FACULDADE DE DIREITO DE VITÓRIA
MESTRADO EM DIREITOS E GARANTIAS FUNDAMENTAIS

LETÍCIA FRAGA DE FIGUEIREDO

O EMPODERAMENTO TECNOLÓGICO DO ESTADO DE VIGILÂNCIA FRENTE AO DIREITO CONSTITUCIONAL À PRIVACIDADE E À PROTEÇÃO DE DADOS: A COLETA E O TRATAMENTO DE DADOS PESSOAIS COMO INSTRUMENTO DE CONTROLE

VITÓRIA
2021

LETÍCIA FRAGA DE FIGUEIREDO

O **EMPODERAMENTO TECNOLÓGICO DO ESTADO DE VIGILÂNCIA FRENTE AO DIREITO CONSTITUCIONAL À PRIVACIDADE E À PROTEÇÃO DE DADOS:** A COLETA E O TRATAMENTO DE DADOS PESSOAIS COMO INSTRUMENTO DE CONTROLE

Dissertação apresentada ao Programa de Pós-graduação Stricto Sensu em Direitos e Garantias Fundamentais da Faculdade de Direito de Vitória (FDV) como requisito para obtenção de grau em Mestre em Direito.
Orientador: Prof. Dr. Américo Bedê Freire Junior.

VITÓRIA
2021

LETÍCIA FRAGA DE FIGUEIREDO

O EMPODERAMENTO TECNOLÓGICO DO ESTADO DE VIGILÂNCIA FRENTE AO DIREITO CONSTITUCIONAL À INTIMIDADE, À VIDA PRIVADA E À PROTEÇÃO DE DADOS: A COLETA E O TRATAMENTO DE DADOS PESSOAIS COMO INSTRUMENTO DE CONTROLE

Dissertação apresentada ao Programa de Pós Graduação Stricto Sensu em Direitos e Garantias Fundamentais da Faculdade de Direito de Vitória (FDV) como requisito para obtenção de grau em Mestre em Direito.

Aprovada em 18 de agosto de 2021.

COMISSÃO EXAMINADORA

_____

Prof. Dr. Américo Bedê Freire Junior.
Faculdade de Direito de Vitória (FDV)
Orientador

_____

Prof. Dr. Cassius Guimarães Chai
Faculdade de Direito de Vitória (FDV)

_____

Profa. Dra. Andréa Walmsley Soares Carneiro
Faculdade Damas da Instrução Cristã

AGRADECIMENTOS

O percurso trilhado pelo pesquisador nem sempre é linear, vários foram os desafios vencidos ao longo desses 02 (dois) anos e o breve resumo de tudo que foi investigado durante esse período está consolidado com a dissertação.

Apesar da pesquisa ser muitas vezes um trabalho solitário, devo ressaltar aqueles que estiveram ao meu lado.

Agradeço à Deus, por me conceder saúde e sabedoria para seguir sempre em frente. Obrigada por ser a minha força e o meu guia em todos os momentos. De modo a fortalecer e incutir-me a confiança necessária para crer que, mesmo em meio às adversidades, a vitória se dá pela persistência.

Agradeço à minha família, pai, mãe e irmã pelo apoio e incentivo em todos os momentos da minha vida. Por acreditarem em mim, e não medirem esforços para a concretização dos meus sonhos. Sem vocês, nada seria possível.

Ao meu noivo Thiago, por ser compreensivo quanto as minhas ausências necessárias para que eu pudesse estudar e me dedicar ao mestrado.

Ao meu orientador querido, o Professor Doutor Américo Bedê Freire Junior, agradeço a acolhida desde o princípio. Pelo entendimento, bom senso, educação, competência ímpar, e por toda a disponibilidade de sempre. Agradeço também os membros do Programa de Pós-graduação da FDV pelo suporte, em especial aos professores do programa cujos ensinamentos foram muitos e certamente contribuíram positivamente para a minha formação.

Agradeço aos membros da banca examinadora, pelo interesse e disponibilidade.

E claro, aos meus alunos, pelos ensinamentos diários. Foram eles o meu grande estímulo nesta caminhada.

To the future or to the past, to a time when thought is free, when men are different from one another and do not live alone - to a time when truth exists and what is done cannot be undone: From the age of uniformity, from the age of solitude, from the age of Big Brother, from the age of doublethink - greetings!

(George Orwell, 1984)

RESUMO

O intuito deste trabalho é de conhecer e analisar os riscos frequentemente denunciados de um estado de vigilância, incubados em nossa sociedade por certos usos da tecnologia da informação e outros medos coletivos. A dissertação divide-se em cinco capítulos. O primeiro capítulo se dedica ao estudo das distopias e obras literárias que representam a clássica tríade de romances distópicos: Admirável Mundo Novo, 1984 e Fahrenheit 451 e como tais obras refletem sociedades dominadas pelo controle, poder e vigilância. Já o segundo capítulo se aprofunda na sociedade de vigilância idealizada por Michael Foucault, além de apresentar reflexões, a partir de casos concretos, acerca dicotomia entre a incolumidade pública e o direito à privacidade e liberdades individuais dos usuários. O terceiro e quarto capítulos se debruçam sobre a temática da proteção de dados pessoais, apresentando paradigmas norteadores e, como tal proteção se distancia do princípio da privacidade e se torna um princípio autônomo, bem como de que forma essa proteção se estrutura dentro do ordenamento jurídico brasileiro. Traz-se ainda o debate acerca da Medida Provisória nº 954/2020 e seus desdobramentos jurídicos. Por fim, o quinto capítulo se propõe a discutir sobre a governança responsável de dados e a necessidade de implementação de procedimentos legais nas operações de tratamento dos dados pessoais baseadas na transparência e integridade. Ao final sugere-se que a prática da boa governança funcione como ferramenta inibitória de atos relacionados à violação do direito à privacidade e o direito à proteção de dados.

Palavras-chave: Surveillance Status. Dystopia. Control. Technology. Protection of Personal Data. Data governance.

ABSTRACT

The purpose of this paper is to know and analyze the frequently reported risks of a state of surveillance, incubated in our society by certain uses of information technology and other collective fears. The dissertation is divided into five chapters. The first chapter is dedicated to the study of dystopias and literary works that represent the classic triad of dystopian novels: Brave New World, 1984 and Fahrenheit 451 and how such works reflect societies dominated by control, power and surveillance. The second chapter goes deeper into the surveillance society conceived by Michael Foucault, in addition to presenting reflections, based on concrete cases, about the dichotomy between public safety and the users' right to privacy and individual freedoms. The third and fourth chapters focus on the theme of personal data protection, presenting guiding paradigms and, as such protection distances itself from the principle of privacy and becomes an autonomous principle, as well as how this protection is structured within the legal system Brazilian. It also brings the debate about Provisional Measure No. 954/2020 and its legal consequences. Finally, the fifth chapter aims to discuss responsible data governance and the need to implement legal procedures in personal data processing operations based on transparency and integrity. In the end, it is suggested that the practice of good governance works as a tool to inhibit acts related to the violation of the right to privacy and the right to data protection.

Key-words: Surveillance. Control. Technology. Personal Data Protection. Pandemic. Dystopia. Surveillance state.

SUMÁRIO

CONSIDERAÇÕES INICIAIS

A sociedade de vigilância idealizada por Michael Foucault em sua obra Vigiar e Punir, caracterizada por um conjunto de ferramentas institucionais e sociais que legitimam a vigilância sobre os indivíduos, evidencia o uso de mecanismos de vigilância como forma de controle de comportamentos e posicionamentos sociais dos vigiados.

Juntamente aos mecanismos de controle social, agrega-se a revolução tecnológica na medida em que potencializa e aperfeiçoa tais mecanismos.

Sob essa perspectiva, na atual sociedade de vigilância, é perceptível o uso de novas tecnologias de comunicação e monitoramento, nas quais os dados pessoais são coletados e tratados sem, necessariamente, a participação, ingerência ou controle dos titulares ao longo desse processo, tais questões são agravadas em momentos de crise, isto porque, o acesso em tempo hábil a dados relevantes pela Administração Pública torna-se primordial quando se trata de gestão de crise.

Stefáno Rodotà constata que, após o atentado às Torres Gêmeas de 11 de setembro de 2001 nos Estados Unidos da América, as dimensões jurídicas acerca da privacidade foram afrouxadas e o mercado, aproveitando-se desse processo de relativização de garantias, criou oportunidades tecnológicas de mecanismos para a captação, triagem e manipulação de dados pessoais para controle de indivíduos[1].

Assim como em 2001, a pandemia causada pelo novo Coronavírus reacendeu a discussão acerca da relativização da privacidade, na medida em que a saúde pública reivindica o uso de tecnologia, notadamente a digital, como estratégia para prevenção e combate à crise sanitária. Nesse contexto, se de um lado, há a imperiosa necessidade de aplicação de todos os meios necessários para controle e combate à pandemia, utilizando-se, assim, de todos os recursos, inclusive os tecnológicos, na tentativa de impedir a propagação da doença. Do outro, há uma preocupação

[1]RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 13.

envolvendo possíveis riscos de abuso estatal decorrentes da implementação de mecanismos de controle e vigilância constantes.

Com vistas a minimizar os efeitos do contágio pelo Coronavírus, diversos países lançaram mão de tecnologias de geolocalização, como principal estratégia para interromper a proliferação da doença, com isso garantiu-se a rápida identificação e quarentena dos indivíduos infectados, bem como a determinação com quem estes tiveram contato próximo nos dias e semanas anteriores, descontaminação dos locais visitados pelo indivíduo infectado e alocação de recursos (mão de obra e suprimentos), para isto, através do mapeamento e cruzamento de dados randomizados de telefonia móvel.

No Brasil, a Medida Provisória nº 954, de 17 de abril de 2020[2] dispunha sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado (STFC) e de Serviço Móvel Pessoal (SMP) com a Fundação Instituto Brasileiro de Geografia e Estatística (IBGE), 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.

Cumpre mencionar que a aludida MP teve sua eficácia suspensa pelo Supremo Tribunal Federal, na medida em que a Corte Constitucional entendeu que o compartilhamento previsto na espécie normativa violava o direito constitucional à intimidade, à vida privada e à proteção de dados, sendo, portanto, inconstitucional (STF, 2020). Logo, os direitos fundamentais emergem como limites a serem observados na condução do Estado, especialmente no que tange à contenção de crises, sejam elas, políticas, de segurança e sanitárias, onde poderá ocorrer a mitigação de direitos.

A problemática surge na medida em que, com a implementação de um estado de vigilância que lança mão do rastreamento de contatos em massa pode haver a colisão entre direitos fundamentais, como a incolumidade pública e os limites do direito à

[2] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm

privacidade e à proteção de dados pessoais. Logo, vem à baila a seguinte indagação: é possível compatibilizar os direitos fundamentais, notadamente a incolumidade pública e o direito à privacidade e à proteção de dados, especialmente em situações de crise, em que ocorre com maior frequência o emprego de meios tecnológicos pelo Estado?

