutro fundamento jurídico. Alguns tipos de tratamento podem servir tanto importantes interesses públicos como interesses vitais do titular dos dados, por exemplo, se o tratamento for necessário para fins humanitários, incluindo a monitorização de epidemias e da sua propagação ou em situações de emergência humanitária, em especial em situações de catástrofes naturais e de origem humana".

14 De acordo com o art. 5º, incido II, dado pessoal sensível é: "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

dados pessoais no ordenamento jurídico brasileiro, no qual se expôs a relação entre o CDC, a Lei do Cadastro Positivo e a LGPD.

A LGPD ainda traz a hipótese de dispensa de consentimento do titular quando os dados forem manifestamente públicos, no art. 7º, § 4º (BRASIL, 2018).

Analisadas as hipóteses que justificam o tratamento de dados pessoais, passa-se a um breve estudo a respeito do tratamento de dados pessoais sensíveis e de crianças e adolescentes.

O art. 11 dispõe sobre o tratamento de dados pessoais sensíveis, cujos requisitos encontram-se a seguir expostos:

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
>
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
>
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
>
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
>
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
>
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (BRASIL, 2018).

Os requisitos ora expostos são similares aos requisitos genéricos no que pertine ao tratamento de dados pessoais. No entanto, o modo pelo qual se realizará o tratamento será diferenciado, isto é, deverá ser observado o tipo de dado coletado e, sendo dado sensível, os mecanismos de supervisão devem ser mais robustos – não necessariamente complexos – em relação ao tratamento de dados que não se enquadrem em tal tipo.

Conforme outrora relatado dado pessoal sensível corresponde ao “dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a

organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (BRASIL, 2018). É o que consta no art. 5º, inciso II da LGPD.

Os dados pessoais sensíveis demandam maior cautela no seu tratamento também em razão da possibilidade de sua utilização com finalidade discriminatória. Em um processo de seleção para contratação de empregados em uma determinada empresa, por exemplo, a coleta de dados pessoais sensíveis, como dado referente a origem racial ou étnica, pode servir de parâmetro para a não contratação de determinados candidatos com base na raça e origem do indivíduo, e não com base nas qualificações profissionais, como se espera.

Ademais, o art. 11, § 3º, contém disposição polêmica ao permitir o uso compartilhado de dados pessoais sensíveis, bem como sua comunicação entre controladores "com o objetivo de obter vantagem econômica". Informa ainda que tal situação poderá ser regulamentada ou até mesmo vedada pela Autoridade Nacional de Proteção de Dados (BRASIL, 2018).

Assim, a LGPD permite a comercialização de dados pessoais sensíveis entre os controladores e, até o presente momento, não há regulamentação pela ANPD sobre o tema.

Ainda referente ao tratamento de dados pessoais sensíveis, a LGPD não consagrou o legítimo interesse como base legal apta a justificar o tratamento para esse tipo de dado pessoal.

Importante dispositivo é a previsão do art. 13, § 4º sobre a pseudonimização, que consiste no "tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro" (BRASIL, 2018).

A pseudonimização é medida recomendada na realização de estudos em saúde pública, bem como a medida de anonimização de dados pessoais. A diferença entre ambas é o caráter da reversibilidade. Na anonimização não é possível sua reversibilidade, ou seja, não é possível identificar seu titular. Também não se considera dado pessoal o dado anonimizado. Por sua vez, a pseudonimização permite a identificação do titular dos dados. Exemplo clássico é a utilização de dois bancos de dados, um contendo informações dos titulares sem a identificação direta da sua condição de saúde e outro banco de dados contendo apenas os dados referentes a tal situação. A possibilidade de reversão dessa situação se dá mediante o cruzamento dos dados utilizados no banco de dados 01 com o banco de dados 02, o qual

apenas profissional previamente designado terá acesso. A utilização de códigos facilita o cruzamento e identificação dos dados de pacientes.

No que pertine ao tratamento de dados pessoais de crianças e adolescentes importa mencionar que a LGPD, tal qual o Estatuto da Criança e do Adolescente (ECA) pugnam pelo princípio da proteção integral do menor e do seu melhor interesse.

O §1º do art. 14 informa que para o tratamento de dados de menores deve-se obter o consentimento específico e em destaque de um dos pais, ao menos, ou de seu responsável legal. Embora o titular dos dados pessoais seja a criança e/ou adolescente, o consentimento por eles concedido é considerado nulo, haja vista o disposto no Código Civil de 2002 quanto a capacidade de direito (BRASIL, 2018).

E seu art. 3º, o Código Civil considera absolutamente incapazes, os menores de 16 (dezesseis) anos. O art. 4º, inciso I, considera os maiores de 16 (dezesseis) anos e menores de 18 (dezoito) anos relativamente incapazes. Tanto crianças quanto adolescentes não são consideradas plenamente capazes para o exercício dos atos da vida civil, tal qual a concessão de consentimento (BRASIL, 2018).

Nessa toada, em regra, os pais ou responsáveis legais respondem pelos atos dos menores, sendo possível, a concessão de consentimento para o tratamento de dados pessoais dos menores por estes.

Por conseguinte, a LGPD ainda traz a possibilidade de coleta de dados pessoais de crianças e adolescentes sem o consentimento de seus pais ou responsável legal "quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento" de, ao menos, um dos pais, ou do representante legal, conforme disposto no § 3º do art. 14 (BRASIL, 2018).

O art. 15 aborda as hipóteses de término do tratamento de dados pessoais, quais sejam: (i) verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; (ii) fim do período de tratamento; (iii) comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou (iv) determinação da autoridade nacional, quando houver violação ao disposto nesta Lei (BRASIL, 2018).

Denota-se a relevância de tal dispositivo ante a compreensão de que o tratamento de dados pessoais segue um ciclo, o ciclo de vida dos dados. A própria definição de tratamento insculpida logo no art. 5º, inciso X da referida norma, aponta, com certa abrangência, situações que perpassam o tratamento de dados. Nesse sentido, tratamento é "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (BRASIL, 2018).

Após o término do tratamento de dados ocorre a etapa da eliminação, salvo nas seguintes hipóteses previstas no art. 16: (i) cumprimento de obrigação legal ou regulatória pelo controlado; (ii) estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; (iii) transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou (iv) uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados (BRASIL, 2018).

De outra banda, importante elucidar as questões relativas a responsabilização nos casos de descumprimento da LGPD, estatuídos nos arts. 42 a 45.

Inicialmente a lei traz a responsabilidade do controlador e do operador de dados para a reparação do dano ocasionado ao titular dos dados, assim como prevê as hipóteses de responsabilidade solidária, sem prejuízo da possibilidade de reconhecimento de excludente da responsabilidade.

Assim:

> O operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei (BRASIL, 2018).

Já "os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei" (BRASIL, 2018). Conforme assegurado nos incisos I e II, respectivamente, do § 1º do art. 42 da LGPD.

A responsabilidade defendida por autores é a responsabilidade subjetiva. Desse modo, autores defendem que o controlador e o operador de dados somente responderão quando for comprovado dolo ou culpa no exercício de suas atribuições.

Por seu turno, o art. 43 aduz pela escusa de responsabilização pelos agentes de tratamento de dados (controlador e operador) (BRASIL, 2018). Nota-se que a lei não discorre sobre a responsabilidade do encarregado de proteção de dados. O que não significa que esse profissional não deverá seguir os preceitos da LGPD.

Pensar de modo diverso iria de encontro ao que propõe a norma. A mudança na cultura organizacional exige uma postura proativa e não só reativa, dos multi *stakeholders*, devendo, cada parte interessada no regular desenvolvimento da Organização, assumir responsabilidade no cumprimento da respectiva lei, não sendo tarefa exclusiva dos agentes de tratamento.

São três hipóteses de escusa de responsabilidade dos agentes de tratamento e todas dependem de prova. A primeira é a comprovação de não realização do tratamento de dados que lhes foi atribuído; a segunda, é a comprovação de ausência de violação à legislação de dados em que pese a confirmação da realização do tratamento. A terceira e última exige a comprovação de que o dano se deu, exclusivamente, por culpa do titular dos dados ou de terceiro (BRASIL, 2018).

Outrossim, o art. 44 aborda a irregularidade no tratamento de dados pessoais e as circunstâncias que a caracterizam. De tal modo, a inobservância da legislação e o não fornecimento da segurança esperada pelo titular dos dados, constituem irregularidade no tratamento de dados. A aferição levará em consta: (i) o modo pelo qual o tratamento é realizado; (ii) o resultado e os riscos que razoavelmente dele se esperam e; (iii) as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado (BRASIL, 2018).

Essas situações demonstram a necessidade de análise do caso concreto. Não existe uma fórmula exata para aferir o grau de comprometimento de cada Organização na cultura do tratamento de dados pessoais, sendo imprescindível a análise a partir da situação concreta. Tarefa complexa não só para a Autoridade Nacional de Proteção de Dados (ANPD) como para o Poder Judiciário, que não pode se imiscuir da apreciação jurisdicional.

Por fim, destacam-se as sanções de caráter administrativo, aplicáveis pela Autoridade Nacional de Proteção de Dados (ANPD), insculpidas no art. 52. Vejamos:

> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - 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;

> III - multa diária, observado o limite total a que se refere o inciso II;
>
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
>
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
>
> VI - eliminação dos dados pessoais a que se refere a infração;
>
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
>
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
>
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados (BRASIL, 2018).

Conforme já relatado, as sanções são de natureza administrativa e serão aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD), observando-se a gradação prevista na lei. A sanção mais branda consiste na aplicação de uma advertência, a sanção mais severa consiste na proibição parcial ou total de tratamento de dados pessoais pelo infrator.

A priori, a Autoridade Nacional de Proteção de Dados (ANPD) evitará a aplicação de sanções, haja vista a recente promulgação da lei de proteção de dados pessoais no Brasil e o fato de ser a primeira legislação específica protetiva sobre o tema.

Assim, as sanções administrativas serão aplicadas em *ultima ratio* e a Autoridade Nacional primará, num primeiro momento, pelo caráter educativo, elucidativo, da lei, como se nota pela publicação de seus Guias Orientativos, ou seja, desprovido de caráter vinculante.

2.3 DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

A Lei Geral de Proteção de Dados (LGPD) destina um capítulo para dispor sobre o tratamento de dados pessoais pelo Poder Público, o capítulo IV, especificamente do art. 23 ao art. 30.

Logo em seu art. 23 apresenta as hipóteses que justificam o tratamento de dados pessoais pelas pessoas jurídicas de direito público. As hipóteses são as seguintes: atendimento da finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público (BRASIL, 2018).

Ainda assim, deverão ser observados determinados requisitos, senão vejamos: “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" bem como "seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais" (BRASIL, 2018).

Dessa forma, verifica-se a necessidade de respeito aos princípios insculpidos na LGPD, sobretudo o princípio da finalidade[15] (art. 6º, I) e o princípio da transparência[16] (art. 6º, VI). Nota-se também a necessidade da designação de um encarregado no tratamento de dados pessoais. O encarregado é a "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)" (BRASIL, 2018). Portanto, a figura do encarregado atua como um mediador (facilitador) entre as partes interessadas, não sendo considerado um agente de tratamento nos termos da lei ora tratada.

Destaca-se que às empresas públicas e as sociedades de economia mista atuantes em regime concorrencial aplicam-se o mesmo tratamento previsto para as pessoas jurídicas de direito privado particulares. Em suma, não são enquadradas no capítulo IV, no tratamento de dados pessoais pelo Poder Público. É o que se extrai do seu art. 24[17] (BRASIL, 2018).

De outra banda, caso as empresas estatais atuem na prestação de serviços públicos, receberão o tratamento previsto para a esfera pública[18] (BRASIL, 2018).

Importante mencionar que a LGPD impõe que os dados pessoais sejam mantidos em formato interoperável e estruturado a fim de possibilitar seu compartilhamento, conforme seu art. 25 (BRASIL, 2018). Tal imposição decorre da leitura do próprio dispositivo que, em vez de utilizar a expressão "poderão" optou pela expressão "deverão", traduzindo a ideia de dever, com força cogente. Assim é imperativo que no tratamento de dados pessoais, o Estado utilize formato interoperável, ou seja, com possibilidade de comunicabilidade entre sistemas,

15 Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I – finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

16 Art. 6º (…) VI – transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

17 Art. 24. As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.

18 Art. 24 (…) Parágrafo único. As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos deste Capítulo.

permitindo o fluxo de dados de um sistema de um determinado órgão público para outro (Receita Federal e INSS, por exemplo). Além disso, os dados pessoais deverão permanecer estruturados, organizados no sistema.

No que pertine a interoperabilidade, esta consiste, em suma, na "capacidade de dois sistemas se interconectarem, de trocarem informações entre si" (FONSECA, 2021, p. 126). Ainda segundo Fonseca (2021, p. 127), a interoperabilidade dos sistemas possui a característica de reforçar a segurança dos dados, concedendo maior eficiência e segurança ao tratamento de dados pessoais realizados pela Administração Pública.

Ademais, os dados só poderão ser compartilhados "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).

Para além disso "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).

Em que pese a possibilidade de compartilhamento de dados pessoais entre entidades públicas, a LGPD ressalva a possibilidade de compartilhamento desses dados com pessoas jurídicas de direito privado. Trata-se de hipóteses excepcionais, a regra é a vedação de compartilhamento de dados pessoais de entidades públicas para entidades privadas. As exceções (possibilidades) estão descritas no art. 26, §1º, *in verbis*:

> 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.
>
> § 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:
>
> I – em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);
>
> II – (VETADO);
>
> III – nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.
>
> IV – quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou

> V – na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades (BRASIL, 2018).

Da leitura do dispositivo supra, depreende-se que o compartilhamento de dados pessoais das entidades públicas para as entidades privadas têm por escopo resguardar o interesse público e o dever fundamental de acesso à informação, bem como os deveres de publicidade e transparência, com a devida garantia dos direitos do titular desses dados.

A respeito do tema informa Têmis Limberger (2016, p. 44) que: "a transparência demonstra ser uma integração do princípio da publicidade conjugado com o direito à informação (art. 5º, XXXIII) e o princípio democrático.

Na perspectiva da atuação do Poder Público não se pode perder de vista a correlação entre tais deveres. É dizer, a atuação da Administração Pública é subsidiada e efetivada através da garantia do acesso à informação, da publicidade e da transparência como meios, inclusive, para a promoção do controle social e do combate a corrupção.