À vista disso, com a disponibilidade quase onipresente de telefones inteligentes – *smartphones* que contém, se não todos, grande parte dos dados pessoais dos titulares, garantir a segurança de dados e a privacidade dos usuários desafia a tecnologia, incluindo as de rastreamento de informações. Isto porque o monitoramento e as intervenções tecnológicas baseadas na coleta e tratamento de dados, além de *taguear* os indivíduos, pode se revelar uma violação aos direitos fundamentais, principalmente a privacidade e as liberdades individuais, sobretudo em momentos de crises, cobertos por incertezas e inseguranças jurídicas.

Nos moldes atuais, a Lei Geral de Proteção de Dados (LGPD)[3] traz disposições acerca da coleta, tratamento e compartilhamento de dados pessoais, por pessoas físicas e jurídicas, e, prevê em seu Capítulo IV sobre o tratamento de dados pessoais pelo Poder Público. Nesse sentido, o artigo 26 da referida lei informa que o uso compartilhado de dados pessoais deverá atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e entidades públicas devendo a atividade de tratamento observar os princípios de proteção de dados pessoais elencados no artigo 6º da mesma lei, que enumera além da boa-fé, especialmente, os princípios da finalidade, da adequação, da necessidade e da transparência.

No que tange à finalidade, o artigo 6º, inciso I, dispõe que a atividade de tratamento de dados deve ter um fim específico, sendo esta de conhecimento prévio do titular, bem como deve ser realizada para propósitos legítimos, explícitos e informados ao titular, vedado o tratamento posterior incompatível com as finalidades ora elencadas. Já no que concerne ao princípio da adequação (art. 6º, inciso II), o tratamento de

[3] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm

dados deverá ser realizado de forma compatível com as finalidades informadas ao titular, bem como de acordo com o contexto do tratamento.

Por outro lado, o princípio da necessidade (art. 6º, inciso III) prescreve que o tratamento de dados pessoais deverá ser limitado ao mínimo necessário para a realização de suas finalidades, com a utilização de dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento. Outrossim, o princípio da transparência (art. 6º, inciso VI) garante aos titulares informações claras, precisas e facilmente acessíveis sobre o tratamento de dados realizado, bem como quanto aos agentes de tratamento, observados os segredos comerciais e industriais.

À vista disso, a escolha do tema se justifica uma vez que é imprescindível estabelecer um diálogo entre o direito regulatório e os meios tecnológicos, principalmente os digitais, na medida em que se visa o tratamento de dados pessoais pelo Estado em conformidade com a legislação vigente, evitando-se a perpetuação de um estado de vigilância. Para tanto, a partir de uma abordagem hipotético-dedutiva, e por meio de um estudo exploratório, bibliográfico e jurisprudencial, parte se da hipótese de que a coleta, o processamento e o compartilhamento de dados pessoais possibilitam e fortalecem a formação de um estado de vigilância, sendo importante que o desenvolvimento de ferramentas digitais ocorra de forma transparente com a observância da ampla proteção aos dados do cidadão.

Ademais, verificam-se as compatibilizações entre os princípios fundamentais da incolumidade pública e o direito à privacidade e à proteção de dados em um estado de vigilância, para isso estruturou-se o presente estudo em cinco capítulos.

O primeiro capítulo traz reflexões acerca das tensões, esperanças e medos que as sociedades representadas por meios da clássica tríade da literatura distópica em suas diferentes vertentes, sejam relacionadas eminentemente à questões políticas e ao totalitarismo na vertente de Estado, como é o caso de 1984 de George Orwell, ou questões ligadas à bioética e ao controle desde o nascimento, como em Admirável Mundo Novo de Aldous Huxley e ainda ao controle pela alienação com o uso da tecnologia e banimento do conhecimento, como retratado em Fahrenheit 451, de Ray Bradbury.

O segundo capítulo apresenta a sociedade de vigilância idealizada por Michael Foucault, que evidencia a criação de mecanismos de vigilância como um meio de controle de comportamentos e posicionamentos sociais dos vigiados. Além disso, apresenta reflexões a partir de casos práticos acerca da dicotomia entre a incolumidade pública e o direito à privacidade e à proteção de dados.

Já o terceiro capítulo dedica-se a reflexões acerca da proteção de dados pessoais, paradigmas bem como, a relação entre os direitos à privacidade e à proteção de dados, sendo este último um direito autônomo. No quarto capítulo são feitas considerações acerca das principais normas que versam sobre a proteção de dados no ordenamento jurídico brasileiro, bem como traz-se à baila o debate em torno da Medida Provisória nº 954/2020 e seus aspectos constitucionais.

Finalmente, no quinto capítulo traz-se a discussão acerca da governança de dados na Administração Pública e a disseminação da cultura organizacional ética – a qual deverá conduzir o comportamento, indistintamente, de todas as lideranças, servidores e empregados públicos, em todos os processos de gestão, como medida a ser implementada com vistas a proteger os direitos previstos na LGPD, evitando-se, assim, o tratamento de dados em desconformidade com os preceitos legais pelo Poder Público.

Assim, os instrumentos de proteção de dados pessoais não devem ser encarados como empecilhos para a viabilização de acesso amplo a dados pessoais a fim que se atinja um interesse maior, ao reverso, é a partir da disciplina da proteção de dados que a utilização destes passa a ter legitimidade na medida em que a transparência perpassa os limites e procedimentos específicos.

1 VIGILÂNCIA, CONTROLE E PODER: AS SOCIEDADES DISTÓPICAS

Inicialmente para compreender as distopias, é necessário, partir do seu conceito oposto, as utopias.

A expressão utopia foi criada em 1516 por Thomas More que, na época, a utilizou para se referir a um lugar imaginário, fantástico, que ainda não existia. Na língua inglesa, a palavra utopia surgiu em 1551 a partir da derivação dos radicais gregos, δυσ ("dis" ou "dys") juntamente com a palavra τόπος (*topos*), que significam respectivamente “não” e “lugar” para designar um lugar que não existe.

Já o termo distopia, como antônimo de utopia, foi usado pela primeira vez em 1868 por John Stuart Mill, em um discurso no Parlamento Britânico ao fazer uma crítica a sociedade britânica e compará-la a utopia de Thomas More, alertando os que ali estavam que a sociedade caminhava para um sentido oposto àquele lugar imaginário.

A distopia não é considerada um gênero literário, mas um universo do qual fazem parte inúmeros gêneros, e busca estabelecer uma relação entre literatura e sociedade, ao fornecer ferramentas capazes de analisar de forma profunda e, muitas vezes, radical, as relações sociais em torno do poder, um fenômeno essencial de qualquer comunidade política que pode ser traduzido como a capacidade de influenciar ações, pensamentos e comportamentos.

Enquanto as utopias se referem à uma descrição imaginativa de uma sociedade dita ideal, fundamentada principalmente em leis justas e desprovidas de dogmas e mitos visando o bem-estar da coletividade, as distopias se relacionam às sociedades opressoras, normalmente retratadas por governos totalitários ou autoritários, que exercem, por meio do uso da tecnologia, um domínio ilimitado e de constante vigilância cujo objetivo é manter as desigualdades através da violência e do controle social.

> As distopias versam sobre sociedades disciplinares, um sistema viabilizado por técnicas de controle, vigilância, catalogação e seleção que emanam de um poder central, mas que, sobretudo, são exercidas por toda a sociedade através de micropoderes. O sujeito observado é personalizado para que um

> controle mais íntimo seja possível e não para a valorização das suas especificidades (GOMES; ZONI, 2020, p. 95).

A perda da individualidade também é uma característica das obras distópicas e não se reduz somente à falta de livre arbítrio, mas, de igual forma, deve o homem ser desprovido de sentimentos, como o amor e a amizade bem como, desprendido de laços familiares, na tentativa de se manter uma estabilidade social.

As distopias provocam reflexões ao criticarem de forma satírica a realidade e, se tornam incômodas ao provocar um mal-estar social, na medida em que projetam um futuro perturbador, sob uma perspectiva pessimista que aponta e antevê o que vai acontecer com a sociedade se ela continuar se comportando de tal maneira, como uma espécie de aviso, capaz de alertar sobre possibilidades e consequências de determinada prática (ALMEIDA; MOTA, 2019, p. 144).

Via de regra, há nessas obras um herói que consegue sair do estado de alienação e se insurge contra o sistema, mas que nem sempre conseguirá romper com ele.

Em Admirável Mundo Novo (1932) Aldous Huxley adverte quanto a bioética e manipulação de genes humanos na tentativa de estabelecer um controle social antes mesmo do seu nascimento; já em 1984 (1949), George Orwell dedica-se a escrever sobre a constante vigilância exercida com a ajuda da tecnologia e o controle político preeminente em uma organização totalitária e, finalmente em Fahrenheit 451(1953), Ray Bradbury alerta sobre uma sociedade desencoraja a exercer sua liberdade de expressão, mantendo-se alienada com o uso da tecnologia e o banimento de livros por serem considerados altamente perigosos.

Zygmunt Bauman ao comparar as obras de Orwell e Huxley diz que, apesar de apresentarem visões futuristas distintas, há um ponto em comum entre elas: a vigilância.

> O que elas compartilhavam era o pressentimento de um mundo estritamente controlado; da liberdade individual não apenas reduzida a nada ou quase nada, mas agudamente rejeitada por pessoas treinadas a obedecer a ordens e seguir rotinas estabelecidas; de uma pequena elite que manejava todos os cordões – de tal modo que o resto da humanidade poderia passar toda sua vida movendo-se como marionetes (...). Quando Orwell e Huxley esboçaram

> os contornos do trágico futuro, ambos sentiram que a tragédia do mundo era seu ostensivo e incontrolável progresso rumo à separação entre os cada vez mais poderosos e remotos controladores e o resto, cada vez mais destituído de poder e controlado (BAUMAN, 2001, p. 64-65).

Essas obras literárias representam a clássica tríade dos romances distópicos e

> [...] permitem dramatizar as tensões, esperanças e medos que vivem as sociedades contemporâneas. Além disso, esses espaços cognitivos que permitem visualizar as morfologias da dominação e do poder. Propiciam cenários de resistências ao futuro, mas também projetos que buscam transformar ficção em realidade (BOTELLO, 2018, p. 232).

Em cenários extremistas, em que a sociedade contemporânea passa por angústias e questionamentos sobre o futuro, é possível vislumbrar que vários dos medos e preocupações foram antecipados pela literatura fantástica.

1.1 O ADMIRÁVEL MUNDO NOVO DE ALDOUS HUXLEY

Aldous Leonard Huxley (1894 - 1963) foi um filósofo e escritor inglês, de uma família tradicional britânica formadas por intelectuais ligados à ciência e pesquisa. Seu avô, Thomas Henry Huxley, era um darwinista convicto e foi quem cunhou o termo agnosticismo, isto é, admitia que a partir de um determinado ponto a ciência não poderia explicar fatos ligados à religião e ao místico.

Huxley vivia na França em 1931 quando escreveu a obra Admirável Mundo Novo[4], sendo publicada em 1932; era um adepto ao uso de drogas alucinógenas, principalmente do LSD (dietilamida do ácido lisérgico). Assim, muitas das vivências pessoais de Huxley acabam permeando sua obra.

Nessa época o mundo vivia a ascensão do nazifascismo de direita liderados por Hitler e Mussolini e, também, do fascismo de esquerda de Stálin, com o prenúncio da Segunda Guerra Mundial, além do emparedamento sofrido pelas democracias liberais

[4] O título do livro, originalmente escrito, Brave New World, foi retirado de um trecho de uma peça de William Shakespeare, The Tempest (1911). O trecho refere-se à cena em que Miranda vê os príncipes de Nápoles desembarcarem de um navio naufragado e exclama: "Esplêndida humanidade, maravilhoso mundo novo, quem pode nutrir seres tão perfeitos?" (RAMONET, 1911).

da Inglaterra e França, por exemplo, fatos estes que permeiam a leitura de Admirável Mundo Novo.

Os anos 30 também são conhecidos como a época de ouro da Era Ford. Henry Ford (1863-1947), criador do modelo fordista de produção industrial, com a organização de trabalho para a fabricação em série e padronização de peças de forma que “cada homem, cada mulher, cada criança tinha a obrigação de consumir tanto por ano, em favor da indústria” (Huxley, 1998, p. 72), é referenciado no mundo imaginário de Huxley como um grande líder.

Sobre esse aspecto Altino José Martins Filho traz uma reflexão interessante

> Por ter sido um ícone do tecnicismo e do funcionalismo na época de Huxley, Ford toma o lugar de Jesus Cristo nesta sociedade do futuro. O aspecto divino e religioso é substituído pela crença em tudo o que é tangível, o que parece demonstrar a valorização exacerbada da tecnologia e do pragmatismo (MARTINS FILHO, 2003, p. 102).

Em Admirável Mundo Novo o mundo é hipoteticamente dividido em departamentos de chefias mundiais. O livro narra então a história de uma comunidade situada em Londres, uma das capitais mundiais, no ano de 632 pós-Ford na qual o Estado, cujo lema é: comunidade, identidade e estabilidade, tem total domínio sobre a vida dos indivíduos, no qual são geneticamente e psicologicamente manipulados, por intermédio de uma ditadura científica do futuro, atemorizada pela constante vigilância.

Nessa realidade futurista, a sociedade é organizada e hierarquizada em um sistema científico de castas, dividida conforme suas características e aptidões, sendo disposta e separada da seguinte forma: a classe Alfa, considerada a mais alta, composta por indivíduos intelectualmente desenvolvidos e que ocupam postos de destaque e liderança na sociedade; a classe Beta; a classe Gama; a classe Delta e, finalmente a classe Ípsilon sendo a classe inferior, cujos indivíduos eram planejados e condicionados apenas para a realização de atividades não complexas e/ou de cunho braçal. Já fora dessa sociedade vivem os chamados selvagens.

Outrossim, o casamento, a família e a procriação foram eliminadas, existindo apenas fora do que eles chamam de civilização. Como em uma linha de montagem, os bebês

são fabricados e desenvolvidos em uma grande incubadora localizada na sala de fecundação e controlada por cientistas do Estado no “Centro de Incubação e Condicionamento de Londres Central - CIC”, por um método totalmente artificial e submetidos ao processo Bokanovsky que possibilitava um óvulo germinar, proliferar e dividir-se em até 96 embriões idênticos (HUXLEY, 1998, p. 14).

"Noventa e seis gêmeos idênticos fazendo funcionar noventa e seis máquinas idênticas! [...] Sabe-se seguramente para onde se vai. - Citou o lema planetário: Comunidade, Identidade, Estabilidade" (HUXLEY, 1998, p.14).

É possível perceber que nesse processo de fecundação e desenvolvimento do feto, a identidade de cada um vai sendo moldada, dentro de uma linha de produção, pela quantidade ideal de oxigênio, vitaminas e nutrientes a ser recebida a depender da casta a qual o indivíduo irá pertencer.

Acrescente-se ainda o fato de que não era socialmente adequado que duas pessoas mantivessem um compromisso sexual por muito tempo, a dinâmica sexual era pensada de forma que os indivíduos sempre estivessem trocando de parceiros. Assim, caso uma mulher engravidasse de forma natural era encaminhada ao “Centro de Aborto”, visto que o ideal era apenas humanos de proveta, gerados em laboratórios por engenharia genética, para controle demográfico e planificação total da sociedade.

Nesse contexto, os serem humanos são planejados para serem altamente produtivos para o Estado através da manipulação de material genético, reprogramação mental e uso frequente de uma substância denominada “SOMA” (HUXLEY, 1998, p. 6) que dá aos indivíduos a sensação de euforia e prazer, resultando em uma sociedade homogênea, desprovida de subjetividade, individualidade e sentimentos, com a eliminação de toda possibilidade de criação, pensamento reflexivo e tomada de decisões, de modo que se mantem a estabilidade social.

> Nesta sociedade, as pessoas são controladas pela cultura do prazer (hedonismo) fundado no sexo livre e banalizado, na droga institucional ministrada pelo Estado e na música sintética de efeito psicodélico. Esse receituário que combina a “droga perfeita” com a proscrição de relações amorosas e a banalização do sexo expressada na fórmula hipnopédica “cada um pertence a todos” age como controle social. Numa realidade em que o

> relacionamento social é pautado no vínculo com o outro (não obstante o fato de não ser o outro, mas um complemento de um corpo social), a droga e o sexo livre asseguram a tão almejada estabilidade e conduzem artificialmente à autossatisfação (ALMEIDA; MOTA, 2019, p. 143).

Outro recurso utilizado pelo Estado nessa sociedade, era a hipnopédia, repetição constante de frases gravadas usadas para condicionar as crianças enquanto dormem e, tinha por objetivo moldar as mentes e os desejos, com efeitos por toda vida, como afirma uma das personagens de Huxley (1998, p. 31):

> [...] até que, finalmente, o espírito da criança seja essas coisas sugeridas, e que a soma dessas sugestões seja o espírito da criança. E não somente o espírito da criança. Mas também o adulto, para toda a vida. O espírito que julga, e deseja, e decide, constituído por essas coisas sugeridas. Mas todas essas coisas sugeridas são aquelas que nós sugerimos, nós! – O Diretor quase gritou, em seu triunfo. – Que o Estado sugere.

Assim, a repetição de frases sugeridas determina o comportamento das pessoas, seus julgamentos e decisões nada mais são que um conjunto de sugestões induzidas na mente dos indivíduos, de modo que, a personalidade seja moldada pelo Estado e baseada na estabilidade social, ordem e disciplina.

A ideia por de trás desse romance distópico é de que a tecnologia encampada pelo interesse do Estado se reverte em técnica de dominação. Assim, o Estado controla e adestra os cidadãos não por meio de violência ou lavagem cerebral, mas através da hipnose, uso de drogas e seleção biológica em incubadoras, para ser tornarem membros úteis e felizes para a sociedade. Logo, a cultura humana e a informação são afundadas em um mar de entretenimento superficial; a arte, a filosofia e a ciência também deixam de ser praticadas.

Desse modo, o Estado detém o poder controlador que tiraniza e impede o indivíduo de alcançar a verdadeira felicidade e ser, de fato, livre. Se antes desse mundo as pessoas passavam por sofrimentos, como miséria, doenças e guerras, supostamente nessa nova sociedade isso não existe mais.

Neste livro já se falava sobre a ineficiência da coerção e da necessidade desse sistema de implantação de condicionamento das pessoas àquilo que viria a ser realmente a sua escravidão, de modo que o homem adore a sua dominação.

1.2 O *BIG BROTHER* E A SOCIEDADE DE VIGILÂNCIA NA PERSPECTIVA DE GEORGE ORWELL NA OBRA “1984”

Assim como Huxley, Orwell fala sobre um futuro distópico, mas com aspectos distintos.

George Orwell, pseudônimo de Eric Arthur Blair nasceu na Índia em 1903, sob o domínio do império britânico; filho de um funcionário colonial, Orwell estudou em escolas de elite e, assim como seu pai, trabalhou na polícia imperial da Índia na Birmânia, quando se deparou com a brutalidade do império britânico na tentativa de dominar os nativos. Diante desse cenário perturbador, Orwell decidiu largar a farda e se dedicar à literatura e ao jornalismo, passando por Paris, Londres e Espanha, quando participou da Guerra Civil espanhola (HITCHENS, 2010, p. 41-42).

Aliás, a experiência na polícia imperial foi responsável por criar em Orwell aversão a qualquer tipo de dominação política.

> Essa sua primeira experiência profissional como oficial de polícia na Birmânia marcou-o profundamente e a essa vivência atribuiu Orwell persistentemente o seu “ódio” ao sistema: “In order to hate the empire you have to be part of it” (ibidem: 127), afirma o autor mais adiante na obra de onde foi extraída a citação. Sem levarmos à letra tão categórica afirmação, que dá uma injustificada primazia ao empírico sobre o ideológico, não é demais acentuar o quanto o seu conhecimento “de dentro” de um governo colonial determinou a sua subsequente posição enquanto opositor do Império. (SILVA; VIERA, 2005, p.13-14)

Em 1941, já como um reconhecido jornalista, Orwell retorna ao seu país de origem para trabalhar na sede da BBC Índia durante a Segunda Guerra Mundial em que as informações divulgadas na colônia britânica eram sempre censuradas e vigiadas. Nesse contexto, Orwell, mesmo sendo anti-imperialista, era responsável por produzir a propagada imperialista para defender a presença da Inglaterra na colônia indiana (HITCHENS, 2010, p. 47).

Entender a trajetória de George Orwell é necessária para compreender, também, o contexto em que se passa a obra 1984.

Um livro quase profético sob o ponto de vista atual, a obra 1984 de George Orwell, escrita em 1948 e publicada em 1949 foi considerada uma distopia ao prever o futuro negativo de uma sociedade oprimida e limitada por um regime totalitário. Ao pensar na proximidade da data em que foi escrito com o ano retratado no livro, é possível imaginar que Orwell advertia sobre uma distopia não tão distante, em que era preciso temer o que vinha pela frente.

Em uma perspectiva ampliada, embora a intenção de Orwell fosse lançar luz sobre os horrores do totalitarismo e os regimes intermináveis de espionagem do Estado impostos aos cidadãos em meados do século XX, e tudo que os permeia como: culto a figura de um líder supremo, unipartidarismo, doutrinação, manipulação de informações e dados históricos, uso da violência, censura, nacionalismo exarcebado, militarização, criação de inimigos imaganários internos e externos. Ademais, fora retratada a forma tenebrosa como seria uma sociedade eternamente controlada por pessoas fanáticas pelo poder, servindo de alerta sobre os perigos dos avanços tecnológicos para a humanidade.