O principal desafio talvez seja o de conjugar os deveres supramencionados com o dever de proteção de dados pessoais.

Por outro lado, a criação de uma Autoridade administrativa para a proteção de dados pessoais, nos moldes de uma autoridade independente, não deve ser desconsiderada. Para tanto, destaque para a Autoridade Nacional de Proteção de Dados (ANPD) cuja criação reforça a importância de uma cultura na proteção de dados pessoais, haja vista que

> Alguns dos aspectos mais relevantes da proteção de dados pessoais, como o fato de que os tratamentos de dados e os seus efeitos são dificilmente passíveis de serem acompanhados de forma eficaz pelo cidadão ou a necessidade de uma constante atualização em função do desenvolvimento tecnológico, entre vários outros, justificaram o recurso a esses órgãos que, hoje, estão presentes na grande maioria dos marcos regulatórios nessa matéria, quase sempre como um de seus sustentáculos (DONEDA, 2020).

Nessa conjectura, a Autoridade Nacional de Proteção de Dados (ANPD) publicou um *Guia Orientativo sobre tratamento de dados pessoais pelo Poder Público*, em sua versão 1.0 no mês de janeiro do ano de 2022.

Destaca-se do referido documento os cuidados a serem observados quando da divulgação de dados pessoais pelo Poder Público.

Tabela 1 – Cuidados a serem observados quando da divulgação de dados pessoais pelo Poder Público

Parâmetro	Recomendação
A coleta do dado pessoal é necessária e adequada para a finalidade do tratamento?	• Verificar a possibilidade de dispensa da coleta ou de eliminação dos dados pessoais, tendo em vista a sua efetiva necessidade para o alcance das finalidades do tratamento; • Verificar se há formas de atingir a finalidade almejada sem o tratamento de dados pessoais e de maneira menos gravosa para o titular de dados.
A divulgação envolve dados pessoais sensíveis?	• Em caso afirmativo, o tratamento deve ser efetuado com maior cautela, observando-se normas específicas, como os dispositivos da LGPD relativos a estudos em saúde pública.
Quais medidas de mitigação de risco para o titular de dados podem ser adotadas?	• Elaboração de relatório de impacto à proteção de dados pessoais, caso necessário; • Medidas de prevenção e segurança, a exemplo de anonimização ou pseudonimização dos dados pessoais sempre que isso não comprometa o exercício do controle social; • Limitação da divulgação àqueles dados necessários para alcançar a finalidade pretendida, observados o contexto, a finalidade e as expectativas legítimas dos titulares; • Transparência do tratamento; e • Garantia de direitos dos titulares.

Fonte: ANPD, 2022

Compete esclarecer que os guias emitidos pela Autoridade Nacional de Proteção de Dados (ANPD) não possuem caráter cogente, impositivo, vinculante, tal qual se infere do próprio nome (orientativo). Trata-se de documento elaborado com vistas a melhor delinear aspectos constantes na Lei Geral de Proteção de Dados (LGPD).

Até porque a LGPD se traduz em uma lei principiológica, ou seja, ela abarca princípios, definições, direitos, tudo isso de modo abstrato, mais amplo. A ideia de uma lei

protetiva sobre proteção de dados pessoais perpassa o caráter puramente normativo, ela impulsiona cada ente regulado a buscar seus próprios meios para a efetiva implementação, pugnando por uma mudança na cultura organizacional.

3 MECANISMOS ASSECURATÓRIOS DA PROTEÇÃO DE DADOS PESSOAIS NA ADMINISTRAÇÃO PÚBLICA 4.0

No presente capítulo serão abordados os mecanismos assecuratórios da proteção de dados pessoais na Administração Pública 4.0 a partir da compreensibilidade de que é plenamente possível a garantia do direito de acesso público à informação em rede, da publicidade e da cibertransparência, sem prejuízo da garantia de proteção aos dados pessoais.

Então, defende-se a necessidade de adoção de uma política de Governança dentro das instituições públicas, bem como a adoção de uma política de Governança de Dados, boas práticas e *compliance,* com base nos documentos disponíveis em rede que facilitam sua implementação, a exemplo da ISO 27.001 sobre segurança da informação e os guias orientativos da ANPD, para além dos dispositivos jurídico-normativos.

Outrossim, o presente trabalho apresenta algumas técnicas que podem e são utilizadas por algumas instituições privadas e públicas na difusão de uma cultura de autorresponsabilidade, que auxiliam na adoção da Governança e nos demais mecanismos acima destacados.

Para tanto, destaca-se o papel da Governança enquanto um instrumento passível para assegurar os deveres da Administração Pública ante os novos desafios que se apresentam na hodierna Revolução Digital.

Desta forma, importante elucidar os conceitos de governabilidade e de governança apresentados por José Matias Pereira em sua obra *Curso de Administração Pública: Foco nas Instituições e Ações Governamentais*. Predito autor estabelece: “enquanto a governabilidade diz respeito às condições do exercício da autoridade política, a governança qualifica o modo de uso dessa autoridade. A capacidade de governança implica a capacidade governamental de criar e assegurar o *enforcement* de regras universalistas nas transações sociais, políticas sociais e econômicas” (PEREIRA, 2014, p. 84).

Assim, a governabilidade se refere a capacidade política e a governança se traduz em um instrumento para a governabilidade, isto é, a governança serve para efetivar as ações governamentais.

Explicita Augustinho Paludo (2022, p. 223) que a Governabilidade relaciona-se ao poder para governar em razão da legitimidade democrática e do apoio da sociedade civil. Por sua vez, a Governança relaciona-se a capacidade de implementar políticas públicas.

Por seu turno, a Governança Pública pode ser compreendida como:

> A capacidade de governar, capacidade de decidir e implementar políticas públicas que atendam às necessidades da população, preservando o equilíbrio de poder e interesses entre governo, administração pública e sociedade/cidadãos.
> A Governança Pública exige que os governos disponibilizem canais adequados e suficientes, e incentivem a participação da sociedade na formulação, implementação e controle dos serviços e políticas públicas (PALUDO, 2022, p. 230).

Aliada ao *New Public Management,* a Governança Eletrônica/Digital, evidencia-se enquanto um dos frutos da Revolução 4.0 ora abordada.

Na visão de Paludo (2022, p. 233), a Governança Eletrônica/Digital: "refere-se à capacidade dos governos utilizarem as tecnologias de informação e comunicação para – com a participação dos cidadãos – definir e implementar políticas públicas com mais eficiência e efetividade. Pode ser vista como uma evolução do Governo Eletrônico, focando maior participação dos cidadãos no meio público".

No *Guia de Boas Práticas da LGPD para implementação na Administração Pública Federal* emitido pela ANPD, em 2020, recomenda-se a adoção de "um conjunto de documentos para melhorar o gerenciamento de riscos de segurança cibernética. Um *framework*, por exemplo, apresenta condutas e recomendações para que sejam aplicados princípios e práticas recomendadas de gerenciamento de riscos para melhorar a segurança e a resiliência" (BRASIL, 2020).

Referido Guia apresenta ainda um conjunto de padrões de interoperabilidade de Governo Eletrônico, o E-Ping, que:

> Define um conjunto mínimo de premissas, políticas e especificações técnicas que regulamentam a utilização da Tecnologia de Informação e Comunicação (TIC) na interoperabilidade de serviços de Governo Eletrônico, estabelecendo as condições de interação com os demais Poderes e esferas de governo e com a sociedade em geral. As áreas cobertas pela ePING estão segmentadas em: • Interconexão; • Segurança; • Meios de Acesso; • Organização e Intercâmbio de Informações; • Áreas de Integração para Governo Eletrônico (BRASIL, 2020).

Por esse ângulo, nota-se que o tema da Governança apresenta diversos e importantes nichos. Contudo, o presente trabalho enfatizará o papel da Governança, em linhas gerais, e o da Governança de Dados, em especial no ambiente virtual, atraindo, então, a Governança Eletrônica/Digital.

Nesse sentido, evidencia-se o papel da Governança e o nicho específico da Governança de Dados, para o atendimento da proteção de dados pessoais e demais deveres do Poder Público, em razão do impacto desses aparatos em toda a estrutura organizacional, a curto e longo prazo.

Seguidamente, aponta-se o papel da segurança, das boas práticas e do *compliance*, ilustrando os dispositivos estatuídos na Lei Geral de Proteção de Dados (LGPD) a respeito do tema, bem como sua importância não só para efetivação dos deveres administrativos, mas também para o monitoramento das ações governamentais na consecução das suas finalidades públicas.

Por fim, salienta-se sobre os dados abertos e os dados pessoais na perspectiva de integração da cibertransparência pública e do direito fundamental à proteção de dados pessoais, partindo-se de um pressuposto que os dados abertos não constituem dados pessoais e, logo, o tratamento será diferenciado entre ambas as situações.

3.1 O PAPEL DA GOVERNANÇA E DA GOVERNANÇA DE DADOS

Para que haja um efetivo tratamento de dados pessoais pelo Poder Público é necessário que exista um efetivo comprometimento com vistas a uma mudança na cultura organizacional. A tarefa não é simples, exige-se uma postura proativa, direcionamento do gestor, assunção de responsabilidades pelos servidores e determinadas mudanças são perceptíveis apenas a longo prazo.

Nesse sentido, com o intuito de viabilizar o regular desenvolvimento da atividade nas Organizações, surgem a Governança, a Governança de dados, as boas práticas e o *compliance*. Em que pese tais mecanismos se encontrarem preponderantemente no setor privado, é cediço que as bases que as constituem podem e devem ser aplicadas e adaptadas ao setor público.

Com o objetivo de melhor elucidar questões relativas ao tema da Governança, o Instituto Brasileiro de Governança Corporativa (IBGC) lançou um *Código das melhores*

práticas de Governança Corporativa. Segundo referido documento Governança Corporativa pode ser definida como um:

> (…) sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas.
>
> As boas práticas de governança corporativa convertem princípios básicos em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor econômico de longo prazo da organização, facilitando seu acesso a recursos e contribuindo para a qualidade da gestão da organização, sua longevidade e o bem comum (INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA, 2015, p. 20).

Depreende-se que o papel primordial da Governança é o de impactar a cultura de cada organização. O termo Organização é expresso em sua forma mais abrangente, ou seja, entidades privadas, entidades públicas, órgãos do governo, associações e empresas são sujeitos ativos na implementação de uma Política de Governança.

Ainda nesse sentido, cumpre citar os princípios que regem a Governança. São eles: transparência, equidade, prestação de contas (*accountability)* e responsabilidade corporativa (INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA, 2015, p. 20-21).

Dos princípios então citados, nota-se sua intrínseca relação com os deveres da Administração Pública no exercício de suas atribuições, sobretudo o princípio da transparência e da prestação de contas (*accountability).*

No que pertine ao tema da Governança voltada aos interesses da coletividade, ao bem-estar social, destaca-se a Governança Pública. Colaciona-se o conceito trazido pelo *Guia da Política de Governança Pública* elaborado pela Casa Civil da Presidência da República em 2018.

Aduz referido documento que: “assim, de forma mais objetiva, na condução da política de governança considera-se que governança pública compreende tudo o que uma instituição pública faz para assegurar que sua ação esteja direcionada para objetivos alinhados aos interesses da sociedade” (CASA CIVIL DA PRESIDÊNCIA DA REPÚBLICA, 2018, p. 16).

A despeito disso, o Tribunal de Contas da União (TCU) também dispôs sobre o tema, com a publicação do *Referencial básico de Governança aplicável a órgãos e entidades da*

Administração Pública, especificando inclusive, normas internacionais em relação a supradita temática. Vejamos:

> A governança de órgãos e entidades da administração pública envolve três funções básicas, alinhadas às tarefas sugeridas pela ISO/IEC 38500:2008:
> a) avaliar o ambiente, os cenários, o desempenho e os resultados atuais e futuros;
> b) direcionar e orientar a preparação, a articulação e a coordenação de políticas e planos, alinhando as funções organizacionais às necessidades das partes interessadas (usuários dos serviços, cidadãos e sociedade em geral) e assegurando o alcance dos objetivos estabelecidos; e
> c) monitorar os resultados, o desempenho e o cumprimento de políticas e planos, confrontando-os com as metas estabelecidas e as expectativas das partes interessadas (BRASIL, 2014, p. 30).

Para além disso, o sistema normativo nacional conta com o Decreto nº 9.203, de 22 de novembro de 2017 que: "dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional" (BRASIL, 2017). Logo em seu art. 2º, inciso I, o Decreto define o conceito de Governança Pública como sendo o: "conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade" (BRASIL, 2017).

Informa o art. 3º sobre os princípios que direcionam a Governança Pública, a saber: capacidade de resposta, integridade, confiabilidade, melhoria regulatória, prestação de contas e responsabilidade e transparência (BRASIL, 2017).

No dispositivo subsequente (art. 4º), abordam-se as diretrizes, dentre as quais destacam-se: promover a simplificação administrativa, a modernização da gestão pública e a integração dos serviços públicos, especialmente aqueles prestados por meio eletrônico (II); fazer incorporar padrões elevados de conduta pela alta administração para orientar o comportamento dos agentes públicos, em consonância com as funções e as atribuições de seus órgãos e de suas entidades (V); implementar controles internos fundamentados na gestão de risco, que privilegiará ações estratégicas de prevenção antes de processos sancionadores (VI), assim como editar e revisar atos normativos, pautando-se pelas boas práticas regulatórias e pela legitimidade, estabilidade e coerência do ordenamento jurídico e realizando consultas públicas sempre que conveniente (IX) (BRASIL, 2017).

As diretrizes traçadas demonstram pressupostos que se coadunam com as boas práticas e o *compliance*. No entanto, antes de adentrar aos respectivos temas, necessário dispor acerca da Governança de Dados, nicho da Governança.

A Governança de Dados "tem foco nos aspectos físicos, operacionais, preparatórios e basais, além de se direcionar para políticas de metadados, linhagem, qualidade/ limpeza, níveis de serviços, segurança e impactos de mudanças" (FRAGA, 2022).

Vanessa de Souza Fraga, conteudista da Escola Nacional de Administração Pública (ENAP) no curso ofertado pela respectiva instituição intitulado *Governança de Dados na Transformação Digital*, aborda os principais aspectos correlacionados à Governança de Dados, abaixo descritos:

> Gestão de Dados Estratégica: GD é a tomada de decisões a respeito de Gestão de Dados pela alta administração, portanto, não deve ser somente aplicada nos níveis táticos e operacionais das empresas.
> Patrocínio: devido aos aspectos culturais e de mudanças trazidas, deve ser constante em todo o programa, cuja falta impacta o andamento e a conclusão das iniciativas.
> Funciona como um Governo: pode ser entendida como a definição de normas, políticas, procedimentos e padrões que devem ser adotados pela Gestão de Dados Executiva (legislativo – Políticas e Padrões). Administra as políticas, a arquitetura e os serviços definidos (executivo – Processos e Procedimentos). É responsável por gerir as questões de conflito existentes em todos os níveis em que a GD é adotada (judiciário).
> Adotada através de um programa: projetos de melhoria demandam esforço temporário empreendido para criar um produto, serviço ou resultado exclusivo, com tempo e orçamentos limitados. Os programas, por sua vez, possuem certa perenidade e envolvem vários projetos.
> Outras Ps que precisam ser consideradas dentro do contexto de Governança são:
> Participação: requer comunicação para divulgar as informações sobre o que está acontecendo nos projetos, *drivers*.
> Performance: avaliação do andamento e do alcance das ações.
> Plataformas: disponibilização em bases tecnológicas (FRAGA, 2022).

Para a existência de uma Política de Governança de Dados eficaz, imperativo pois, a existência de uma Política de Governança eficaz. É dizer, a partir da eficiência dos mecanismos da Governança, parte-se para a implementação de uma Política de Governança de Dados para a atuação da Administração Pública na perspectiva da Lei Geral de Proteção de Dados (LGPD).

Não há como conceber uma estrutura inócua de Governança e, ainda assim admitir que a Governança de Dados estará bem implementada. Uma depende da outra. A LGPD, enquanto lei principiológica, fomenta uma Política de Governança, mediante boas práticas e *compliance*, conforme outrora destacado.

Partindo-se do conceito de Governança, é possível desvelar o conceito de Governança de Dados. Com vistas a isso, o Decreto nº 10.046, de 09 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" (BRASIL, 2019).

O Decreto define, no inciso XV, art. 2º, a Governança de Dados tal como o: "exercício de autoridade e controle que permite o gerenciamento de dados sob as perspectivas do compartilhamento, da arquitetura, da segurança, da qualidade, da operação e de outros aspectos tecnológicos" (BRASIL, 2019).

Portanto, a Governança de Dados caracteriza-se como o conjunto de mecanismos aptos a boa gestão das informações no ambiente organizacional, permitindo o real cumprimento as disposições da LGPD, evitando incidentes de segurança (ciberataques, vazamento de dados, acesso não autorizado por terceiros).

A curto prazo, a Governança de Dados evita aplicações de sanções pela Autoridade Nacional de Proteção de Dados (ANPD), bem como ações cíveis indenizatórias e até mesmo ações penais, a depender do caso concreto.

A longo prazo, apresenta-se como um diferencial de "mercado", com grandes possibilidades de reconhecimento em âmbito nacional e internacional, influindo em referência perante demais entidades públicas e até mesmo, privadas, nacionais e no exterior.

Outrossim, uma Organização referência em Governança, inclusive em Governança de Dados, evita crises reputacionais, as quais podem prejudicar a relação do país com outros organismos internacionais, sobretudo em relação a acordos internacionais de cooperação.

Retomando o Decreto nº 10.046, de 09 de outubro de 2019, prevê ainda, em seu art. 5º, a possibilidade de compartilhamento de dados entre as entidades da administração pública federal direta, autárquica e fundacional e os demais Poderes da União, sem a necessidade de celebração de convênio, acordo de cooperação técnica ou outros instrumentos congêneres, desde que observadas as diretrizes impostas pelo mesmo Decreto, bem como o previsto na Lei Geral de Proteção de Dados (BRASIL, 2019).

Ademais, dispõe sobre o Cadastro Base do Cidadão, que tem por finalidade, dentre outras, o aprimoramento da gestão de políticas públicas (I) e o aumento da confiabilidade dos cadastros de cidadãos já existentes na Administração Pública, por meio de mecanismos de

manutenção da integridade das bases de dados com o fito de torná-las qualificadas e consistentes (II) (BRASIL, 2019).

Instituiu também um Comitê Central de Governança de Dados que detém a competência para apreciar as controvérsias decorrentes do compartilhamento de dados entre órgãos e o gestor de dados[19], previsto no art. 26 do mesmo instrumento normativo (BRASIL, 2019).

De outra banda, as boas práticas ganharam mais destaque com a promulgação da Lei Geral de Proteção de Dados (LGPD). Prevista nos arts. 46 ao 51, no capítulo VII, divide-se em duas seções: a primeira trata da segurança e do sigilo de dados, por sua vez, a segunda seção aborda especificamente o tema das boas práticas e da governança (BRASIL, 2018).

Ante tais considerações, destaca-se a evolução da Governança de Dados no Brasil, cuja tabela foi elaborada pela conteudista Vanessa de Souza Fraga (2002).

Tabela 2 – Evolução da Governança de Dados no Brasil

2000	**2001**	**2002**	**2003**	**2004**
– Política E-gov - Programa de Informação Social – Comitê executivo de Governo Eletrônico (CEGE)	– Chaves de Infraestrutura Pública – Portal do Governo Eletrônico	– Website Rede Governo	– Comunicações de Rede Infovia Brasília – Comitê Gestor para a internet no Brasil	– Portal da Transparência
2005	**2006**	**2007**	**2008**	**2009**
– E-governo Interoperabilidade (e-ping) – Website E-procuração – Programa Nacional para Gestão pública/ Desburocratização	– Portal da Inclusão Digital – Survey da Evolução dos Serviços com Indicadores do Governo Eletrônico	– Modelo de Acessibilidade em Governo Eletrônico (eMAG) – Avaliador de Acessibilidade de sítios (ASES)	– Padrões da Web (ePWG) – Infraestrutura de Dados Espaciais Nacionais (INDE) - Estratégia Tecnológica de Informações Gerais (EGTI)	– Decreto Cidadão: simplificação e integração do serviço público
2010	**2011**	**2012**	**2013**	**2014**

19 O Gestor de Dados é o órgão ou a entidade responsável pela governança de determinado conjunto de dados, conforme disposto no art. 2º, XIII, do Decreto nº 10.046, de 09 de outubro de 2019.

– Programa Banda Larga Nacional – TIC Pesquisa em Governo Eletrônico	– Comitê Interministerial de Plano de Ação em Governo Aberto Nacional	– Websites acessíveis para pessoas com incapacidades – Lei de Acesso a Informação – Infraestrutura Nacional de Dados Abertos (INDA) – Portal de Dados Abertos Brasileiro	– Programa Cidades Digitais – Decreto nº. 8.135: Comunicação de dados com o governo federal	– Marco Civil da Internet – VLibras (tradutor digital automático de Libras através da Língua Brasileira de Sinais) – Identidade de Governo Digital – Decreto n°. 8.243: Participação Social de Política Nacional – Portal Participa.br
2015	**2016**	**2017**	**2018**	**2019**
– Programa Brasil Bem Mais Simples – Processo Eletrônico Nacional (PEN)	– Decreto nº. 8.638: Política de Governança Digital – Estratégias de Governança Digital (EGD) - Decreto nº. 8.777: Política de Dados Abertos – Plataforma de Cidadania Digital – Decreto nº. 8.789: Compartilhamento de Dados Federais	– Decreto nº. 9.094: Simplificação do Serviço Público – Decreto nº. 9.203: Política de Governança Federal – Lançamento da Plataforma Govdata – Previsão dos serviços usando autenticação “Cidadão Brasileiro”	- Decreto nº. 9.319 Sistema Nacional de Transformação Digital e Estratégias Brasileiras para a Transformação Digital (E-Digital) - Ordem n°. 107: Versão revisada das Estratégias de Governança Digital (EGD) – Lei de Proteção de Dados Gerais (Lei n°. 13.709/2018)	– Decreto n°. 10.046: Governança de Compartilhamento de Dados e Cadastro Base do Cidadão e o Comitê Central de Governança de Dados – Decreto n°. 9.723: institui o CPF como instrumento suficiente e substitutivo da apresentação de outros documentos – Decreto nº. 9.929: Sistema Nacional de Informações de Registro Civil – Sirc
2020	**2021**	**2022**		
– Decreto nº. 10.332, Estratégia de	– Lei n°. 14.129/2021: Governo Digital	– O Decreto nº. 10.996 de 14 de março de 2022,		

Governo Digital para o período de 2020 a 2022 – 18 estratégias e mais de 50 iniciativas com uma carteira de mais de 1000 projetos de transformação digital – Decreto nº. 10.403: Governança no Compartilhamento de Dados e o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados	para o aumento da eficiência pública	altera o Decreto nº 10.332, de 28 de abril de 2020, que institui a Estratégia de Governo Digital para o período de 2020 a 2022 – aproxima as GovTechs às ações de transformação digital do país		

Fonte: ENAP, 2022.

O objetivo da positivação do capítulo ora citado consiste na necessidade de compreensão de que o tratamento de dados pessoais impõe uma mudança de paradigmas nas Organizações, uma verdadeira filosofia de gestão, ou seja, exige uma mudança de perspectiva referente a proteção de dados pessoais.

Ocorre que, para a viabilidade dessa mudança de postura no ambiente das Organizações, sobretudo na Administração Pública e com vistas a prestação de serviços públicos, tanto as boas práticas, quanto a Governança e o *compliance*, é imperativo a existência de mecanismos que repercutam em todo o sistema organizacional, ou seja, inicialmente, surge a mudança na cultura da própria organização para, então, emergir uma mudança na cultura de proteção de dados pessoais.

3.2 DO *COMPLIANCE,* DA SEGURANÇA E DAS BOAS PRÁTICAS

Feitas algumas ponderações introdutórias a respeito das boas práticas e do *compliance* no tópico anterior, em razão da interseção entre os temas, mostra-se necessária a realização de uma análise mais detida, sobretudo alinhada a questão da segurança no ambiente informacional digital.

No que pertine ao *compliance*, a expressão deriva do termo "*to comply*" que significa comprometimento, assunção de compromisso. Trata-se de comprometimento com a integridade, mediante o reconhecimento da missão, da visão e do valor que a Organização possui no bojo de sua atividade e para com a sociedade.

Para Giovani Agostini Saavedra, "*compliance* é a área do conhecimento que procura definir qual é esse conjunto complexo de medidas que permite, em face de um cenário futuro 'x' de risco, assegurar 'hoje', com a máxima eficácia, um estado de conformidade de todos os colaboradores de uma determinada organização com uma determinada 'orientação de comportamento'" (SAAVEDRA, 2021).

Nesse diapasão, a implementação de *compliance* no ambiente organizacional perpassa a segurança e as boas práticas. Trata-se de uma inter-relação entre estas de modo que, a ineficácia de uma dessas medidas, importa na fragilidade das demais.

Por outro lado, LGPD, em seu art. 46, alude à segurança e as boas práticas, nestes termos: "Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito" (BRASIL, 2018).

A segurança é tratada como um princípio na LGPD em seu art. 6º, inciso VII, definido como a "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão" (BRASIL, 2018).

Depreende-se dos supraditos dispositivos que as medidas aptas a assegurar a proteção de dados pessoais devem abarcar medidas preventivas e reparatórias, com ênfase nas medidas preventivas.

Tais medidas devem, ainda, ser observadas, "desde a fase de concepção do produto ou do serviço até a sua execução" (BRASIL, 2018) intitulado *privacy by design*. É o que estatui o §2º do art. 46 da LGPD.

Além do *privacy by design*, Edson Pires da Fonseca alude ao *privacy by default*, que "significa que o padrão operacional do tratamento de dados já oferecerá ao titular a maior proteção possível à privacidade, sem que ele precise fazer alguma coisa" (FONSECA, 2021, p. 167).

Tudo isso com vistas a resguardar a proteção de dados pessoais desde antes da coleta até a eliminação dos respectivos dados outrora coletados.

A segurança da informação, consiste em hábil mecanismo viabilizador para a implementação da LGPD. Para tanto, ilustra-se a *International Organization for Standardization*, ou "Organização Internacional de Padronização" ou somente, ISO 27.001.

Dito documento adota o ciclo *Plan/Do/Check/Act* (PDCA) em português Planejar/Realizar/Verificar/Agir, como modelo, para a estruturação do Sistema de Gestão em Segurança da Informação (SGSI).

Importante mencionar que: "o PDCA padroniza as informações de controle, reduz e evita erros lógicos, facilita o entendimento das informações, melhora a realização das atividades e proporciona resultados mais confiáveis. Também é chamado de Ciclo da Melhoria Contínua" (PALUDO, 2022, p. 320).

Abaixo, colaciona-se um modelo para implementação de um sistema em segurança da informação aliado a um programa de gestão, isto é, um programa de segurança da informação aliado à própria estrutura organizacional o que, de fato, reforça a necessidade e a importância de sistemas integrados as Organizações, a partir da atenção às necessidades e riscos que cada entidade assume no trato das informações.

Tabela 3 — Modelo PDCA aplicado aos processos do SGSI

Plan (planejar) (estabelecer o SGSI)	Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.
Do (fazer) (implementar e operar o SGSI)	Implementar e operar a política, controles, processos e procedimentos do SGSI.
Check (checar) (monitorar e analisar criticamente o SGSI)	Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção.
	Executar as ações corretivas e preventivas,

Act (agir) (manter e melhorar o SGSI)	com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

Fonte: ISO nº 27.001

Necessário pois, que cada Organização estabeleça seus Relatórios de Impactos de Riscos. A LGPD também prevê o Relatório de Impacto à Proteção de Dados Pessoais, o qual poderá ser solicitado pela Autoridade Nacional, cuja definição encontra amparo no inciso XVII do art. 5º, assim definido: "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco" (BRASIL, 2018).

Com vistas a isso, a Autoridade Nacional de Proteção de Dados (ANPD) emitiu um *Guia de Avaliação de Riscos de Segurança e Privacidade* com base na Lei Geral de Proteção de Dados (LGPD), publicado no mês de novembro de 2020.

Na conjectura do *privacy by design*, o Guia adota o *security by design*, com a necessidade de incorporação da segurança da informação durante todo o ciclo de vida do sistema.