A obra *orwelliana* foi escrita ao final da Segunda Guerra Mundial e cria um paralelo com o cenário de guerra vivido, isto porque, assim como na Alemanha nazista, em "1984" a sociedade é mantida sob controle do chamado *"Big Brother"* ou o "Grande Irmão" - aquele que tudo vê e tudo sabe, mas não é visto – líder totalitário do partido, obcecado em manter e perpetuar seu poder por meio da opressão surgida após uma 3ª Guerra Mundial e que tem como grande inimigo do Partido, o revolucionário Goldstein.

O "mundo" imaginário de Orwell é dividido entre três domínios: Oceania, Lestásia e Eurásia, sendo um reflexo dos países que venceram a 2ª Guerra Mundial. A história se passa no território da Oceania, onde tal sociedade distópica, dominada pelo socialismo inglês (sistema "ingsoc"), é dividida em três classes: núcleo do partido (classe privilegiada); partido externo (subserviente ao núcleo) e os proletas (a grande massa ignorante e alheia aos acontecimentos), sendo as duas primeiras classes responsáveis por manipular informações, falsear a realidade, controlar a privacidade e estimular a ignorância e o ódio.

O protagonista da história é o Winston Smith, um homem solitário e membro do partido externo que trabalhava no departamento de documentação do Ministério da Verdade e seria responsável pelo revisionismo histórico, Winston então revisa e altera documentos, para que os registros históricos sempre aparentam apoiar a ideologia do partido.

Sobre este ponto a história do personagem se mistura com a do próprio autor, visto que

> Boa parte do tempo de Orwell era gasta contornando a vigilância e a interferência. A certa altura, ele foi compelido a aconselhar E. M. Forster a não mencionar a obra de K. S. Shelvankar, cujo livro fora proibido na Índia. Contudo, não muitos meses depois, vemos Orwell escrevendo pessoalmente a Shelvankar para pedir-lhe que participasse, sem pseudônimo, de programas de rádio sobre a história do fascismo. (HITCHENS, 2010, p.20)

Hitchens (2010, p. 34) ainda relata que: "a sala onde aconteciam as reuniões editoriais dos Eastern Services da BBC era a Sala 101 na sede de *Portland Place*, que foi um dos modelos arquitetônicos para o Ministério da Verdade".

Ainda durante a narrativa de Orwell, somos apresentados à teletela uma espécie de televisão bicameral, que permitia tanto ver como ser visto, sendo um instrumento fundamental para o Grande Irmão exercer a vigilância sobre os cidadãos e transmitir informações do partido, de modo que, os indivíduos são monitorados o tempo inteiro, em suas casas e pelas ruas de Oceânia, pelas telas de vídeo bidirecionais.

Há outros elementos interessantes apresentados por Orwell que se ligam à ideia da sociedade de vigilância, como: a polícia das ideias, responsável pela vigilância dos pensamentos e ações, em que ao se pensar de forma contrária aos interesses do Partido, mesmo que de modo inconsciente, já configuraria o crime de "pensamento-crime" (ORWELL, 2009, p. 29). Há ainda os Ministérios da Verdade, responsável pela alteração da realidade, o Ministério do Amor que, de maneira contraditória, era incumbido das prisões e torturas, o Ministério da Paz, encarregado da guerra e o Ministério da Fartura, responsável pelas atividades econômicas.

Ademais, há o chamado “dois minutos de ódio e a semana do ódio”, quando havia a eleição de um inimigo do povo e o direcionamento de xingamentos e de raiva irracional a ele, de modo a desviar e afastar a sociedade dos verdadeiros problemas.

Revela-se ainda no enredo orwelliano a ideia do duplipensamento que pode ser entendido como a capacidade de ter pensamentos e crenças contraditórias e acreditar em ambas ao mesmo tempo, fazendo com que as pessoas não tivessem mais certeza ou convicção sobre nada.

Em sua obra Orwell define o duplipensar como um:

> Saber e não saber, ter consciência de completa veracidade ao exprimir mentiras cuidadosamente arquitetadas, defender simultaneamente duas opiniões opostas, sabendo-as contraditórias e ainda assim acreditando em ambas; usar a lógica contra a lógica, repudiar a moralidade em nome da moralidade, crer na impossibilidade da democracia e que o Partido era o guardião da democracia; esquecer tudo quanto fosse necessário esquecer, trazê-lo à memória prontamente no momento preciso, e depois torná-lo a esquecer; e acima de tudo, aplicar o próprio processo ao processo. Essa era a sutileza derradeira: induzir conscientemente a inconsciência, e então, tornar-se inconsciente do ato de hipnose que se acabava de realizar. Até para compreender a palavra “duplipensar” era necessário usar o duplipensar. (ORWELL, 2005, p. 36-37)

Outro artifício utilizado pelo Grande Irmão é a Novilíngua, por meio da qual o idioma local era sempre reescrito com o objetivo de se tornar cada vez mais simplório. Palavras deixavam de existir e eram substituídas por novas, bem mais objetivas. Isso contribuía para a ignorância do povo, que aos poucos não tinha vocabulário suficiente para formular pensamentos críticos e expressá-los.

Nesse cenário cria-se a ideia de submissão, no sentido de que nesse reino não existem leis e sim inúmeras regras determinadas pelo partido.

1984 mostra a paixão pelo autoritarismo; a falta de privacidade vivida hoje em nações democráticas sugere uma capacidade do Estado de regular assuntos inseridos dentro dos espaços mais íntimos da vida privada, excedendo qualquer ideia imaginada em 1984.

Como Marjorie Cohn (2014) indicou em uma tradução livre acerca da realidade estadunidense e, que de certa forma também é aplicavel ao Brasil:

> Orwell nunca poderia ter imaginado que a National Security Agency (NSA) iria acumular metadados em bilhões de nossas ligações telefônicas e 200 milhões de nossas mensagens de texto todos os dias. Orwell não poderia ter previsto que nosso governo leria o conteúdo de nossos e-mails, transferências de arquivos e bate-papos ao vivo nas redes sociais que usamos.

Fato coincidente e que chama a atenção é que em 1983, ou seja, um ano antes do período em que se passa a obra *orwelliana*, o Tribunal Constitucional Alemão, em razão do surgimento do processamento de dados, instaurou precedente importante ao adicionar a dimensão da autodeterminação informativa ao direito à privacidade, de modo que, criou uma barreira contra a ingerência abusiva do Estado sobre os dados pessoais dos cidadãos (TORRES; AZEVEDO, 2020).

Se antes a sociedade distópica imaginada por Orwell parecia distante e quase impossível de ser concretizada, torna-se cada vez mais claro que a representação de Orwell do estado moderno fundado em um ideal democrático enraizado no direito à privacidade foi transformada e mutilada, quase irreconhecível.

Pertinente o entendimento de Fátima Vieira e Jorge Bastos da Silva acerca da importância da produção literária de Orwell no contexto político atual:

> Embora seja detectável na sua vastíssima obra a influência de contextos históricos definidos e datáveis, permanece atual o seu olhar crítico sobre o cinismo da cena política e a forma inteligente como lidou com a questão da liberdade, expondo a estupidez de todo o tipo de submissão. (VIEIRA; SILVA, 2005, p.5)

Assim como a fábula de Orwell se transformou ao longo do tempo em um "romance realista" ou em um "documentário da vida real", a captação e circulação de dados pessoais foi radicalmente alterada em uma era de troca global permanente e ininterrupta de informações, desse modo, “A tecnologia de hoje possibilita um tipo de vigilância onipresente, antes restrita aos mais criativos autores de ficção científica” (GREENWALD, 2014, p.12).

Desta forma, as fronteiras não são mais um obstáculo para a coleta de informações e espionagem de governos, indivíduos, políticos proeminentes, empresas e grupos corporativos. Ao mesmo tempo, a proteção de dados pessoais e o direito à privacidade é ansiosamente abandonado por milhões de pessoas pelas maravilhas proporcionadas pelos *smartphones* e redes sociais.

Pelas teletelas atuais ampliou-se o acesso à vida dos indivíduos do que as retratadas no livro “1984”, enquanto nessas havia a possibilidade de ver e ouvir aquilo que era externados pelos indivíduos, hoje, com os algoritmos presentes em aplicativos e redes sociais (DILLMANN; PIRES FILHO, 2018), é possível acompanhar cada movimento do cidadão, lugares, predileções, preferências partidárias, sendo possível, inclusive, prever quais serão os próximos passos a serem dados.

É possível dizer que a sociedade imaginada por Orwell é revestida por sistema totalitário visível, concreto e incontestável, já na atual e real sociedade há um totalitarismo disfarçado e revestido por uma frágil democracia que é contestada sempre que seus valores são contrários ao poder hegemônico.

A grande questão da obra de Orwell é nos questionar: o que pode ocorrer em uma sociedade altamente vigiada? Quando essa vigilância se transforma em mecanismo de controle das pessoas?

1984 é, portanto, tema da dominação e da alienação, isto é, de que maneira a dominação e a vigilância profundas produzem alienação.

1.3 A QUEIMA DOS LIVROS EM FAHRENHEIT 451: O APAGAMENTO DA MEMÓRIA E DO CONHECIMENTO

“Queimar era um prazer” (BRADBURY, 2012, p. 25) assim começa o romance distópico de Ray Douglas Bradbury (1920 - 2012), escritor americano que durante a primavera de 1950, começou a escrever sua obra Fahrenheit 451, publicada apenas em 1953, período imediatamente após a 2ª Guerra Mundial e início da Guerra Fria.

“A rápida emersão da televisão como um fator determinante da indústria cultural, a expansão da publicidade, o abuso da tecnologia a partir do complexo militarindustrial, a degradação das massas” (ZIPPES apud KOPP, 2011, p. 225) são fatores que compõem Fahrenheit 451, no qual se tecem críticas aos meios de comunicação e ao excessivo conformismo que dominava a sociedade.

O título do livro ao indicar a temperatura de 451ºF ou, convertido para Celsius, 233 graus fazem alusão à temperatura de combustão do papel que remete a um dos pontos chaves dessa distopia: o apagamento da memória e do conhecimento; a queima dos livros é simbólica ao mesmo tempo que é concreta.

O livro é visto como um elemento desestabilizador da história justamente por trazer conhecimento.

> [...] livros são queimados ou por apresentarem ideias que pudessem fazer com que os indivíduos refletissem sobre o estado autoritário em que viviam ou porque podiam apresentar outras situações de vida que poderiam deflagrar processos de autoconhecimento ou mesmo experiências lúdicas e estéticas que estariam para além das possibilidades simplórias e reduzidas vivenciadas naquele contexto (RIBEIRO, 2007).

O número 451 ainda é visto no uniforme dos bombeiros, responsáveis por incinerarem os livros.

Nessa realidade distópica, ambientada na América do século XXI, “que vive sob o jugo do alto controle imposto pelas forças autoritárias personificadas pelos bombeiros” (RIBEIRO, 2007), é possível acompanhar a história do personagem principal Guy Montag, um bombeiro que seguiu a profissão do pai e do avô, cujo objetivo principal de seu ofício não é o de apagar incêndios, já que as casas e edifícios são equipados com tecnologia antichamas, mas sim começá-los, mais especificamente, seu trabalho é focado em receber denúncias de posse de livros, considerados extremamente perigosos e, portanto, proibidos, incendiando-os, e, aqueles que os detém são tidos como loucos e internados em hospícios.