Ademais, aponta 14 (catorze) riscos utilizados na avaliação, a saber: (i) acesso não autorizado; (ii) coleta excessiva de dados; (iii) compartilhar ou distribuir dados pessoais com terceiros fora da Administração Pública Federal sem o consentimento do titular dos dados; (iv) falha em considerar os direitos do titular dos dados pessoais (ex.: perda do direito de acesso); (v) falha ou erro de processamento; (vi) informação insuficiente sobre a finalidade do tratamento; (vii) modificação não autorizada; (viii) perda; (ix) reidentificação de dados pseudonimizados; (x) remoção não autorizada; (xi) retenção prolongada de dados pessoais sem necessidade; (xii) roubo; (xiii) tratamento sem consentimento do titular dos dados pessoais (caso o tratamento não esteja previsto em legislação ou regulação pertinente); (xiv) vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular (BRASIL, 2020).

Por óbvio, não se objetiva restringir os eventuais riscos atinentes ao tratamento de dados pessoais ao número de 14 (catorze) tampouco adotar um modelo específico e

padronizado a ser observado por toda e qualquer Organização. O objetivo da ANPD na emissão dos Guias Orientativos consiste na melhor elucidação das disposições constantes na LGPD.

Não se pode perder de vista que a legislação protetiva dos dados pessoais dialoga com as demais normas vigentes no ordenamento jurídico brasileiro e, até mesmo, com a legislação internacional, a exemplo da GDPR e demais documentos internacionais, como Convenções e Declarações.

Dessa forma, uma Organização que consiga traduzir para um Relatório de Impacto, suas necessidades, seus déficits e suas potencialidades, bem como adequá-los ao seu modelo de gestão, alcançará benefícios que repercutirão na sua identidade reputacional e no diferencial competitivo.

Figura 1. Benefícios da Avaliação de Riscos

Fonte: Autoridade Nacional de Proteção de Dados (ANPD), 2020

A figura 1 ilustra bem os benefícios oriundos da avaliação de riscos no ambiente organizacional. O amadurecimento de processos internos; a adaptação de contratos; o auxílio a construção do Relatório de Impacto à Proteção de Dados (RIPD); o auxílio na transparência com o titular dos dados pessoais; a identificação e o monitoramento dos riscos e; a conformidade legal com a LGPD.

No que pertine as Boas Práticas e Governança, o art. 50 *caput* e §2º, inciso I explicitam:

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.
> I - implementar programa de governança em privacidade que, no mínimo:
>
> a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
>
> b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
>
> c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
>
> d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
>
> e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
>
> f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
>
> g) conte com planos de resposta a incidentes e remediação; e
>
> h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas (BRASIL, 2018).

Da leitura dos supraditos dispositivos, visualiza-se a estreita relação das boas práticas e da Governança ao *compliance*. A implementação de um Programa de Governança em Privacidade (PGP) impõe a assunção de comprometimento pelos multi *stakeholders* e a consequente adoção dos pilares aplicados ao *compliance*, tais como o "*tone from the top*; Código de Ética e de Conduta; políticas; procedimentos e controles internos; investigações internas; treinamentos; canais de denúncia; auditoria; *due diligence*; *risk assesment* etc." (SAAVEDRA, 2021).

Cumpre mencionar a importância do Programa de Integridade nas Organizações. Frisa-se que esse tipo de programa contribui para a adoção de boas práticas, do *compliance* e da Governança, bem como constitui instrumento hábil ao combate à corrupção.

A respeito do tema, cita-se a Lei nº 14.129/2021, Lei do Governo Digital, em seu capítulo VII referente à Governança, Gestão de Riscos, Controle e Auditoria. O parágrafo único do art. 47 informa parâmetros mínimos para as práticas de Governança: (i) formas de

acompanhamento de resultados; (ii) soluções para a melhoria do desempenho das organizações e; (iii) instrumentos de promoção do processo decisório fundamentado em evidências (BRASIL, 2021).

Por sua vez, o art. 48 dispõe que a Administração Pública deverá "estabelecer, manter, monitorar e aprimorar sistema de gestão de riscos e de controle interno com vistas à identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica de riscos da prestação digital de serviços públicos que possam impactar a consecução dos objetivos da organização no cumprimento de sua missão institucional e na proteção dos usuários" (BRASIL, 2021).

Destarte, o Decreto nº 8.420, de 18 de março de 2015, explicita o Programa de Integridade nos arts. 41 e 42. Estabelece que o Programa de Integridade "consiste, no âmbito de uma pessoa jurídica, no conjunto de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e na aplicação efetiva de códigos de ética e de conduta, políticas e diretrizes com objetivo de detectar e sanar desvios, fraudes, irregularidades e atos ilícitos praticados contra a administração pública, nacional ou estrangeira" (BRASIL, 2015).

Do mesmo modo que a partir da adoção da Governança torna-se plausível a Governança de Dados, a implementação do *compliance* viabiliza o *compliance* digital ou *compliance* de dados, tal qual se denota no disposto na Lei do Governo Digital.

Chama-se a atenção ao fato de que esses instrumentos devem ser estimulados tanto na esfera privada quanto na esfera pública, independentemente do porte das Organizações, até porque, não se exige alta complexidade e altos custos quanto à adoção de melhores condutas e aderência normativa, em especial à Lei Geral de Proteção de Dados (LGPD).

Portanto, as disposições pertinentes ao *compliance* alinham-se com a LGPD, sobretudo em razão das boas práticas e da Governança. Em verdade, a Governança, as Boas Práticas e o *Compliance* estão interligadas. Explica-se: o primeiro passo para a implementação de um programa de *compliance* em uma Organização é a realização de um Programa de Integridade, baseado em boas práticas. A partir de tal constatação, os resultados terão impacto na Governança, como medidas que a subsidiam na tomada de decisões por parte dos gestores.

3.3 DADOS ABERTOS *VERSUS* DADOS PESSOAIS: INTEGRANDO A CIBERTRANSPARÊNCIA AO DEVER DE PROTEÇÃO DE DADOS

Um dos primeiros passos para a implementação da LGPD pela Administração Pública, em especial, na Administração Pública 4.0, é a compreensão acerca do ciclo de vida dos dados pessoais. Posteriormente, importante analisar quais os tipos de dados coletados pois, a depender do tipo de dado, pessoal ou pessoal sensível, o nível de proteção e a necessidade da adoção de um mecanismo de supervisão mais robusto deverá ser analisado. Geralmente, os dados pessoais sensíveis demandam maior cuidado, em razão da sua própria natureza, cujas informações dizem respeito a esfera mais íntima do indivíduo.

Por outro lado, existem os dados abertos, regulamentados pelo Decreto nº 8.777/2016, Decreto nº 9.903/2019 e pela Resolução nº 03/2017. Em que pese já ter sido objeto de análise no presente trabalho, importante ressaltar o conceito de dados abertos, estatuído pelo Decreto nº 8.777/2016, no inciso III do art. 2º, *in verbis*: "dados acessíveis ao público, representados em meio digital, estruturados em formato aberto, processáveis por máquina, referenciados na internet e disponibilizados sob licença aberta que permita sua livre utilização, consumo ou cruzamento, limitando-se a creditar a autoria ou a fonte" (BRASIL, 2016).

Com base em tal definição, parte-se de uma compreensão de que os dados abertos são reflexos da Administração Pública 4.0 numa clara demonstração de promoção do acesso público à informação, da publicidade, da cibertransparência e da ciberdemocracia.

Ante esse entendimento, não se vislumbra aparente contradição entre a Política de Dados Abertos e a LGPD, haja vista que a predita lei aduz pela possibilidade de transferência de dados a entidades privadas nos casos em que os dados forem acessíveis publicamente, isto é, é possível o compartilhamento de dados entre entidades públicas e privadas no que pertine aos dados abertos – dados acessíveis ao público, consoante o previsto no inciso III do §1º do art. 26.

Esses dados representam informações atreladas ao direito social, ou seja, que influirão nas demandas sociais e nas políticas públicas, não afetando, ao menos em um primeiro momento, direitos individuais, como a honra e a privacidade.

Alguns aplicativos que utilizam dados abertos já se encontram disponíveis, a exemplo do Repasse, "ferramenta para visualização das transferências do governo federal

para a sua cidade e possibilitar a análise do impacto das mesmas". Outro exemplo é o aplicativo Cuidando do meu bairro, que apresenta, em tempo real, informações a respeito da execução orçamentária no Município de São Paulo.

Conforme já relatado, dados abertos representam a expressão da Revolução Digital na atuação estatal. De outro modo, os dados pessoais – relacionados a pessoa natural identificada ou identificável, são representação dos direitos e liberdades fundamentais. Não atoa, à proteção de dados pessoais é assegurado o *status* de direito fundamental, hodiernamente previsto de forma expressa na Constituição Federal de 1988, por meio da Emenda Constitucional nº 115/2022.

Ultrapassadas as discussões acerca dos dados abertos e dos dados pessoais, passíveis de convivência harmônica no ordenamento pátrio, passa-se ao estudo da implementação da LGPD na Administração Pública.

Para além dos mecanismos outrora citados: Governança, Governança de Dados, Programa de Integridade, Gestão em Segurança da Informação, Boas Práticas, *Compliance* e *Compliance* de Dados, bem como a técnica *Plan/Do/Check/Act* (PDCA), ilustram-se outras importantes técnicas aptas a assegurar a implementação da LGPD, sobretudo com base numa coordenação intergovernamental. A técnica de B*enchmarking*, a técnica *5W+1H+SHOW ME*, a Abordagem *Lean* e o *Brainstorming*.

O *benchmarking* é uma técnica de Auditoria, um dos pilares do *compliance*, imprescindível também para a Governança e adoção de boas práticas.

Para sua utilização é imprescindível para a Organização

> Conhecer suas operações e avaliar seus pontos fortes e fracos (processos e diagnósticos internos), e selecionar indicadores e fatores de comparabilidade; conhecer/selecionar os concorrentes e organizações líderes de mercado, identificar suas práticas, habilidades, pontos fortes e resultados, para compará-los com as práticas, os pontos fortes/fracos e resultados de sua empresa; e implantar na organização o "melhor do melhor": os pontos fortes e as práticas dos concorrentes, e, se possível, ultrapassá-los – monitorando os resultados (PALUDO, 2022, p. 317-318).

Segundo o documento elaborado pela Coordenadoria de Fiscalização e Controle do Tribunal de Contas da União (TCU) sobre o tema, predita técnica pode ser definida como: "uma técnica voltada para a identificação e implementação de boas práticas de gestão. Seu propósito é determinar, mediante comparações de desempenho e de boas práticas, se é possível aperfeiçoar o trabalho desenvolvido em uma organização. O *benchmarking* pode

ajudar na identificação de oportunidades de melhorar a eficiência e proporcionar economia" (BRASIL, 2000).

Apresentam-se, ademais, os seus tipos.

> *Benchmarking* organizacional é a comparação de uma organização com outras similares do setor público ou privado, nacionais ou internacionais, com o objetivo de identificar boas práticas.
> *Benchmarking* de desempenho é a comparação feita por meio da utilização de uma série de padrões e de indicadores de desempenho. Normalmente esses indicadores estão relacionados aos aspectos da produtividade, da utilização de recursos, dos custos unitários e, quando possível, da qualidade do serviço.
> *Benchmarking* de processo é a comparação de processos organizacionais, incluindo comparações quantitativas e qualitativas. Pode ser externo, entre organizações, ou interno, comparando setores dentro de uma mesma organização (BRASIL, 2000).

Nada obsta que uma entidade da Administração Pública, por exemplo, realize uma comparação – palavra-chave para essa técnica – em relação a outras entidades de caráter público ou privada, com vistas a adoção de boas práticas implementadas por estas e que geraram bons resultados na gestão.

No mesmo sentido, a Administração Pública pode adotar padrões e indicadores importados de outras entidades que também apresentaram bons resultados, realizando assim, uma comparação de desempenho entre a Administração Pública em questão e a entidade que serve de "bom exemplo".

Por fim, o *benchmarking* de processo, visa a melhoria de processos organizacionais, podendo ser adotado modelo de referência de um setor específico. A título exemplificativo, imagina-se um setor de recursos humanos que apresenta produtividade com redução no tempo de resposta a demandas de ouvidorias com a resolução de litígios dentro da própria Organização.

Nesse caso, realiza-se um estudo para identificar o processo organizacional produtivo, aspectos que influenciaram a redução do tempo de resposta e a efetividade das resoluções de tais demandas. Diante disso, busca-se expandir a "gestão" dos recursos humanos para outros setores da mesma Organização, respeitadas as peculiaridades de cada setor.

No tratamento de dados pessoais essa técnica coopera na adoção de melhores práticas entre as entidades. No setor público pode, ainda, contribuir para a coordenação

intergovernamental na formulação de uma Política de Privacidade adequada ao setor e na corregulação por meio de Associações interestatais.

Outra importante técnica é a *5W+1H+SHOW ME.* O 5W representa os 05 (cinco) questionamentos: What?, Who?, Where? When?Why?, How? Acrescido da expressão SHOW ME, em português: O que, qual, quê?, Quem?, Onde?, Quando?, Por quê e Como? Acrescido da expressão Mostre-me (PETER; MACHADO, 2014, p. 129).

Asseveram Maria da Glória Arrais Peter e Marcus Vinícius Veras Machado: "essa técnica permite efetuar questões abertas e evitar perguntas que possibilitem apenas uma resposta. É uma ferramenta útil que possibilita comprovar se o que está descrito sobre normas e rotinas é de fato realizado" (PETER; MACHADO, 2014, p. 129).

O uso de tal técnica aliada ao tratamento de dados pessoais viabiliza as respostas que a entidade precisa para realizar o adequado tratamento de dados pessoais respondendo-se aos seguintes questionamentos: Quais dados pessoais serão tratados? Quem realizará o tratamento de dados (encarregado) e quem é o titular? Onde será realizado esse tratamento (ambiente físico e/ou digital)? Quando será realizado? (delimitar duração do tratamento) Porque deve ser realizado o tratamento de dados (bases legais)? Como será realizado esse tratamento? (delimitação das etapas, compreensão do ciclo de vida dos dados).

A partir da obtenção das respostas, procede-se a seguinte afirmação: "Mostre-me", é o princípio da transparência e/ou cibertransparência, traduzido na ideia de publicizar o tratamento de dados pessoais, em especial através da Política de Privacidade de Dados e do respeito ao direito do titular de obter do controlador, informações sobre seus dados por ele tratados, "a qualquer momento e mediante requisição", conforme dispõe o art. 18 da LGPD.