> A sociedade de Fahrenheit deve esquecer o passado que traz sofrimento às pessoas e que nada acrescenta às suas vidas. Eis por que os livros são queimados: eles representam o passado, o conhecimento da história e a

> possibilidade de uso da fantasia, o que pode colocar em risco o projeto autoritário da sociedade (GOMES; ZONI, 2020, p. 88).

O argumento utilizado e repetido pelos bombeiros para a queima dos livros é: “Os livros não tem nada a dizer, eles tornam os homens diferentes e queimá-los faz de nós ou nos tornam mais felizes” (BRADBURY, 2012, p. 26).

O departamento que incinerava os livros raramente precisava fazer isso porque as pessoas decidiram que não querem mais ler por vontade própria. Ademais, é comentado que os livros ilegais mais achados são principalmente obras famosas de Walt Whitman, um poeta da Revolução Americana e de William Faulkner, considerado um dos maiores romancistas norte-americano.

Outrossim, a tecnologia é um elemento muito presente na obra, o ambiente é tecnologicamente sofisticado e desenvolvido, há meios de transporte ultrarrápidos, robôs de alta tecnologia e todas as casas possuem super telas interativas (*wall screen*), sendo a principal fonte de entretenimento, fazendo com que a população se tornasse alienada e pouco preocupada com a realidade. Não há interações entre as pessoas, apenas com máquinas.

A massificação do entretenimento tecnológico, através do rádio e da televisão, esconde ainda uma manipulação de informações pelo governo. Há uma ameaça de destruição nuclear, mas pouco se fala sobre isso, a mídia comenta brevemente se tratar de uma guerra ganha, mas não se sabe ao certo quem é o inimigo. A censura faz com que a população se mantenha apática e feliz, passíveis de manipulação. Aliado a esse entretenimento, há ainda o uso de medicamentos capazes de minimizar a angústia e a tristeza.

Diferente dos outros clássicos distópicos que antecedem esta obra, em Fahrenheit 451 o totalitarismo não é governamental e sim comportamental, a sociedade foi condicionada a rechaçar qualquer tipo de manifestação cultural escrita, abrindo espaço para o entretenimento televiso, vazio de qualquer pensamento crítico e reflexivo.

> [...] Se não quiser um homem politicamente infeliz, não lhe dê os dois lados de uma questão para resolver; dê lhe apenas um. Melhor ainda, não lhe dê nenhum. Deixe que ele se esqueça de que há uma coisa como a guerra. Se o governo é ineficiente, despótico e ávido por impostos, melhor que ele seja tudo isso do que as pessoas se preocuparem com isso. Paz Montag. Promova concursos em que vençam as pessoas que se lembrarem das letras das canções mais populares ou dos nomes das capitais dos estados ou de quanto foi a safra de milho do ano anterior. Encha as pessoas com dados incombustíveis, entupa-os com "fatos" que elas se sintam empanzinadas, mas absolutamente "brilhantes" quanto a informações. Assim elas imaginarão que estão pensando, terão uma sensação de movimento sem sair do lugar. E ficarão felizes, porque fatos dessa ordem não mudam. Não as coloque em terreno movediço, como filosofia ou sociologia, com que comparar suas experiências. Aí reside melancolia. Todo homem capaz de desmontar um telão de tv e montá-lo novamente, e a maioria consegue, hoje em dia está mais feliz do que qualquer outro homem que tenta usar a régua de cálculo, medir e comparar o universo, que simplesmente não será medido ou comparado sem que o homem se sinta bestial e solitário. [...] (BRADBURY, 2012, p. 92).

Assim, as ideias dissidentes eram coibidas por meio da vigilância tecnológica. Por exemplo, Sabujo, como era chamado o cão de caça mecânico, era dotado de um sofisticado sistema de armazenamento de odores corporais e capaz de perceber qualquer alteração na temperatura corporal da pessoa, podendo se lembrar de até 10.000 cheiros diferentes, em uma vigilância biológica aos resistentes.

Ademais, os indivíduos são, a todo tempo, encorajados a delatar os rebeldes. Assim, o sistema de controle do Estado funciona a partir de informações dos denominados informadores que, utilizando-se da caixa de informação, denunciam seus pares que possuam livros em casa (RIBEIRO, 2007).

> Nesta obra está presente a lógica do panóptico e a tensão que decorre dela. Não há observação propriamente dita realizada por instrumentos, mas pelos indivíduos uns sobre os outros. Não importa efetivamente se os sujeitos estão sendo vigiados ou não; para que haja o efeito de poder e de controle basta a sensação de vigilância (GOMES; ZONI, 2020, p. 89).

O totalitarismo retratado nessa obra distópica, se difere dos modelos totalitários apresentados nas obras antecedentes, Admirável Mundo Novo e 1984, conforme salienta Manoel da Costa Pinto ao escrever o prefácio da edição de 2012 de Fahrenheit 451

> O que interessa aqui, porém, é frisar a singularidade da distopia de Bradbury. Pois enquanto Huxley e Orwell escreveram seus livros sob o impacto dos regimes totalitários (nazismo e stalinismo), Bradbury percebe o nascimento

> de uma forma mais sutil de totalitarismo: a indústria cultural, a sociedade de consumo e seu corolário ético – a moral do senso comum (BRADBURY, 2012, p. 15 - 16)

Ao contrário de Admirável Mundo Novo e 1984 em que as histórias se desenvolvem com foco no estado totalitário e repressor, em Fahrenheit 451 o ponto central está nas pessoas, Ray Bradbury mostra como os estados totalitários não começam de uma hora para outra e de cima para baixo, o movimento é oposto, começa pela população, na medida em que para de ler livros por conta própria e os troca por um entretenimento mais cômodo, a televisão.

> [...] A coisa não veio do governo. Não houve nenhum decreto, nenhuma declaração, nenhuma censura como ponto de partida. A tecnologia, a exploração das massas e a pressão das minorias realizaram a façanha, graças a Deus. Hoje, graças a elas, você pode ficar o tempo todo feliz (BRADBURY, 2012, p. 88).

Logo, o povo não aparece como vítima de um estado autoritário, mas sim como cúmplice dele.

Interessante observar como vários dos elementos antevistos pela literatura distópica - como uso da tecnologia, vigilância e controle são transportados para o mundo real como se verá ao longo desse estudo.

2 A SOCIEDADE DE VIGILÂNCIA E SEUS NOVOS CONTORNOS

O fenômeno do uso de dados e seu tratamento massivo é uma realidade cada vez mais incontornável, “o vigiar e punir é substituído pelo monitorar, registrar e reconhecer” (VIANNA, 2007, p. 25). O exercício do poder já não é a base da coerção física, mas, muito mais a base do controle de dados e informações.

> A atual conjuntura vivida pelo Brasil traz à tona elementos distópicos na mesma perspectiva huxley-orwellana, marcadamente por traços particulares sobre a sua política, ciência, tecnologia, economia, cultura... e traços gerais da própria história da humanidade, distinguida pelas decadentes relações sociais capitalistas das quais o país faz parte, capaz de sepultar qualquer expressão utópica (ALMEIDA; MOTA, 2019, p. 146).

O professor historiador Yuval Noah Harari (2020) afirmou que muitas das medidas de emergência de curto prazo implementadas durante a pandemia, se tornarão estruturas instituídas, de modo que, os momentos de crise acabam funcionando com grandes aceleradores de rupturas paradigmáticas.

Muitas das soluções tomadas, em princípio, para permanecerem apenas durante o período da crise podem acabar, por uma série de circunstâncias se estendendo para além da crise. Entender esse processo, as razões pelas quais isso existe é sempre algo complexo, ao mesmo tempo que se mostra como uma grande janela de oportunidades para que diversos interesses, que muitas vezes não teriam repercussão em um cenário de normalidade, por serem antidemocráticos ou por envolverem restrições de direitos, acabem por prevalecer e perpetuar até mesmo após passada a crise que o justificariam.

Diante do cenário pandêmico, há uma tendência de aceitar que o Estado tome iniciativas mais contundentes e invasivas na vida dos cidadãos, isto porque, ao que parece, a privacidade e a proteção de dados se expressam como direitos de menor relevância ante a necessidade e urgência de combate à pandemia e à garantia do direito à saúde.

Assim, quando ao pensar em um processo de aceleração histórica por meio de uma crise, invariavelmente há um temor de que possamos sair dela “piores”, ou seja, de

que essa brecha propiciada pelo momento seja mal utilizada e, consequentemente, em um cenário pós-pandêmico tenhamos uma série de medidas restritivas de direitos e, com repercussões que certamente perdurarão no tempo.

O panóptico descrito por Foucault permanece presente, não mais como uma estrutura arquitetônica visível e imponente, mas por intermédio de tecnologias que monitoram e mapeiam o comportamento humano e direcionam as opiniões em uma sociedade que caminha para a aceitação da escravidão de modo passivo como previu Aldous Huxley em Admirável Mundo Novo. Sob esta ótica, Harari (2020) menciona que estamos mudando de uma "vigilância sobre a pele para uma vigilância sob a pele".

2.1 O PANÓPTICO: VIGILÂNCIA E DISCIPLINA

A ideia e descrição da vigilância da sociedade distópica de Orwell pode ser considerada semelhante à do Panóptico de Michel Foulcault[5].

O primeiro a usar o termo "panóptico" foi o filósofo e político britânico Jeremy Bentham em 1785. Bentham projetou a estrutura arquitetônica do panóptico ou, também chamada de casa de inspeção, para ser um modelo ideal de prisão, em que haveria um arquétipo circular dividido em celas, em que cada cela haveria duas janelas, uma para a face interna do anel em que estaria localizada uma torre central de observação de onde o vigilante teria uma visão de 360º sob toda a estrutura e a outra para a face externa por onde entraria luz. Além disso, a torre central estaria coberta por cortinas, de modo que os presos não pudessem ver o vigilante, mas o vigilante pudesse ver a todos (GUNDALINI; TOMIZAWA, 2013, p. 24).

Foucault (2002, p. 165) utiliza e aperfeiçoa a ideia do panóptico e o descreve da seguinte forma:

> Na periferia uma construção de anel; no centro, uma torre; esta é vazada de largas janelas que se abrem sobre a face interna do anel; a construção periférica é dividida em três celas, cada uma atravessando toda a espessura da construção; elas têm duas janelas, uma para o interior, correspondendo

[5] Michel Foucault foi um filósofo francês nascido em Poitiers, no dia 15 de outubro de 1926 e faleceu em Paris, no dia 25 de julho de 1984. Foi um importante filósofo e professor da cátedra de História no Collége de France desde 1970 até 1984.