Nota-se a importância dessa técnica porquanto os mecanismos outrora citados exigem uma postura proativa dos multi *stakeholders* mediante o diálogo aberto e a adoção de práticas que, de fato, representem as atribuições da própria Organização. O Código de Conduta de uma empresa que atue em regime de concorrência, por exemplo, não será o mesmo que o adotado por uma empresa de *marketing* que, por sua vez, não será o mesmo adotado pela Administração Pública Federal, em decorrência da realidade das atribuições de cada setor, ou seja, não existe um modelo de gestão que se aplique a toda e qualquer Organização, é imperativo destacar as finalidades precípuas de cada setor.

A abordagem *lean,* por seu turno*,* pode ser traduzida como uma abordagem enxuta, considerada uma filosofia de gestão.

Tal filosofia já vem sendo implementada na Administração Pública, em especial na perspectiva de sua transformação digital. A Fundação Escola Nacional de Administração Pública (ENAP) informa: "Mais especificamente em relação ao serviço público, existem três vertentes principais de conhecimento *Lean* que podem ser aplicadas na Administração Pública: *Lean Government, Lean Services, e Lean Office* (estes dois últimos com adaptações às particularidades do setor público). Outras, como *Lean Healthcare, Lean Higher Education* são sub-ramificações do *Lean Services* adaptadas. No contexto do governo brasileiro, busca-se trilhar um caminho em direção à transformação digital, por meio da Estratégia de Governo Digital" (LIMA, 2022).

Essa técnica pode ser implementada nos mais diversos setores, como os setores de saúde e educação. No tratamento de dados pessoais essa filosofia de gestão é nomeada *Lean Data*. Em suma, consiste em adotar os preceitos dessa abordagem ao tratamento de dados pessoais.

Trata-se de relevante instrumento hábil a apoiar a Governança no setor público, haja vista que a abordagem *lean*, pugna pela mudança de paradigmas, isto é, exige uma mudança na cultura organizacional, tal qual as demais técnicas abordadas.

O quadro abaixo elucida as diferenças entre a cultura tradicionalmente adotada e a abordagem *lean*.

Tabela 4. Comparativo entre a Cultura Tradicional e a Cultura *Lean*

CULTURA TRADICIONAL	***CULTURA LEAN***
Silos de função	Equipes Interdisciplinares
"Faça Assim!"	"O que Você Acha?"
Líderes = Ditadores	Líderes Ouvem e Ensinam/Capacitam
Culpar as pessoas	Culpar o processo
Recompensas Individuais	Recompensas Coletivas
Conhecimento é um ativo individual	Conhecimento é um ativo coletivo (*Yokoten*)
Reduz-se custos aumentando o volume de produção	Reduz-se custos removendo desperdícios
Foco = Melhorar Eficiência	Foco = Agregação de Valor para o Cliente
Melhoria periódica orientada por especialistas	Melhoria Contínua Orientada por Processos

Fonte: Lauria (2013). Elaboração: CEPED/UFSC (2022).

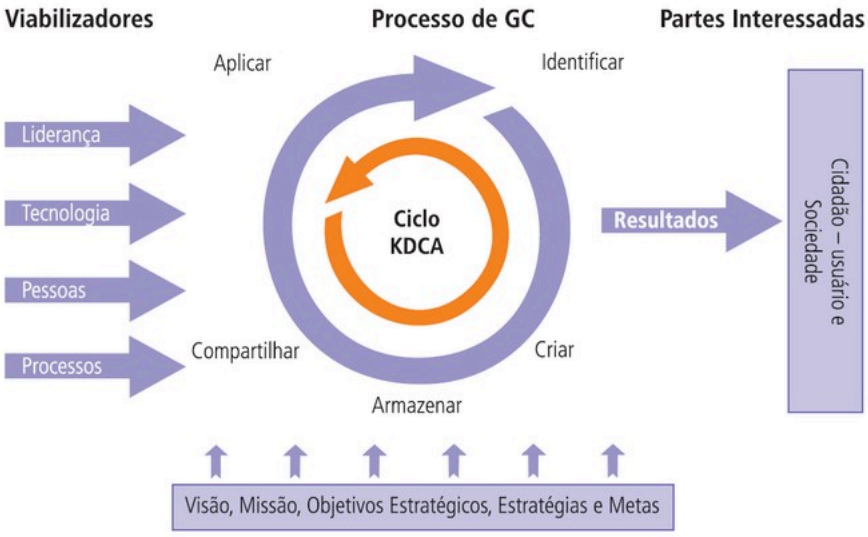
Percebe-se que a cultura *lean* propõe abordagem responsiva, postura proativa das múltiplas partes interessadas (equipe interdisciplinar) e a melhoria contínua na persecução das

finalidades públicas orientada pelo monitoramento das ações e busca pelas melhores técnicas aptas a assegurar a prestação de serviços públicos de forma mais eficiente.

Todas essas técnicas apresentadas, contribuem sobremaneira na mudança da cultura de proteção de dados pessoais, porque contribuem para o *New Public Management* (NPM), traduzido como Nova Gestão Pública.

Quanto ao *brainstorming*, em português "tempestade de ideias", enfatiza-se o *Modelo de Gestão do Conhecimento para a Administração Pública Brasileira: Como implementar a Gestão do conhecimento para produzir resultados em benefício do cidadão*, de autoria de Fábio Ferreira Batista e divulgado pelo Instituo de Pesquisa Econômica Aplicada (IPEA) no ano de 2012. O modelo de gestão demonstra os benefícios da gestão do conhecimento no setor público. Desse modo, a Gestão do Conhecimento (GC) "ajuda as organizações a enfrentar novos desafios, implementar práticas inovadoras de gestão e melhorar a qualidade dos processos, produtos e serviços públicos em benefício do cidadão-usuário e da sociedade em geral" (BATISTA, 2012).

Figura 2. Modelo de Gestão do Conhecimento para a Administração Pública



Fonte: Fábio Ferreira Batista, 2012.

Para a efetivação de um modelo de gestão do conhecimento deve-se ter como ponto de partida a estipulação da visão, da missão, dos objetivos estratégicos, estratégias e metas

relativos aos processos organizacionais. Em seguida, parte-se para os eixos viabilizadores, liderança, tecnologia, pessoas e processos. Fábio Ferreira Batista esclarece sobre a liderança:

> Em primeiro lugar, é ela que deve dirigir o esforço de implementação da GC. Cabe a liderança apresentar e reforçar a visão e as estratégias de GC que, (...) devem estar alinhadas com os direcionadores estratégicos da organização.
> Compete, também, à liderança estabelecer a estrutura de governança e os arranjos organizacionais para formalizar as iniciativas de GC. Isso pode incluir: a instituição de unidade central de coordenação da gestão da informação e do conhecimento; a nomeação de um gestor chefe de gestão da informação e do conhecimento; a criação de equipes de GC; comunidades de prática; redes de conhecimento, entre outras iniciativas.
> É a liderança quem aloca recursos financeiros para viabilizar as iniciativas de GC e assegura a utilização da GC para melhorar processos, produtos e serviços (BATISTA, 2012).

O eixo viabilizador da liderança remete ao pilar do *compliance* do "*tone at the top*", em português, suporte da alta administração, traduzido na ideia do "exemplo vem de cima" na qual, além de prover os recursos financeiros, compete a alta administração assumir a responsabilidade de respeitar os preceitos da Organização. No que toca a tecnologia, o autor cita algumas ferramentas da Tecnologia da Informação (T.I) que colaboram na Gestão do Conhecimento, tais como os sistemas de *workflow, data warehouse e data mining,* abaixo definidas:

> (…)
> Sistemas de *workflow* – são práticas ligadas ao controle da qualidade da informação apoiado pela automação do fluxo ou trâmite de documentos. *Workflow* é o termo utilizado para descrever a automação de sistemas e processos de controle interno, implantada para simplificar e acelerar os negócios. É utilizado para controle de documentos e revisões, requisições de pagamentos, estatísticas de desempenho de funcionários etc
> (…)
> *Data Warehouse* (ferramenta de TI para apoio à GC) – tecnologia de rastreamento de dados com arquitetura hierarquizada disposta em bases relacionais, permitindo versatilidade na manipulação de grandes massas de dados.
> *Data mining* (ferramenta de TI para apoio à GC) – os mineradores de dados são instrumentos com alta capacidade de associação de termos, permitindo-lhes "garimpar" assuntos ou temas específicos (BATISTA, 2012).

Ressalta-se que as ferramentas *data warehouse* e *data mining* são de extrema relevância no contexto da implementação da LGPD nas Organizações, sendo importante o alinhamento entre a Segurança da Informação, a Gestão do Conhecimento e a Governança de Tecnologia da Informação (T.I).

Em relação ao eixo viabilizador pessoas, necessário remeter ao pilar do *compliance* do treinamento e da comunicação. A gestão do conhecimento exige também a implementação pelas partes envolvidas com o constante aperfeiçoamento mediante a promoção de cursos de capacitação, *workshops* e demais métodos que proporcionam aprendizagem contínua.

Por fim, sobre o eixo viabilizador referente ao processo, Batista (2012) aponta tratar-se de "conjunto de atividades que transformam insumos (ou entradas) em produtos e serviços (saída) na organização por meio de pessoas que utilizam recursos entregues por fornecedores. É uma sequência de passos que aumenta a contribuição do conhecimento na organização".

Nesse eixo o autor desta a importância da técnica de *benchmarking* e das melhores práticas, dentre outros.

O processo de Gestão do Conhecimento (GC) envolve cinco etapas primordiais: aplicar, identificar, compartilhar, armazenar e criar, com suporte na técnica KDCA, derivada do ciclo PDCA onde o P de *Plan* (Planejar), é substituído pelo K, *Knowledge* (Conhecimento) (BATISTA, 2012).

Os resultados podem ser imediatos e finais, os imediatos são aprendizagem e inovação. Os finais: "decorrem dos imediatos (aprendizagem e inovação; e aumento da capacidade de realização individual, de equipes, da organização e da sociedade) e aparecem na definição de GC na administração pública, a saber: aumentar a eficiência; melhorar a qualidade e a efetividade social; e contribuir para a legalidade, impessoalidade, moralidade e publicidade na administração pública e para o desenvolvimento brasileiro" (BATISTA, 2012).

No que pertine as partes interessadas, último componente na Gestão de Conhecimento (GC), os destinatários são o cidadão-usuário e a sociedade. Em vista tratar-se de Gestão do Conhecimento na Administração Pública, nada mais razoável que os resultados sejam apresentados aos destinatários da prestação de serviços públicos.

Adentrando especificamente no tema do *brainstorming,* frisa-se que este decorre na implementação de Gestão de Conhecimento, podendo ser definida como:

> Uma maneira simples de ajudar um grupo de pessoas a gerar ideias novas e diferentes. O processo é normalmente dividido em duas fases: divergência e convergência. Na fase de divergência, todos concordam em não criticar as ideias. Em outras palavras, todas as ideias são consideradas válidas. Já na fase de convergência, os participantes criticam as ideias apresentadas destacando, em primeiro lugar, o que eles acharam de positivo para, só depois, citar as ideias com as quais não concordam (BATISTA, 2012).

Aludida técnica fomenta novas ideias para a estrutura e manutenção da Governança e das boas práticas, respeitando a proatividade das partes interessadas com vistas a mudança na cultura organizacional. Quando o ambiente organizacional propicia o surgimento de novas ideias, as partes interessadas entendem a importância da autorresponsabilidade (abordagem responsiva) e do compromisso com as boas práticas na gestão.

Na perspectiva da Administração Pública digital o fomento as novas ideias assume um caráter ainda mais acentuado. Não se pode perder de vista que a criação de cursos livres abertos à população promovidos no ciberespaço, a elaboração de Guias, Manuais e instrumentos congêneres auxiliam na difusão do conhecimento e na implementação de legislações como a LGPD e de boas práticas, *compliance* e Governança.

Situação viável em decorrência das ideias difundidas e aceitas no ambiente organizacional. Afinal, os mecanismos citados são elaborados por servidores, geralmente de diversos setores e, até mesmo, de órgãos públicos e esferas diferentes.

No mês de abril de 2022 foi publicado um Relatório de Auditoria do Tribunal de Contas da União (TCU) no que diz respeito ao nível de implementação da LGPD pelos órgãos da Administração Pública. Na ocasião foram avaliadas 382 (trezentos e oitenta e duas) Organizações.

No que pertine a condução de iniciativa para identificação e planejamento das medidas necessárias à adequação à LGPD e a resposta ao questionamento: A organização conduziu iniciativa para identificar e planejar as medidas necessárias à adequação à LGPD? O Relatório informa que, dentre as 382 (trezentos e oitenta e duas) Organizações avaliadas, 171,45% (cento e setenta e um inteiros e quarenta e cinco centésimos por cento) CONCLUÍRAM as iniciativas para implementação da LGPD, 171,45% (cento e setenta e um inteiros e quarenta e cinco centésimos por cento) CONCLUÍRAM PARCIALMENTE e 40,10% (quarenta inteiros e dez centésimos por cento) NÃO CONDUZIRAM QUAISQUER INICIATIVAS para adequação à referida lei (BRASIL, 2022).

Em relação a identificação das categorias dos titulares dos dados, 177,46% (cento e setenta e sete inteiros e quarenta e seis centésimos por cento) conseguiram identificar ALGUMAS categorias de dados pessoais; 86,23% (oitenta e seis inteiros e vinte e três centésimos por cento) identificaram TODAS as categorias de dados pessoais, enquanto 119,31% (cento e dezenove inteiros e trinta e um centésimos por cento) NÃO

CONDUZIRAM QUALQUER INICIATIVA para identificação das categorias de dados pessoais (BRASIL, 2022).

A respeito da identificação dos dados pessoais tratados pelas Organizações, o Relatório aponta que 224,59% (duzentos e vinte e quatro inteiros e cinquenta e nove centésimos por cento) conseguiram identificar PARCIALMENTE os dados pessoais tratados por ela; 104,27% (cento e quatro inteiros e vinte e sete centésimos por cento) NÃO CONSEGUIRAM IDENTIFICAR os dados pessoais tratados por ela. Apenas, 54,14% (cinquenta e quatro inteiros e catorze centésimos por cento) das 382 Organizações avaliadas conseguiram identificar TODOS os dados pessoais tratados por ela (BRASIL, 2022).