> às janelas da torre; outra, que dá para o exterior, permite que a luz atravesse a cela de lado a lado. Basta então colocar um vigia na torre central, e em cada cela trancar um louco, um doente, um condenado, um operário ou um escolar. Pelo efeito da contraluz, pode se perceber da torre, recortando-se extremamente sobre a claridade, as pequenas silhuetas cativas nas celas da periferia. Tantas jaulas, tantos pequenos teatros, em que cada ator está sozinho, perfeitamente individualizado e constantemente visível. O dispositivo panóptico organiza unidades espaciais que permitem ver sem parar e recolher imediatamente.

Assim, a arquitetura do panóptico é toda pensada para fazer com que o vigia possa observar o que se passa em qualquer uma das celas e que cada ocupante da cela veja apenas a torre, mas esteja impedido de ver o que se passa em seu interior, assim o ocupante da cela sabe que pode estar sendo visto a qualquer momento, mas não sabe exatamente quando ou por quem, em contrapartida o vigia vê sem ser visto, de modo a tornar um sistema de vigilância contínua sobre o indivíduo (BRÍGIDO, 2013, p. 65).

Tal estrutura foi considerada perfeita para ser adotada em penitenciárias e prisões, ou ainda em qualquer tipo de estabelecimento em que as pessoas precisam ser vigiadas, como manicômios, hospitais, escolas e fábricas.

Acerca desse ponto Pedro Scuro Neto (2010, p. 244) explica que

> [o] mesmo tipo de mecanismo é aplicado também a sujeitos submetidos a internação (encarceramento e/ou hospitalização), e no processo de segregação de minorias raciais, étnicas ou religiosas. Isolado o indivíduo deve vivenciar a própria impotência diante da férrea objetividade dos mecanismos de controle aplicados – é compelido experimentar uma sensação física e moral, profunda e "peculiar", uma dualidade, um sentimento de estar sempre olhando para si mesmo através dos olhos dos outros e medindo a própria alma com a fita métrica do mundo que o encara atemorizado, com desprezo ou piedade.

Nesse contexto, Foucault (2001, p. 166-167) ressalta que "para ser eficiente, o panóptico deve ser 'visível' e 'inverificável'; o indivíduo não precisa saber que está sendo observado, mas precisa ter certeza de que poderá sê-lo a qualquer momento", isto é, parte-se da ideia de que os prisioneiros, ao não verem os guardas, se sentiriam sempre vigiados. Outrossim, o panóptico deve ser entendido como "uma utopia de uma sociedade e de um tipo de poder que é, no fundo, a sociedade que atualmente conhecemos" (FOUCAULT, 2001, p. 88).

Foucault como um estudioso da sociedade e das formas de disciplinarização identifica nos séculos XVIII e XIX a emergência de um novo tipo de sociedade, a sociedade disciplinar. Essa nova forma de exercer o poder e de organizar a sociedade que, de forma diversa da sociedade medieval em que os criminosos eram condenados e punidos por meio de espetáculos públicos de dor e sofrimento, obedece ao modelo do panóptico. Logo, a partir da pós-modernidade há uma significativa alteração do controle social (GUNDALINI; TOMIZAWA, 2013, p. 25-26).

Nessa perspectiva, o Estado é um órgão que possui poder, mas esse poder não se restringe apenas e tão somente ao Estado, na verdade os indivíduos estão inseridos em relações de poder. Assim, o poder não está concentrado em uma instituição específica, mas distribuído entre a sociedade.

> É preciso não tomar o poder como um fenômeno de dominação maciço e homogêneo de um indivíduo sobre os outros, de um grupo sobre os outros, de uma classe sobre as outras; mas ter bem presente que o poder não é algo que se possa dividir entre aqueles que o possuem e o detém exclusivamente e aqueles que não o possuem. O poder deve ser analisado como algo que circula, ou melhor, como algo que só funciona em cadeia. Nunca está localizado aqui ou ali, nunca está nas mãos de alguns, nunca é apropriado como uma riqueza ou um bem. O poder funciona e se exerce em rede. Nas suas malhas os indivíduos não só circulam mas estão sempre em posição de exercer este poder e de sofrer sua ação; nunca são o alvo inerte ou consentido do poder, são sempre centros de transmissão. Em outros termos, o poder não se aplica aos indivíduos, passa por eles. (FOUCAULT, 2002, p. 193)

Outrossim, Foucault (2002, p. 201-203) divide o poder em duas esferas: o poder real e o poder disciplinar. O poder real se relaciona a figura de uma autoridade, o rei, em que tal poder se concentra na figura de uma única pessoa, sendo algo palpável. Além disso, o poder real é exercido de forma ostensiva, por exemplo, através de castigos físicos e violentos, tornando-se um grande espetáculo que servia de exemplo para o resto da população ter conhecimento do que acontecia com aquele que cometesse um crime.

Em contrapartida, o poder disciplinar se baseia na domesticação e docilização dos corpos. A partir dessa perspectiva, o medo e o controle não são mais exercidos do exterior para o interior, como eram nos suplícios; agora, o próprio indivíduo que faz pressão em si mesmo. A ideia de estar sendo sempre observado, faz com que o

indivíduo mude sua postura e passe a se policiar o tempo inteiro sobre suas atitudes e comportamentos, em outras palavras, a fórmula do poder disciplinar era: mais vigilância e menos punição.

Nesse sentido, Foucault se apropria do conceito de visão global de monitoramento para descrever o poder de controle que as instituições públicas exercem sobre o indivíduo, desde a infância até a fase adulta, mesmo que o indivíduo não seja criminoso.

> [...] sem necessitar de armas, violências físicas, coações materiais. Apenas um olhar. Um olhar que vigia e que cada um, sentindo-o pesar sobre si, acabará por interiorizar, a ponto de observar a si mesmo. Fórmula maravilhosa: um poder contínuo e de custo afinal de contas irrisório. (FOUCAULT, 2002, p. 218)

De igual forma, Foucault (2002, p. 167) diz que o ocupante da cela é um objeto de informação, mas nunca sujeito de uma comunicação, visto que este esta impedido de se comunicar com os seus pares, de modo que, “quanto maior o número de informações em relação aos indivíduos, maior a possibilidade de controle de comportamento desses indivíduos” (FOUCAULT, 2002, p. 57).

Foucault (2002, p. 169) ainda destaca, a partir do seu ponto de vista teórico que o efeito geral desse esquema arquitetônico de Benthamé o de permitir a introjeção mais eficiente da norma social, isto é, um processo de normalização visto que enquanto o ocupante da cela está sendo vigiado, mas não sabe quando ou por quem, o indivíduo está se “autovigiando” o tempo todo.

Nas palavras de Foucault:

> É, ao mesmo tempo excessivo e muito pouco que o prisioneiro seja observado sem cessar por um vigia: muito pouco, pois o essencial é que ele se saiba vigiado; excessivo, porque ele não tem necessidade de sê-lo efetivamente. (FOUCAULT, 2002, p. 191).

Além disso, o esquema de vigilância idealizado a partir do panóptico faz com que o indivíduo se torne, ao mesmo tempo, sujeito e objeto da relação de poder. Cumpre ainda destacar, conforme também alertado por Foucault, o quanto o panóptico permite a economia do poder, visto que é possível observar a maior quantidade possível de

pessoas com um número reduzido de inspetores. Acrescenta-se ainda a intenção de que o mecanismo do panóptico se espraia para o resto do tecido social, para fora das instituições fechadas, assim através do poder disciplinar a sociedade torna-se, em igual medida, disciplinar (GUNDALINI; TOMIZAWA, 2013, p. 26).

Nesse sentido, Foucault vai além de Bentham ao considerar o panóptico mais do que apenas uma estrutura arquitetônica, e sim como um princípio de organização social, o panoptismo.

> Haveria, numa analogia, uma inversão do papel do circo dentro da sociedade. Se no circo há uma multidão observando o espetáculo feito por uma minoria, na sociedade, a partir do panoptismo, haveria uma minoria observando a maioria. Indo mais além, Foucault afirma que nesse caminho, o homem acabaria por se tornar parte da engrenagem de vigilância, sendo às vezes observado e às vezes observador, de acordo com as necessidades ditadas por quem exerce o poder (COUTO, 2007, p.143).

Enquanto Bentham apresenta uma solução técnica para um problema técnico, qual seja: como gerir de maneira mais eficiente e mais utilitária possível pessoas em uma instituição fechada; Foucault identifica um novo princípio de organização social, considerada uma fórmula geral que sintetiza um processo histórico em que um novo tipo de sociedade é formado a partir de uma nova lógica de poder, o poder disciplinar (GUNDALINI; TOMIZAWA, 2013, p. 30-31).

Sob esta ótica, o poder disciplinar produz uma sociedade com indivíduos úteis economicamente e politicamente dóceis por intermédio do adestramento e treinamento (BRÍGIDO, 2013, p. 66).

Logo, o conceito da eterna vigilância é fundamental para compreender que, na verdade, a vigilância não vem do outro e sim do próprio ser vigiado que por isso está constantemente sendo punido. Dessa forma, “o corpo é ajustado ao tempo e, uma vez disciplinado, gerará gestos eficientes” (BRÍGIDO, 2013, p. 68)

A eficiência do poder disciplinar se deve a constante vigilância. Após o uso da docilização dos corpos, processo pelo qual o indivíduo passa desde a infância de condicionamento e submissão, pela sociedade disciplinar, há a implantação de um

sistema de controle muito mais sutil que atua através da docilização não mais dos corpos, mas das mentes, como ocorre na atual sociedade de informação.

Vinte anos depois, outro filósofo revisita o conceito de disciplina e se apropria da ideia de panóptico, o francês Gilles Deleuze que se utilizou do termo para descrever que já "estamos em pleno processo de instalação progressiva e dispersa de um sistema de controle e dominação" (DELEUZE,1992, p. 215).

Deleuze ainda escreveu, bem antes da era digital, no início dos anos 90 que "estamos entrando nas sociedades de controle que não funcionam mais por confinamento, mas por controle contínuo e mensagens instantâneas" (1992, p. 221).

Nesse sentido,

> A sociedade disciplinar passa a ser um sistema de controle contínuo, intensificado por uma tecnologia sofisticada que produz novos regimes visíveis e enunciáveis. A sociedade de controle é a sociedade das telas, dos computadores, dos satélites, dos celulares, do processamento instantâneo de dados em rede, da realidade vigiada e examinada por monitores (MELLO, 2018, p. 135).

Desse modo, passa-se para uma era do poder de controle, em que o exercício do poder não se baseia mais na disciplina, mas no controle.

> [...] Enquanto a disciplina demanda por um longo e descontínuo período de tempo necessário ao adestramento dos comportamentos, o controle se exerce em curto prazo, além de ser contínuo e ilimitado. Por isto, a eficiência do controle produz efeitos mais rápidos, haja vista o desenvolvimento da informática que, por meio de uma linguagem binária, criou um recurso simples, a senha, capaz de identificar e de localizar as pessoas onde quer que estejam, e o que quer que estejam fazendo (FERREIRA, 2014, p. 114)

Para que se tenha sucesso na implantação desse sistema de controle é imprescindível que as pessoas não percebam que estão, de fato, sendo controladas, esse controle deve passar despercebido.

Ao transportar tais ideias para o contexto atual, em que as novas tecnologias auxiliam na captação e análise de dados pessoais, "podemos supor que o estado de

emergência chegará ao fim, mas essas tecnologias permanecerão e a vigilância estatal será fortemente impulsionada pela crise atual" (DELANTY, 2020, p. 6).

2.2 O PARADOXO ENTRE SEGURANÇA E LIBERDADE NO MUNDO PÓS 11 DE SETEMBRO

Os atentados de 11 de setembro mudaram a percepção de segurança, fazendo com que a sociedade enfrentasse, logo no início do século, o paradoxo entre direitos, à primeira vista conflitantes, a liberdade *versus* a segurança.

Após o ataque terrorista, houve diversas mudanças significativas em relação à segurança do tráfego aéreo, com mecanismos de controle intensos nos aeroportos não apenas nos Estados Unidos da América, como em todos os aeroportos ao redor do mundo.

Com o advento de políticas que visavam reforçar a segurança dos aeroportos, o governo norte-americano, por meio da publicação do *USA PATRIOT Act*[6]*,* publicado em 26 de outubro de 2001, previa diversas determinações que violavam garantias constitucionais americanas, especialmente no que tange às questões de privacidade, com adoções de práticas que restringiam as liberdades individuais, consideradas um pilar da democracia americana.

Uma das medidas de segurança adotadas pelos aeroportos americanos após os atentados foi uso do *backscatter,* o escâner corporal. Popularmente conhecido como "raio X", o *backscatter* gerou muita polêmica logo após a sua implementação.

A tecnologia utilizada no escâner corporal gerava imagens da pessoa completamente nua, sendo possível, inclusive, visualizar as partes íntimas no momento em que os passageiros eram inspecionados pelo equipamento de segurança antes do embarque.

Esse novo equipamento gerou polêmica há época e foi considerada uma das maiores invasões de privacidade de todos os tempos, já que não foram encontrados registros

[6] Disponível em: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf

de exigência da nudez pública para garantir a segurança por nenhum governo nem durante a Segunda Guerra Mundial.

Após a polêmica, o equipamento de escâner corporal foi aprimorado e, atualmente, já não mostra tantos detalhes para além da sua finalidade, limitando-se a detectar tão somente a presença de materiais proibidos.

Essa medida de segurança desproporcional tomada pelo governo norte-americano logo após os atentados pode trazer à baila as mesmas reflexões em relação aos limites do direito à privacidade e liberdades individuais. Inquestionavelmente as ações e estratégias traçadas como resposta imediata ao ataque terrorista eram, naquele momento, imprescindíveis para garantir a segurança e evitar a ocorrência de novos episódios. Entretanto, essas medidas não devem ultrapassar a finalidade a que se propõem, qual seja a segurança pública.

Uma pesquisa de opinião da *Princeton Survey Reaserch Associates* (ROPER CENTER, 2001) feita apenas dez dias após os atentados entrevistou 1005 cidadãos estadunidenses, por telefone, com a seguinte pergunta: “Para controlar o terrorismo no país, você acha que será necessário às pessoas comuns renunciarem a algumas de suas liberdades civis, ou não?”.

De acordo com os resultados obtidos pela pesquisa, 63% dos entrevistados entendiam ser necessária uma redução de suas liberdades civis para o combate ao terrorismo (ROPER CENTER, 2001).

Apesar do resultado da pesquisa realizada pela *Princeton Survey Reaserch Associates* ter demonstrado que a maior parte dos norte-americanos apoiavam medidas no combate ao terrorismo, uma outra pesquisa de opinião, também feita por telefone, pelo *Los Angeles Times* apontou que uma parte relevante (37%) dos entrevistados estavam preocupados com a eminência de limitação de suas liberdades civis.

Essas pesquisas corroboram o paradoxo entre liberdade e segurança já naquele primeiro momento de tensão entre os estadunidenses.

Além disso, os atentados às torres gêmeas também deram início a uma negociação muito intensa entre o governo norte-americano e a União Europeia, tendo o grupo europeu de autoridades de proteção de dados especial importância para evitar que houvesse uma forte limitação das liberdades dos seus cidadãos. Isto porque, os métodos de vigilância de dados são freqüentemente apresentados como uma forma eficiente de triagem de identidade, com capacidade de promover os objetivos do policiamento preventivo.

As denúncias de Edward Snowden quanto as atividades da *National Security Agency* – NSA por intermédio do programa *Prism* - programa de espionagem de coleta de informações, provocaram reações de grande relevância em nível político, com posicionamentos das presidentes da Alemanha, Ângela Merkel e do Brasil, Dilma Rousseff.

O Programa *Prism,* também foi usado para interceptar e coletar metadados de todas as ligações telefônicas dos consumidores da empresa VERIZON, uma das maiores empresas americanas do ramo de telecomunicações. Por meio desse método de espionagem, era possível saber quem ligou, a hora, a duração e o local da chamada. Diversos registros de cidadãos americanos que não possuíam qualquer ligação criminal foram coletados (GREENWALD, 2013).

Não apenas cidadãos americanos foram alvo desses registros, mas também pessoas de outras partes do mundo, que foram alvo do acesso de dados pelo *Prism,* que também coletava informações dos usuários de empresas como Google e Facebook (GELLMAN; POITRAS, 2013).

Todos esses eventos podem ser vistos como desdobramentos da vigilância constante instaurada pelo Governo dos Estados Unidos a partir dos atentados de 11 de setembro e, marcaram de forma relevante o contexto geopolítico internacional.

Evidentemente, diante de um cenário em que predominavam o medo e o caos constante na eminência de novos ataques, o contexto de segurança precisava ser reforçado e alterado, através da adoção de novos parâmetros e medidas mais

direcionadas. No entanto, não se deve perder de vista a coexistência entre a segurança e a liberdade.

2.3 A NARRATIVA DA VIGILÂNCIA COMO GARANTIDORA DO BEM ESTAR

A evolução do estado de vigilância não se limitou apenas ao território norte-americano, mas colocou todos as demais nações em estado de alerta. Para além da atenção a possíveis ataques terroristas, as atenções se voltavam para a segurança *lato sensu*.

Com o avanço da tecnologia, esforços foram despendidos em mecanismos de segurança e controle total de tudo e de todos. Dentre esses mecanismos, o reconhecimento facial pode ser considerado um dos avanços tecnológicos mais recentes e também um dos meios mais utilizados no controle dos indivíduos.

Um exemplo desse controle exacerbado é o Sistema *Skynet* na China, que consegue mapear um determinado segmento da população por meio das suas mais de vinte milhões de câmeras espalhadas pelo país. Esse sistema chinês detecta pedestres em tempo real e é capaz de identificar características como idade, gênero e até mesmo as roupas, além de ser possível a identificação de veículos.

Na pandemia, o governo chinês utilizou-se da tecnologia do reconhecimento facial para checar a temperatura das pessoas e, inclusive, para controlar se as pessoas estavam, de fato, em casa cumprindo a quarentena e averiguar a utilização de máscaras. Ainda sobre as medidas adotadas na China durante a pandemia:

> Toda a infraestrutura para a vigilância digital se mostrou agora ser extremamente eficaz para conter a epidemia. Quando alguém sai da estação de Pequim é captado automaticamente por uma câmera que mede sua temperatura corporal. Se a temperatura é preocupante todas as pessoas que estavam sentadas no mesmo vagão recebem uma notificação em seus celulares. Não é por acaso que o sistema sabe quem estava sentado em qual local no trem. As redes sociais contam que estão usando até drones para controlar as quarentenas. Se alguém rompe clandestinamente a quarentena um drone se dirige voando em sua direção e ordena que regresse à sua casa. Talvez até lhe dê uma multa e a deixe cair voando, quem sabe. Uma situação que para os europeus seria distópica, mas que, pelo visto, não tem resistência na China (HAN, 2020, s./p.)

Muito embora não seja uma novidade o 'tecnonacionalismo chinês' por ser considerada um país onde não há uma preocupação e sequer uma cultura em relação à preservação da privacidade, a tecnologia do reconhecimento facial já tem sido utilizada em outros países, inclusive no Brasil.

No período de carnaval em 2019, o governo do Rio de Janeiro se utilizou dessa tecnologia para controlar criminosos que eventualmente estivessem nas ruas e teve êxito na prisão de quatro pessoas com mandados de prisão em aberto[7].

Foram instaladas vinte e oito câmeras de reconhecimento facial em Copacabana, um sistema que era parte de um projeto piloto da Polícia Militar do Estado do Rio de Janeiro. O sistema em questão era capaz de comparar as fotos de procurados que estavam no banco de dados da Polícia Militar com os rostos das pessoas filmadas em tempo real.

A utilização desse sistema gerou preocupação por parte do Idec – Instituto Brasileiro de Defesa do Consumidor, tendo solicitado à PM que esclarecesse a segurança dos dados coletados por meio do sistema de reconhecimento facial, sob o argumento de que é necessário garantir que essas informações coletadas por esse tipo de tecnologia não sejam utilizadas para nenhuma outra finalidade.

A carta enviada pelo Idec reconheceu a importância do uso dessa tecnologia para a segurança pública, entretanto, alertou para a necessidade do tratamento adequado das informações coletadas pela tecnologia:

> Consideramos que o desenvolvimento de novos instrumentos de Segurança Pública é prioritário e urgente, especialmente no estado do Rio de Janeiro, e deve contar com o apoio de toda a sociedade. Contudo, a eventual ausência de cuidados básicos no tratamento dessas informações, como acesso do fornecedor da tecnologia aos dados gerados, pode gerar riscos para os consumidores. Por isso, o Idec, no exercício de sua missão de defender os consumidores, deseja contribuir para que tais inciativas sejam executadas sem sacrificar direitos de privacidade dos cidadãos, cujos dados pessoais podem ser indevidamente utilizados por terceiros para práticas de outras ilegalidades. (IDEC, 2019)

[7] Veja a reportagem em: https://noticias.r7.com/rio-de-janeiro/cameras-de-reconhecimento-facial-levam-a-4-prisoes-no-carnaval-do-rio-08032019

Na mesma carta enviada pelo Idec, foram enviados os seguintes questionamentos à Secretaria da Polícia Militar do Rio de Janeiro:

> Considerando que falhas e omissões de cuidado na condução desse projeto podem impactar de forma irreparável direitos difusos e individuais dos cidadãos, e diante da proximidade de sua implementação, o Instituto Brasileiro de Defesa do Consumidor se dirige respeitosamente à Secretaria da Polícia Militar do Rio de Janeiro para consultá-los sobre os cuidados e as garantias que estão sendo adotadas para evitar externalidades não previstas no funcionamento desse sistema de vigilância, e que podem evitar os graves danos mencionados:
>
> 1. Quanto à parceria com a empresa Oi, que desenvolveu o software de reconhecimento facial utilizado. Quais os termos em que essa parceria foi firmada? O que levou à decisão final pela empresa? Houve processo de licitação em concorrência com outras empresas? Qual a contrapartida à empresa Oi, considerando que foi afirmado que a implementação da ferramenta terá "custo zero" ao governo do Estado?
>
> 2. Quanto à segurança da ferramenta. Houve avaliação a respeito dos potenciais riscos e impacto à segurança dos cidadãos? Quais as garantias de segurança levadas à cabo pela Secretaria da Polícia Militar para evitar danos ao banco de dados, como possíveis vazamentos ou utilização inadequada das informações coletadas? O processo de escolha da tecnologia levou em consideração potenciais falhas que ela possa vir a apresentar?
>
> 3. Quanto ao funcionamento da tecnologia. A realização do reconhecimento facial pelo software ocorre em tempo real? Há procedimentos posteriores de anonimização dos dados pessoais coletados? Há posterior descarte das informações e imagens não utilizadas pela PMERJ? Por quanto tempo as imagens seriam armazenadas? (IDEC, 2019)

A preocupação do Idec com o tratamento adequado das informações coletadas e com o direito à privacidade em relação ao uso de câmeras inteligentes veio antes mesmo do envio da carta à Secretaria da Polícia Militar do Rio de Janeiro. Uma notícia publicada no site do Instituto em 24 de janeiro de 2019 já alertava para possíveis problemas com o uso do sistema[8].