A avaliação de riscos associada ao tratamento de dados pessoais também apresenta dados preocupantes. 153,67% (cento e cinquenta e três inteiros e sessenta e sete centésimos por cento) das Organizações NÃO AVALIARAM os riscos relativos ao tratamento de dados pessoais contra 75,33% (setenta e cinco inteiros e trinta e três centésimos por cento) que CONSEGUIRAM IDENTIFICAR os riscos associados ao tratamento de dados pessoais (BRASIL, 2022).

De acordo com o TCU:

> Este diagnóstico retrata a ausência da cultura de gestão de riscos na APF. Ademais, cumpre frisar que a análise de riscos não deve ocorrer apenas durante o projeto de adequação, é algo que deve ser realizado continuamente. Por fim, é importante que a organização considere tanto as consequências que podem ocorrer para ela própria como para os titulares de dados pessoais caso os riscos se materializem (BRASIL, 2022).

O Relatório de Impacto à Proteção de Dados também foi negligenciado por parte das instituições públicas. O documento informa que 314,82% (trezentos e catorze inteiros e oitenta e dois centésimos por cento) NÃO ELABORARAM o Relatório; 37,10% (trinta e sete inteiros e dez centésimos por cento) elaboraram Relatório que abrange ALGUNS processos de tratamento de dados pessoais que podem gerar riscos aos titulares; 24,6% (vinte e quatro inteiros e seis décimos por cento) NÃO EXECUTAM processo de tratamento de dados pessoais que pode gerar riscos às liberdades civis e aos direitos fundamentais dos titulares e, apenas 7,2% (sete inteiros e dois décimos por cento) elaboraram Relatório de Impacto à Proteção de Dados Pessoais que abrange TODOS os processos de tratamento de dados pessoais que podem gerar riscos aos titulares (BRASIL, 2022).

Compete ressaltar que o Relatório de Impacto à Proteção de Dados (RIPD): "deve ser elaborado antes de a instituição iniciar o tratamento de dados pessoais, preferencialmente, na fase inicial do programa ou projeto que tem o propósito de usar esses dados" (BRASIL, 2020), cujas etapas encontram-se delimitadas no *Guia de Boas Práticas LGPD para implementação na Administração Pública Federal*, e consistem em: (i) identificar os agentes de tratamento e o encarregado; (ii) identificar a necessidade de elaborar o Relatório; (iii) descrever o tratamento; (iv) identificar partes interessadas consultadas; (v) descrever necessidade e proporcionalidade; (vi) identificar e avaliar os riscos; (vii) identificar medidas para tratar os riscos; (viii) aprovar o Relatório; (ix) manter revisão" (BRASIL, 2020). São etapas cíclicas, isto é, os procedimentos são contínuos.

Em relação a adoção de Política de Segurança ou de instrumentos similares, 291,76% (duzentos e noventa e um inteiros e setenta e seis centésimos por cento) das Organizações afirmam que POSSUEM, contra 91,24% (noventa e um inteiros e vinte e quatro centésimos por cento) que afirmam NÃO possuir nenhuma Política de Segurança. Para o TCU: "O resultado é alarmante, pois, mesmo abrangendo a minoria, a análise do número por outra perspectiva leva à conclusão de que cerca de uma em cada quatro organizações não possui a política, o que é grave, pois a segurança da informação é um dos pilares que viabilizam a proteção de dados pessoais" (BRASIL, 2022).

Não se pode perder de vista que existem normas específicas dispondo sobre segurança da informação, a exemplo da ABNT ISO/IEC 27002, abordada no presente trabalho.

O Relatório de Auditoria mostra outro grave problema, a ausência de uma Política de Proteção de Dados Pessoais em grande parte das Organizações. Das 382 (trezentos e oitenta e duas) entidades avaliadas apenas 68,18% (sessenta e oito inteiros e dezoito centésimos por cento) POSSUEM Política de Proteção de Dados Pessoais. Em contrapartida, 314,82% (trezentos e catorze inteiros e oitenta e dois centésimos por cento) NÃO POSSUEM referida Política (BRASIL, 2022).

Outras relevantes informações podem ser extraídas do Relatório do TCU. No que pertine a publicação da nomeação do encarregado de dados em veículo oficial e a divulgação das informações pertinentes do encarregado, depreende-se que 197,75% (cento e noventa e sete inteiros e setenta e cinco centésimos por cento) PUBLICARAM a nomeação do

encarregado em veículo oficial, já 67,25% (sessenta e sete inteiros e vinte e cinco centésimos por cento) NÃO PUBLICARAM (BRASIL, 2022).

177,67% (cento e setenta e sete inteiros e sessenta e sete centésimos por cento) das Organizações DIVULGARAM a identidade e as informações de contato do encarregado de dados na internet, por sua vez, 87,33% (oitenta e sete inteiros e trinta e três centésimos por cento) NÃO DIVULGARAM (BRASIL, 2022).

Tais dados revelam a importância da publicidade dos atos da gestão pública na efetivação da cibertransparência e, sobretudo, na tutela de direitos fundamentais do (ciber)cidadão. Em que pese a percentagem positiva no questionamento, não se pode perder de vista que, ainda há grande parcela de instituições públicas que não publicizaram as informações pertinentes ao encarregado de dados, o que propicia clara violação aos direitos dos titulares desses dados. Ressalta-se que a violação a preceitos fundamentais ocorreu, na situação apresentada, pela ausência de publicidade de dados abertos (que deveriam ser disponibilizados à sociedade como instrumento de controle social), ou pela ausência de disponibilização de um encarregado de dados com suas respectivas informações (profissionais, como e-mail institucional, telefone para contato do setor público onde se encontra alocado), com vistas ao necessário tratamento de dados pessoais.

Em outro momento, o Relatório aponta que 202,53% (duzentos e dois inteiros e cinquenta e três centésimos por cento) das Organizações possuem ALGUNS colaboradores diretamente envolvidos em atividades que realizam tratamento de dados pessoais receberam treinamentos relacionados ao tema. 140,37% (cento e quarenta inteiros e trinta e sete centésimos por cento) NÃO POSSUEM colaboradores diretamente envolvidos em tais atividades. Apenas em 40,10% das Organizações (quarenta inteiros e dez centésimos por cento) TODOS os colaboradores estão diretamente envolvidos em atividades que realizam tratamento de dados pessoais receberam treinamentos relacionados ao tema (BRASIL, 2022).

Um dos pilares para que a implementação de uma cultura de proteção de dados pessoais se instale em uma Organização é o constante aperfeiçoamento. Isto pode ocorrer mediante a participação em cursos, simpósios, *workshops*, congressos, dentre outros. No que pertine a participação em cursos, renomadas instituições já os promovem de forma totalmente virtual, gratuita e com direito a certificado, a exemplo da Fundação Getúlio Vargas (FGV), do Instituto Brasiliense de Direito Público (IDP) através do *Open Class*, nesses casos as aulas do

curso são síncronas (em tempo real) e da Fundação Escola Nacional de Administração Pública (ENAP).

Quanto a ENAP, a instituição concede baixa nos certificados de participação dos cursos de sua autoria junto a outras instituições públicas do país. Há cursos livres (abertos para toda a sociedade), assim como cursos voltados apenas para a capacitação de servidores públicos.

Os dados apresentados pelo Tribunal de Contas da União (TCU) refletem a urgência e a importância da adoção de mecanismos que assegurem os direitos e liberdades fundamentais dos cidadãos, em especial, o direito fundamental à proteção de dados pessoais, sem prejuízo aos deveres de acesso público à informação, publicidade, transparência e cibertransparência, haja vista que a aplicação da LGPD não se resume ao ciberespaço.

Para tanto, os mecanismos de Governança, Governança de Dados, boas práticas, segurança da informação e *compliance* auxiliam sobremaneira no processo de implementação da LGPD, inclusive na Administração Pública, que detém verdadeiro *Big Data* e não pode se escusar de assegurar os deveres que constitucionalmente lhe foram assegurados.

Todavia, cabe mencionar que a efetividade dos mecanismos acima destacados vindicam a mudança na cultura organizacional, a partir de uma abordagem responsiva, da corregulação ou autorregulação regulada, da governança nodal, da prestação de contas e *accountability*. Pressupostos presentes também na Lei Geral de Proteção de Dados (LGPD).

As técnicas já expostas tem o condão de impactar a estrutura das Organizações pois, constituem meios para a implementação de uma Governança e de uma Gestão baseada na melhoria contínua, também vindicando mudança de paradigmas.

A importância da adequação das Organizações à LGPD, em particular, da Administração Pública sobretudo na era do Governo Digital com a consequente prestação digital de serviços públicos se dá, não apenas, pela necessidade de estrita observância à lei, mas também em razão dos possíveis danos reputacionais.

Não se pode olvidar que, “para além das tradicionais sanções administrativas admoestativas (advertência), pecuniárias (multas) e restritivas de atividades (bloqueio ou eliminação dos dados pessoais a que se refere a infração), a lei introduz também sanção com impactos reputacionais, ao prever, no art. 52, IV, a possibilidade de ‘publicização da infração após devidamente apurada e confirmada a sua ocorrência” (WIMMER, 2021).

Ademais, a responsabilização e a prestação de contas são princípios insculpidos na LGPD e referem-se a "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas" (BRASIL, 2018), de acordo com o inciso X do art. 6º.

Tanto os princípios quanto as sanções são aplicáveis a Administração Pública. A bem da verdade, as disposições estatuídas na norma de proteção de dados se aplicam as entidades do Poder Público.

O documento denominado *We need talk about data: Framing the debate around free flow of data and data sovereignty*, em português Precisamos falar sobre dados: enquadrando o debate em torno do livre fluxo de dados e soberania de dados, emitido pela *The Internet & Jurisdiction Policy Network*, organização multi *stakeholder* atuante no ciberespaço, revela aspectos a ser considerados nos debates que envolvem dados pessoais. Senão Vejamos:

> The unusual characteristics of data: the massive volumes at stake, its non-rivalrous nature, the inherently transnational aspects, and the complexity of its value chains.
> The diversity of uses across all sectors: this matters more than the purely technical transport or storage and processing locations.
> Analogies should be used wisely: Analogies are useful to approach unfamiliar situations related to data, but taking them too literally can lead to misguided policy choices.
> Legitimate concerns must be addressed: They overlap security, economic and human rights dimensions, as consequences of growing digital interdependence.
> Implementation pitfalls should be considered: The devil is in the details, unilateral measures concerning data can have unintended consequences and their generalization may be damaging[20] (De La Chapelle, B. and L. Porciuncula, 2021, p. 51).

Depreende-se que as problemáticas pontuadas perpassam a necessária identificação da categoria dos dados, a finalidade do seu tratamento e a avaliação de riscos. Em suma, o impacto do tratamento de dados pessoais não só no ambiente organizacional, mas também na sociedade.

---

20 As características incomuns dos dados: os grandes volumes em jogo, sua natureza não rival, os aspectos inerentemente transnacionais e a complexidade de suas cadeias de valor. A diversidade de usos em todos os setores: isso importa mais do que o transporte puramente técnico ou os locais de armazenamento e processamento. As analogias devem ser usadas com sabedoria: as analogias são úteis para abordar situações desconhecidas relacionadas aos dados, mas interpretá-las muito literalmente pode levar a escolhas políticas equivocadas. Preocupações legítimas devem ser abordadas: elas se sobrepõem às dimensões de segurança, economia e direitos humanos, como consequências da crescente interdependência digital. As armadilhas da implementação devem ser consideradas: o diabo está nos detalhes, medidas unilaterais sobre dados podem ter consequências não intencionais e sua generalização pode ser prejudicial (tradução livre).

O documento também apresenta alguns objetivos que contribuem para o debate e até mesmo para a implementação de uma Política de Proteção aos Dados Pessoais. Vejamos:

> Maximizing the wellbeing of individuals and societies, with a fair distribution of economic and social benefits, and obligations.
> Addressing concrete issues and bridging currently separated silos that prevent the understanding of interrelations between sectoral approaches.
> Defining the distribution of responsibilities among actors regarding who can prescribe, adjudicate, and enforce rules to organize the Datasphere[21] (De La Chapelle, B. and L. Porciuncula, 2021, p. 52).

Assim, o foco no bem estar social, na análise *case by case* e a atribuição e distribuição de responsabilidades para as partes interessadas são indicadores que viabilizam o debate acerca dos dados pessoais na perspectiva da mudança de paradigmas nas Organizações.

À face do exposto, nota-se ainda relutância por parte da Administração Pública no que diz respeito aos cuidados no tratamento de dados pessoais. Nota-se ainda a baixa adesão de Governança dentro das instituições públicas, conforme se extrai do Relatório do TCU sobre LGPD.

Em vista disso, defende o presente trabalho, a necessidade de implementação – não sua possibilidade – de uma Política de Governança, de boas práticas, de segurança da informação e *compliance*, baseadas na autorresponsabilidade de cada servidor, inclusive do dirigente máximo do órgão; no fiel cumprimento das leis; na criação de um código de conduta a ser seguido por todos os membros da instituição; no fortalecimento dos canais de denúncia com prazo razoável de resposta; na difusão de boas práticas entre setores e até mesmo, entre instituições e na aplicabilidade das sanções ante descumprimento de normas de conduta ou legais.

Quanto a este último aspecto, cumpre destacar a necessidade de resguardar a ANPD a aplicação de multa ao poder público em face do descumprimento da LGPD. Até porque o setor público não se encontra em situação similar a iniciativa privada, isto é, detém privilégios, não aufere lucro (em regra), não sofre sanções de ordem moral, haja vista ausência de competitividade, tampouco se preocupa com questões reputacionais.

21 Maximizar o bem-estar dos indivíduos e das sociedades, com uma distribuição justa dos benefícios econômicos e sociais e das obrigações. Abordar questões concretas e colmatar silos atualmente separados que impedem a compreensão das interrelações entre abordagens setoriais. Definir a distribuição de responsabilidades entre os atores sobre quem pode prescrever, adjudicar e fazer cumprir as regras para organizar a *Datasphere* (tradução livre).

Qual seria o meio mais eficaz para a Administração Pública agir em respeito ao direito fundamental da proteção de dados pessoais? Responde-se: o fator financeiro. A possibilidade de aplicação de multa surge como meio mais eficiente não só para coibi-la, mas também para incentivá-la a promover os meios necessários a implementação da LGPD assegurando, ainda, o acesso público à informação, à publicidade e à cibertransparência.

Portanto, para que sejam efetivados os direitos/deveres abordados no presente trabalho, necessário pois, que cada servidor compreenda o processo organizacional do órgão o qual faz parte, entenda se este órgão lida com dados abertos, dados pessoais e/ou dados pessoais sensíveis; realize o tratamento conforme assegurado na respectiva lei e demais documentos normativos ou não, que possam contribuir no processo organizacional e limite os servidores responsáveis pelo tratamento de dados pessoais concedendo-lhe atribuições e responsabilidades com a possibilidade de aplicação de penalidades em caso de descumprimento.

Em suma, necessário que os servidores conheçam as leis pertinentes a sua área de atuação, tais como a LGPD e a Lei de Acesso à Informação, busque aprimoramento sobre os temas em cursos e especializações, difunda o conhecimento agregado para os demais servidores atuantes e vice-versa, e, sobretudo, entenda suas responsabilidades dentro da Organização.

Somente assim, será possível respeitar os deveres constitucionalmente consagrados, implementar Política de Governança, de Governança de Dados, do *compliance*, adotar e difundir boas práticas e respeitar as normas de segurança da informação.

4 CONSIDERAÇÕES FINAIS

Ante o desenvolvimento de novas tecnologias disruptivas oriundas da Quarta Revolução Industrial, também conhecida por Revolução Digital com a consequente quebra das barreiras físicas, a sociedade passa por importantes mudanças que reverberam o cenário social, cultural, econômico e ambiental.

Nessa conjuntura, não cabe repelir ou abolir as novas tecnologias, mas sim de incluí-las na sociedade com vistas ao desenvolvimento humano sustentável. O ser humano não serve a tecnologia, em verdade, a tecnologia serve para melhorar a vida do ser humano. Reconhecer essa premissa não importa a desconsideração das problemáticas decorrentes da má utilização

do aparato tecnológico. Muito pelo contrário, reconhecer essa premissa permite identificar os princípios e os valores que devem permear sua utilização.

Em relação a atuação estatal, emerge a Administração Pública 4.0 ou Administração Pública Digital, especialmente com a promulgação da Lei do Governo Digital, com vistas a prestação digital de serviços públicos e o aumento da eficiência pública.

Ademais, no ciberespaço os deveres constitucionais administrativos devem ser assegurados, sem prejuízo ao respeito de direitos e garantias dos cidadãos. Deve-se assentir a releitura dos direitos deveres outrora positivados, inclusive na Constituição Federal de 1988, bem como a possibilidade de existência de novos direitos e deveres.

É o que ocorre com o direito fundamental à proteção de dados pessoais que, embora as discussões sobre o tema não sejam tão recentes, foi alçado a *status* de direito fundamental no cenário brasileiro pela PEC nº 17/2019 posteriormente convertida na EC nº 115/2022.

É o que ocorre também com o dever de transparência que, em decorrência da prestação digital de serviços públicos, foi nomeado cibertransparência.

Outrossim, o presente trabalho buscou explorar os aspectos da Administração Pública 4.0 na perspectiva da necessária conjugação do direito fundamental à proteção de dados pessoais, com o direito fundamental de acesso público à informação, a publicidade e a cibertransparência.

Para tanto, foram apresentados mecanismos e técnicas que viabilizam o rearranjo das Organizações mediante uma mudança na cultura, numa verdadeira mudança de paradigmas. Dentre as medidas apontou-se o papel da Governança e da Governança de Dados, aliadas à Segurança da Informação, às boas práticas e ao *compliance*.

Dentre as técnicas, o presente trabalhou pontuou a importância do ciclo PDCA, do *benchmarking*, da técnica *5W+1H+SHOW ME*, da abordagem *lean* e do *brainstorming*, cujos objetivos primordiais são o fomento as novas ideias e a difusão do conhecimento mediante a atuação de equipes interdisciplinares e a melhoria contínua na gestão pública, intitulada *New Public Management (NPM)*, em português, “Nova Gestão Pública”.

Portanto, defende-se, não apenas a necessidade de conjugação de deveres e direitos constitucionalmente assegurados, mas também a necessidade de reconhecimento de novos deveres e direitos derivados da Revolução Digital.

Para além disso, defende-se a necessidade de adoção de uma estrutura sólida de Governança no setor público, o que certamente, viabilizará estruturas sólidas de Governança

de Dados, da Segurança da Informação, das boas práticas e de *compliance*, com a cooperação das técnicas outrora analisadas mediante o conhecimento dos processos organizacionais dos órgãos públicos, das leis e de instrumentos não normativos, a exemplo da ISO 27.001 sobre segurança da informação e dos guias orientativos da ANPD com o objetivo de promover uma cultura organizacional que assegure os direitos e os deveres previstos na Constituição Federal de 1988.

REFERÊNCIAS

Ação Penal nº 307-3 DF, Relator: Min. Ilmar Galvão, Data de Julgamento: 01/09/1997, DJ Data de Publicação: 10/09/1997 P-43165.

ALEXY, Robert. **Teoria dos direitos fundamentais**. Tradução de Virgílio Afonso da Silva. São Paulo: Malheiros, 2008.

ASSAD, Frederico Jorge Vaz De Figueiredo; LEITE, Flavia Piva Almeida. Aspectos do direito fundamental à proteção de dados pessoais. XXVII Encontro Nacional do CONPEDI: **Direito, Governança e Novas Tecnologias I**. Porto Alegre – RS: 2018, fls. 187-205. Disponível em: http://site.conpedi.org.br/publicacoes/34q12098/9l053031/55dfpNn0G509WEvB.pdf. Acesso em: 10 jul. 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR *ISO/IEC 27001:* **Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos**. Rio de Janeiro, 2006.

BARROSO, Luís Roberto. **Curso de Direito Constitucional Contemporâneo**: os conceitos fundamentais e a construção do novo modelo. São Paulo: Saraiva, 2010.

BARROSO, Luís Roberto. Neoconstitucionalismo e Constitucionalização do Direito: o triunfo tardio do direito constitucional no Brasil. **Revista de Direito Administrativo**. Rio de Janeiro, 240: p. 01-42, Abr./Jun. 2005. Disponível em: https://bibliotecadigital.fgv.br/ojs/index.php/rda/article/view/43618/44695. Acesso em: 09 nov. 2021.

BATISTA, Fábio Ferreira. **Modelo de gestão do conhecimento para a administração pública brasileira: como implementar a gestão do conhecimento para produzir resultados em benefício do cidadão**. Brasília: Ipea, 2012. Disponível em: http://repositorio.ipea.gov.br/bitstream/11058/754/1/Modelo%20de%20Gest%c3%a3o%20do%20Conhecimento%20para%20a%20Administra%c3%a7%c3%a3o%20P%c3%bablica%20Brasileira.%20Livro.pdf. Acesso em: 10 jul. 2022.

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

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **Guia de Avaliação de Riscos de segurança e privacidade: Lei Geral de Proteção de Dados (LGPD)**. Brasília, DF: ANPD, versão 1.0, novembro de 2020. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_avaliacao_riscos.pdf. Acesso em: 10 jul. 2022.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **Guia de Boas Práticas Lei Geral de Proteção de Dados (LGPD) para implementação na Administração Pública Federal**. Brasília, DF: ANPD, versão 2.0, agosto de 2020. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf. Acesso em: 22 de janeiro de 2023.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **Guia Orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado**. Brasília, DF: ANPD, versão 2.0, abril de 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf. Acesso em: 10 jul. 2021.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **Guia Orientativo sobre tratamento de dados pessoais pelo Poder Público**. Brasília, DF: ANPD, versão 1.0, janeiro de 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 10 jul. 2022.

BRASIL. Ministério da Economia. Brasil está entre os 20 países com melhor oferta de serviços públicos digitais. **Ministério da Economia**. Brasília, 20 de julho de 2020. Disponível em: https://www.gov.br/economia/pt-br/assuntos/noticias/2020/julho/brasil-esta-entre-os-20-paises-com-melhor-oferta-de-servicos-publicos-digitais. Acesso em: 10 jul. 2022.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília, DF: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 11 set. 2021.

BRASIL. Controladoria Geral da União (CGU). **Portal da Transparência**. Disponível em: https://www.portaltransparencia.gov.br/sobre/o-que-e-e-como-funciona. Acesso em 11 nov. 2021.

BRASIL. **Decreto-Lei nº 4.657, de 04 de setembro de 1942**. Lei de Introdução às Normas do Direito Brasileiro. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del4657compilado.htm. Acesso em: 08 jun. 2022.

BRASIL. **Decreto nº 592, de 6 de julho de 1992**. Atos Internacionais. Pacto Internacional sobre Direitos Civis e Políticos. Promulgação. Decreto. Brasília, DF, 7 de julho de 1992. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm. Acesso em: 27 de maio de 2022.

BRASIL. **Decreto nº 5.687, de 31 de janeiro de 2006**. Promulga a Convenção das Nações Unidas contra a Corrupção, adotada pela Assembléia-Geral das Nações Unidas em 31 de

outubro de 2003 e assinada pelo Brasil em 9 de dezembro de 2003. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Decreto/D5687.htm. Acesso em: 27 de maio de 2022.

BRASIL. **Decreto nº 7.724, de 16 de maio de 2012**. Regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7724.htm. Acesso em: 25 de maio de 2022.

BRASIL. **Decreto nº 8.420, de 18 de março de 2015**. Regulamenta a Lei nº 12.846, de 1º de agosto de 2013, que dispõe sobre a responsabilização administrativa de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/decreto/d8420.htm. Acesso em: 10 jul. 2022.

BRASIL. **Decreto nº 8.777, de 11 de maio de 2016**. Institui a Política de Dados Abertos do Poder Executivo Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8777.htm. Acesso em: 27 dez. 2021.

BRASIL. **Decreto nº 8.936, de 19 de dezembro de 2016**. Institui a Plataforma de Cidadania Digital e dispõe sobre a oferta de serviços públicos digitais, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8936.htm. Acesso: em 27 dez. 2021.

BRASIL. **Decreto nº 9.203, de 22 de novembro de 2017**. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Diário Oficial da União, Brasília, 2017a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/decreto/d9203.htm. Acesso em: 07 de maio de 2022.

BRASIL. **Decreto nº 9.319, de 21 de março de 2018**. Institui o Sistema Nacional para a Transformação Digital e estabelece a estrutura de governança para a implantação da Estratégia Brasileira para a Transformação Digital. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9319.htm. Acesso em: 27 dez 2021.

BRASIL. **Decreto nº 9.637, de 26 de dezembro de 2018**. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, *caput*, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/56970098/do1-2018-12-27-decreto-n-9-637-de-26-de-dezembro-de-2018-56969938. Acesso em: 27 dez. 2021.

BRASIL. **Decreto nº 9.690, de 23 de janeiro de 2019**. Altera o Decreto nº 7.724, de 16 de maio de 2012, que regulamenta a Lei nº 12.527, de 18 de novembro de 2011 – Lei de Acesso à Informação. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d9690.htm. Acesso em: 28 de maio de 2021.

BRASIL. **Decreto nº 9.756, de 11 de abril de 2019**. Institui o portal único "gov.br" e dispõe sobre as regras de unificação dos canais digitais do Governo federal. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9756.htm. Acesso em: 27 dez. 2021.

BRASIL. **Decreto nº 9.854, de 25 de junho de 2019**. Institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9854.htm. Acesso em: 10 jul. 2022.

BRASIL. **Decreto nº 10.046, de 09 de outubro de 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 27 dez. 2021.

BRASIL. **Decreto nº 10.160, de 09 de dezembro de 2019**. Institui a Política Nacional de Governo Aberto e o Comitê Interministerial de Governo Aberto. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d10160.htm. Acesso em: 08 de maio de 2022.

BRASIL. **Decreto nº 10.332, de 28 de abril de 2020**. Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10332.htm. Acesso em: 27 dez. 2021.

BRASIL. **Lei Complementar nº 101, de 04 de maio de 2000**. Estabelece normas de finanças públicas voltadas para a responsabilidade na gestão fiscal e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp101.htm. Acesso em: 08 jun. 2022.

BRASIL. **Lei Complementar nº 166, de 8 de abril de 2019**. Altera a Lei Complementar nº 105, de 10 de janeiro de 2001, e a Lei nº 12.414, de 9 de junho de 2011, para dispor sobre os cadastros positivos de crédito e regular a responsabilidade civil dos operadores. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/LCP/Lcp166.HTM. Acesso em: 27 de maio de 2022.

BRASIL. **Lei nº 8.078, de 12 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm. Acesso em: 25 de maio de 2022.

BRASIL. **Lei nº 8.666, de 21 de junho de 1993**. Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8666cons.htm. Acesso em: 08 jun. 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*. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9507.htm. Acesso em 25 de maio de 2022.

BRASIL. **Lei nº 9.784, de 29 de janeiro de 1999**. Regula o processo administrativo no âmbito da Administração Pública. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9784.htm. Acesso em: 08 jun. 2022.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 10 jul. 2022.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do artigo 5º, no inciso II do & 3º do art. 37 e no & 2º do art.216 da Constituição Federal; altera a Lei n. 8.112, de 11 de dezembro de 1990; revoga a lei n.11.111, de 5 de maio de 2005, e dispositivos da Lei n. 8.159,de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em 25 de maio de 2022.

BRASIL. **Lei nº 12.965, de 24 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 27 de maio de 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 30 de maio de 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. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm. Acesso em: 27 dez. 2021.

BRASIL. **Medida Provisória nº 928, de 23 de março de 2020**. Altera a Lei nº 13.979, de 6 de fevereiro de 2020, que dispõe sobre as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019, e revoga o art. 18 da Medida Provisória nº 927, de 22 de março de 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Mpv/mpv928.htm. Acesso em: 25 de maio de 2022.

BRASIL. **Medida Provisória nº 954, de 17 de abril de 2020**. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Disponível em: https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/141619. Acesso em: 30 de maio de 2022.

BRASIL. Senado Federal. **Projeto de Lei nº 3, de 2019**. Susta a aplicação do Decreto nº 7.724, de 16 de maio de 2012, no que diz respeito à delegação da competência de classificação de informações públicas nos graus de sigilo ultrassecreto ou secreto. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135454. Acesso em: 07 jun. 2022.

BRASIL. Senado Federal. **Projeto de lei nº 6212 de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), para dispor sobre a corregulação. Disponível em: https://legis.senado.leg.br/sdleg-getter/documentodm=8049526&ts=1575650467579&disposition=inline. Acesso em: 09 jun. 2022.

BRASIL. Senado Federal. **Proposta de Emenda à Constituição nº 17, de 2019**. Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm. Acesso em: 30 de maio de 2022.

BRASIL. Superior Tribunal de Justiça, 2ª Seção. **REsp 1419697/RS**, Rel. Ministro PAULO DE TARSO SANSEVERINO, j. em 12/11/2014. Disponível em: http://https://bdjur.stj.jus.br/jspui/bitstream/2011/114173/REsp1419697.pdf. Acesso em: 31 de maio de 2022

BRASIL. Supremo Tribunal Federal. **Ação Originária nº 2.367**. Relator Ministro Luís Roberto Barroso, Brasília, 23 de agosto de 2018.

BRASIL. Supremo Tribunal Federal. **Mandado de Segurança nº 21729-4-DF**, Relator: Min. MARCO AURÉLIO, Relator p/ Acórdão: Min. NÉRI DA SILVEIRA, Tribunal Pleno, julgado em 05/10/1995, DJ 19-10-2001 PP-00033 EMENT VOL-02048-01 PP-00067 RTJ VOL-00179-01 PP-00225. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=85599. Acesso em: 11 set. 2021.

BRASIL. Supremo Tribunal Federal. **Medida Cautelar na Ação Direta de Inconstitucionalidade 6387-DF**. Medida Provisória 954/2020. Requerente: Conselho Federal da Ordem dos Advogados do Brasil. Relatora: Min. Rosa Weber, 24 de abril de 2020. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629. Acesso em: 30 de maio de 2022.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 71.652**. Relator Ministro Thompson Flores, Brasília, 24 de maio de 1971.

BRASIL. Supremo Tribunal Federal. **RE: 418416 SC**, Relator: Min. SEPÚLVEDA PERTENCE, Data de Julgamento: 10/05/2006, Tribunal Pleno, Data de Publicação: DJ 19-12-2006 PP-00037 EMENT VOL-02261-06 PP-01233. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=500962. Acesso em: 11 set. 2021.

BRASIL. Supremo Tribunal Federal. **Resolução nº 724, de 02 de março de 2021**. Institui o Comitê Executivo de Proteção de Dados para identificar e implementar as medidas necessárias à adequação do Supremo Tribunal Federal às exigências da Lei n. 13.709, de 14 de agosto de 2019 (Lei Geral de Proteção de Dados – LGPD). Disponível em: http://stf.jus.br/ARQUIVO/NORMA/RESOLUCAO724-2021.PDF. Acesso em: 31 de maio de 2022.

BRASIL. Tribunal de Contas da União (TCU). **Acórdão 1384/2022**. Plenário. Relator: Augusto Nardes. Sessão de 15/06/2022. Disponível em: https://portal.tcu.gov.br/data/files/B4/25/78/27/D9C818102DFE0FF7F18818A8/038.172-2019-4-AN%20-%20auditoria_Lei%20Geral%20de%20Protecao%20de%20Dados.pdf. Acesso em: 10 jul. 2022.

BRASIL. Tribunal de Contas da União (TCU). **Referencial básico de governança: aplicável a órgãos e entidades da administração pública**. Brasília: TCU; Secretaria de Planejamento, Governança e Gestão, 2014. Disponível em: https://portal.tcu.gov.br/data/files/FA/B6/EA/85/1CD4671023455957E18818A8Referencial_basic_governanca_2_edicao.PDF. Acesso em: 07 de maio de 2022.

BRASIL. Tribunal de Contas da União (TCU). **Técnicas de Auditoria: Benchmarking**. Brasília: TCU, Coordenadoria de Fiscalização e Controle, 2000.

CARVALHO, Artur Potiguara; PEIXOTO, Fabiano Hartmann; CARVALHO, Fernanda Potiguara. Governança de dados aplicada ao big data analytics: a necessidade de gestão dos dados em big data para além da LGPD. **Direito, governança e novas tecnologias II** [Recurso eletrônico online] organização CONPEDI; Coordenadores: Danielle Jacon Ayres Pinto; Ayres Jose Rover, Fabiano Hartmann Peixoto – Florianopólis: CONPEDI, 2020. Disponível em: http://conpedi.danilolr.info/publicacoes/olpbq8u9/lxxdq7f2/nC0tdO80Ds5cd8Zv.pdf. Acesso em: 10 jul. 2022.

CASA CIVIL DA PRESIDÊNCIA DA REPÚBLICA. **Guia da política de governança pública**. Brasília: Casa Civil da Presidência da República, 2018. Disponível em: https://www.gov.br/casacivil/pt-br/centrais-de-conteudo/downloads/guia-da-politica-de-governanca-publica. Acesso em: 07 de maio de 2022.

CASTELLS, Manuel. **A sociedade em rede** (A era da informação, economia, sociedade e cultura). 6 ed. São Paulo: Paz e Terra, 1999.

CASTELLS, Manuel. **A galáxia da Internet: reflexões sobre a Internet, os negócios e a sociedade**. Rio de Janeiro: J. Zahar, 2003.

CONSELHO DA EUROPA. **Convenção para a Proteção dos Indivíduos com relação ao Processamento de Dados Pessoais (Convenção 108)**, 1981. Disponível em: https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf. Acesso em: 10 de jul. 2022.

CUNHA, Paulo Roberto da. Direito e sociedade: democracia, política e transparência – o acesso as informações na perspectiva da sociedade. **Direitos e garantias fundamentais I** [Recurso eletrônico online] organização CONPEDI/UNICURITIBA; Coordenadores: Carlos Alberto Simões de Tomaz, Eloy Pereira Lemos Junior, Rui Decio Martins – Florianopólis: CONPEDI, p. 78-93, 2016. Disponível em: http://site.conpedi.org.br/publicacoes/02q8agmu/z23nop3l/7h2C7N7sVda5ZlPA.pdf. Acesso em: 10 jul. 2022.

CÚPULA IBERO-AMERICANA DE CHEFES DE ESTADO E DE GOVERNO. **Declaração de Santa Cruz de La Sierra**. Aprovada na XIII Cúpula Ibero-americana de Chefes de Estado e de Governo, Santa Cruz de La Sierra, 2003. Disponível em: https://www.segib.org/wp-content/uploads/DECLARASAO-STA-CRUZ-SIERRA.pdf. Acesso em: 13 set. 2021.

DECLARAÇÃO DE PRINCÍPIOS SOBRE LIBERDADE DE EXPRESSÃO, 2000. Disponível em: http://www.cidh.oas.org/basicos/portugues/s.Convencao.Libertade.de.Expressao.htm. Acesso em: 27 de maio de 2022.

DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS, 1948. Disponível em: https://brasil.un.org/sites/default/files/2020-09/por.pdf. Acesso em: 27 de maio de 2022.

DE LA CHAPELLE, B. AND L. PORCIUNCULA. **We Need to Talk About Data: Framing the Debate Around Free Flow of Data and Data Sovereignty**. Internet and Jurisdiction Policy Network, 2021. Disponível em: https://www.internetjurisdiction.net/uploads/pdfs/We-Need-to-Talk-About-Data-Framing-the-Debate-Around-the-Free-Flow-of-Data-and-Data-Sovereignty-Report-2021.pdf. Acesso em: 10 jul. 2022.

DIAS, Clara Angélica Gonçalves Cavalcanti; SILVA, Raquel Torres de Britto. A aplicabilidade dos direitos fundamentais sob a ótica horizontal: um supino fruto do constitucionalismo democrático contemporâneo. **Revista Eletrônica da Procuradoria Geral do Estado do Rio de Janeiro** – PGE-RJ, Rio de Janeiro, v.3, n.1, 2020.

DI PIETRO, Maria Sylvia Zanella. **Direito Administrativo**. 33. ed. – Rio de Janeiro: Forense, 2020.

DONEDA, Danilo Cesar Maganhoto. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law**, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 05 jun. 2022.

DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais** [livro eletrônico]: elementos da formação da Lei Geral de Proteção de Dados / Danilo Cesar Maganhoto Doneda. -- 2. ed. -- São Paulo: Thomson Reuters Brasil, 2020.

FLÔRES, Mariana Rocha de; SILVA, Rosane Leal da. Desafios e perspectivas da proteção de dados pessoais sensíveis em poder da Administração Pública: entre o dever público de informar e o direito do cidadão de ser tutelado. **Revista de Direito**, Viçosa, v. 12, n. 02, 2020.

FONSECA, Edson Pires da. **Lei Geral de Proteção de Dados Pessoais** – LGPD. Salvador: Editora JusPodivm, 2021.

FRAGA, Vanessa de Souza. **Governança de Dados na transformação digital: A Governança de Dados na Administração Pública**. Fundação Escola Nacional de Administração Pública (ENAP), Diretoria de Desenvolvimento Profissional. Brasília: ENAP, 2022.

G1. **Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber**. 28 jan. 2021. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml. Acesso em: 25 mar. 2023.

GABRIEL, Martha. **Você, eu e os robôs: pequeno manual do mundo digital**. – [3. Reimpr.]. São Paulo: Atlas, 2019.

HARARI, Yuval Noah. **21 lições para o século 21**. São Paulo: Companhia das Letras, 2018.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). **Código das melhores práticas de governança corporativa**. 5.ed. / Instituto Brasileiro de Governança Corporativa. - São Paulo, SP: IBGC, 2015. Disponível em: https://edisciplinas.usp.br/pluginfile.php4382648mod_resource/contentLivro_Codigo_Melhores_Praticas_GC.pdf. Acesso em: 07 de maio de 2022.

IRAMINA, Aline. RGPD v. LGPD: Adoção Estratégica da Abordagem Responsiva na Elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento Geral de Proteção de Dados da União Europeia. **Revista de Direito, Estado e Telecomunicações**, Brasília, v. 12, nº 2, p. 91-117, Outubro de 2020.

LÉVY, Pierre. **Cibercultura**. Tradução por Carlos Irineu da Costa. São Paulo: Ed. 34, 1999.

LIMA, Eduardo de Souza. **Abordagem *lean* aplicada à transformação digital na Administração Pública**. Fundação Escola Nacional de Administração Pública (ENAP), Diretoria de Desenvolvimento Profissional. Brasília: ENAP, 2022.

LIMBERGER, Têmis. **Cibertransparência: informação pública em rede: a virtualidade e suas repercussões na realidade**. Porto Alegre: Livraria do Advogado, 2016.

MEIRELLES, Hely Lopes. **Direito Administrativo Brasileiro**. 42 ed. atual. até a Emenda Constitucional 90, de 15.9.2015. - São Paulo: Malheiros, 2016.

MELLO, Celso Antônio Bandeira de. **Curso de Direito Administrativo**. 32 ed. atual. até a Emenda Constitucional 84, de 2.12.2014. São Paulo: Editora Malheiros, 2015.

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. Pensar, **Revista de Ciências Jurídicas**, Fortaleza, v. 25, n. 4, p. 1-18, out./dez. 2020.

NOHARA, Irene Patrícia. **Direito Administrativo**. 9 ed. São Paulo: Atlas, 2019.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS (OEA). **Lei Modelo sobre Acesso à Informação Pública 2.0** / [Preparado pelo Departamento de Direito Internacional da Secretaria de Assuntos Jurídicos da OEA], 2020. Disponível em: http://www.oas.org/en/sla/dil/docs/Publicacao_Lei_Modelo_Interamericana_2_0_Acesso_Informacao_Publica.pdf. Acesso em: 27 de maio de 2022.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). **Síntese Diretrizes da OCDE para a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais**, 1980. Disponível em: https://www.oecd.org/sti/ieconomy/15590254.pdf. Acesso em: 10 jul. 2022.

PALUDO, Augustinho. **Administração Pública**. 10. ed. rev. ampl. E atual. - São Paulo: Editora JusPodivm, 2022.

PARLAMENTO EUROPEU. **Carta de Direitos Fundamentais da União Europeia, de 7 de dezembro de 2000**. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 12 set. 2021.

PEREIRA, José Matias. **Curso de Administração Pública: foco nas instituições e ações governamentais**. 4.ed. São Paulo: Atlas, 2014.

PETER, Maria da Glória Arrais; MACHADO, Marcus Vinícius Veras. **Manual de Auditoria Governamental**. 2. ed. São Paulo: Editora Atlas, 2014.

RIO GRANDE DO SUL. Tribunal de Justiça. **Apelação Cível Nº 70069420503**. Sexta Câmara Cível. Comercialização de dados cadastrais de consumidores. Apelante: Confederação Nacional de Dirigentes Lojistas (SPC Brasil); SERASA S.A. Apelado: Ministério Público. Relator: Ney Wiedemann Neto, Porto Alegre, 25 de agosto de 2016. Disponível em: https://tj-rs.jusbrasil.com.br/jurisprudencia/899195030/apelacao-civel-ac-70069420503-rs/inteiro-teor-899195093. Acesso em: 31 de maio de 2022.

SAAVEDRA, Giovani Agostini. *Compliance* de Dados. In: **Tratado de proteção de dados pessoais** / coordenadores Danilo Doneda ... [et al.].– Rio de Janeiro: Forense, 2021.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional**. 13. ed. rev. e atual. - Porto Alegre: Livraria do Advogado, 2018.

SARMENTO, Daniel. **Dignidade da pessoa humana: conteúdo, trajetórias e metodologia**. Belo Horizonte: Fórum, 2016.

SCHWAB, Klaus. **A quarta revolução industrial**. Trad. Daniel Moreira Miranda. São Paulo: Edipro, 2016.

SIQUEIRA, Eva Cecília Trindade; MACHADO, Carlos Augusto Alcântara. O Ministério Público como instituição de fomento ao direito fundamental de acesso à informação no âmbito das entidades sem fins lucrativos. **Revista Brasileira de Direitos e Garantias Fundamentais**. | Evento Virtual | v. 6 | n. 1 | p. 36-52 | Jan/Jun. 2020.

UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR)**, 2016. Disponível em: https://gdpr-info.eu/. Acesso em: 10 jul. 2022.

WIMMER, Miriam. Desafios do *enforcement* na LGPD: Fiscalização, aplicação de sanções administrativas e coordenação intergovernamental. In: **Tratado de proteção de dados pessoais** / coordenadores Danilo Doneda ... [et al.].– Rio de Janeiro: Forense, 2021.