Inicialmente, a preocupação era com a terceirização do serviço à empresa de telefonia Oi, que já havia sido multada em 2014 pela criação de um software que vendia informações acerca de seus clientes de internet sem o consentimento destes.

[8] Disponível em: https://idec.org.br/idec-na-imprensa/camera-inteligente-no-rj-tera-sistema-da-oi-multada-por-violar-privacidade

A TNL PCS, uma divisão da concessionária de serviços de telecomunicações Oi, foi multada em três milhões e quinhentos mil reais pelo Ministério da Justiça, através do Departamento de Proteção e Defesa do Consumidor (DPDC), por ter vendido informações de seus clientes para agências de publicidade. Segundo o DPDC, essa prática teria violado os princípios da boa-fé e da transparência. Essa foi a primeira violação comprovada da neutralidade da rede definida pelo Marco Civil da Internet[9].

O Idec também interveio na utilização de câmeras inteligentes em São Paulo, tendo entrado com uma Ação Civil Pública contra a Via Quatro, empresa concessionária do Metrô na capital paulistana. As câmeras estavam presente nos monitores publicitários instalados no metrô da Linha 4-Amarela nas plataformas de embarque e desembarque e tinham por objetivo capturar as reações dos passageiros a cada anúncio publicitário que era exibido nos respectivos monitores.

A concessionária Via Quatro foi multada em 100 milhões de reais pela coleta indevida de dados. Na recente sentença da 37ª Vara Cível da Comarca do Estado de São Paulo, a juíza destacou que:

> A situação exposta no caso concreto é muito diferente da captação de imagens por sistemas de segurança com objetivo de melhoria na prestação do serviço, segurança dos usuários ou manutenção da ordem, o que seria não só aceitável, mas necessário diante da obrigação da fornecedora de serviço público zelar pela segurança de seus usuários dentro de suas dependências. É evidente que a captação da imagem ora discutida é utilizada para fins publicitários e consequente cunho comercial, já que, em linhas gerais, se busca detectar as principais características dos indivíduos que circulam em determinados locais e horários, bem como emoções e reações apresentadas à publicidade veiculada no equipamento. Ademais, restou incontroverso que os usuários não foram advertidos ou comunicados prévia ou posteriormente acerca da utilização ou captação de sua imagem pelos totens instalado nas plataformas, ou seja, os usuários nem mesmo tem conhecimento da prática realizada pela requerida, o que viola patentemente o seu direito à informação clara e adequada sobre os produtos e serviços, bem como à proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, ambos elencados no artigo 6º, III e IV do Código de Defesa do Consumidor (TJ-SP – ACP 1090663-42.2018.8.26.0100, 37ª Vara Cível do Foro Central Cível da Comarca de São Paulo).

[9] Disponível em: https://oglobo.globo.com/economia/defesa-do-consumidor/oi-multada-em-35-milhoes-por-invasao-de-privacidade-feita-por-velox-13348505

A sentença considerou, portanto, que a conduta da concessionária violava o direito à imagem dos consumidores usuários do serviço público, bem como as disposições sobre a proteção especial que deveria ser dada aos dados pessoais sensíveis e, também, a violação de direitos básicos do consumidor, especificamente no tocante à informação e à proteção com relação às práticas comerciais abusivas.

Todos esses casos apresentados até aqui chamam a atenção para o risco que envolve a terceirização dos serviços públicos, especialmente os de segurança pública. A terceirização desses serviços é uma preocupação que ganha ainda mais relevância quando se está diante de empresas que ofertam essa tecnologia e que já possuem algum histórico de violação à privacidade, como a utilização indevida de dados pessoais, por exemplo.

Para além do histórico dessas empresas, não é possível estabelecer ao certo um controle muito efetivo por parte do Estado acerca desses dados, já que o controle de toda a tecnologia – ou pelo menos boa parte desse controle – fica por conta das empresas e não do Estado.

Informações como hábitos simples do dia a dia das pessoas são muito valiosos para determinadas empresas, de modo a dar suporte a chamada publicidade direcionada, um método utilizado com muita frequência pelas empresas como *Google* e *Facebook,* que possuem um armazenamento muito significativo de dados pessoais, inclusive de caráter sensível. Segundo Eli Pariser (2012, p. 41), esses dados utilizados pela *Google* e *Facebook,* embora tenham estratégias diferentes, possuem os mesmos propósitos:

> A questão é que a base dos dois negócios é essencialmente a mesma: publicidade direcionada, altamente relevante. Os anúncios contextuais que o Google coloca ao lado dos resultados de pesquisas e em sites são sua única fonte significativa de lucro. E, embora as finanças do Facebook não sejam reveladas ao público, alguns *insiders* já deixaram claro que a publicidade está no âmago dos rendimentos da empresa. O Google e o Facebook tiveram pontos de partida e estratégias diferentes — um deles apoiou-se nas relações entre informações, o outro nas relações entre pessoas-, porém, em última análise, os dois competem pelos mesmos dólares advindos da publicidade. Do ponto de vista do anunciante on-line, a questão é simples: qual empresa irá gerar o maior retorno por cada dólar investido? É aí que a relevância entra na equação. As massas de dados acumuladas pelo Facebook e pelo Google têm dois propósitos: para os usuários, os dados são a chave para a oferta de notícias e resultados pessoalmente relevantes; para os anunciantes, os

> dados chave para encontrar possíveis compradores. A empresa que tiver a maior quantidade de informações e souber usá-las melhor ganhará os dólares da publicidade.

Desse modo, observa-se o valor econômico e a relevância de mercado que esses dados pessoais possuem. Nas palavras de Marcelo Cardoso Pereira (2011, p. 186-188):

> O êxito dos negócios na denominada "economia digital" está pendente de que os Prestadores de Serviços da Sociedade da Informação possam apresentar produtos e serviços adequados a pessoas adequadas. Para isso, devem, esses prestadores (...), saber os gostos, preferências, hábitos, costumes, etc., de potenciais clientes que não são outros, como já dissemos, senão os usuários da Rede.

Para além do campo publicitário, o vazamento dessas informações que aparentemente são simplórias pode acarretar risco à própria segurança pública. Isso porque pode ocorrer o vazamento de dados para organizações criminosas, que poderão utilizar essas informações para mapear determinados hábitos ou situações específicas para a prática de crimes.

A preocupação com a segurança sempre foi foco de atenção da maioria dos países, especialmente aqueles que são constantemente ameaçados por atentados terroristas. Com a pandemia de COVID-19, o inimigo mudou. O centro das atenções passou a ser o controle e monitoramento da propagação do vírus.

A tecnologia que vinha sendo constantemente utilizada para monitoramento da segurança pública passou a ser utilizada com escopo sanitário de vigilância.

> A narrativa que justifica tais ações supõe que o bem-estar – traduzido, no momento, por controle e eliminação da covid-19 – viria com uma vigilância maior sobre as ações cotidianas dos cidadãos, garantindo-os um mínimo de bem-estar. Para tanto, seria necessário o uso de rastreadores e outros artefatos para a extração de dados de celulares, possível com parcerias estabelecidas com operadoras de telefonia. Identificar padrões de movimentos das pessoas e verificar se as pessoas estariam seguindo recomendações do governo de distanciamento social seriam algumas das atividades que justificariam tal uso. Entretanto, a maioria das ações governamentais vem sendo implementadas sem considerar questões como a estipulação de um prazo de duração da vigilância ou o tipo de proteção de privacidade que seria garantida ao cidadão durante o processo (FREITAS; CAPIBERIBE; MONTENEGRO, 2020, p. 193).

Um exemplo prático e claro dessa mudança é o serviço de segurança *Shin Bet* em Israel, um serviço que antes era utilizado para dar suporte ao programa de vigilância de combate ao terrorismo passou a ser usado para o monitoramento de pacientes com coronavírus ou eventuais portadores do vírus[10]. O serviço israelense foi alvo de apreciação pela Corte de Israel, que entendeu não ser razoável a sua utilização sem uma legislação especial que autorizasse o programa e estabelecesse limites. A Corte afirmou ainda que o *Shin Bet* não teria autoridade para fazer o rastreamento de civis como forma de conter o avanço da crise sanitária, justamente em razão do risco de violação à privacidade e à democracia[11].

Outros países pelo mundo também se apropriaram do uso de tecnologias para o controle sanitário. Em Moscou, a polícia conseguiu localizar 200 pessoas que teriam inobservado as regras de isolamento impostas pelo governo, baseando-se em uma reportagem de um jornal russo que teria apontado supostos infratores que estavam fora de suas respectivas residências[12].

Na Rússia, dados telefônicos e informações relativas às transações de cartões de crédito foram utilizadas para mapear pessoas que teriam tido contato com pessoas contaminadas pelo vírus. Além dessa checagem de dados críticos como esses, o sistema russo de monitoramento contou com 170 mil câmeras com mecanismo de reconhecimento facial[13].

Um sistema parecido foi utilizado na Coreia do Sul, que também se apropriou dos dados relativos às transações de cartão de crédito, geolocalização de aparelhos telefônicos e imagens de câmeras de vigilância para a identificação de pessoas que pudessem estar portando o vírus da COVID-19[14].

---

[10] Disponível em: https://www.jota.info/opiniao-e-analise/colunas/juiz-hermes/ferramentas-tecnologicas-e-controle-da-pandemia-14062020

[11] Disponível em https://edition.cnn.com/2020/03/29/europe/russia-coronavirus-authoritarian-tech-intl/index.html

[12] Disponível em: https://edition.cnn.com/2020/03/29/europe/russia-coronavirus-authoritarian-tech-intl/index.html

[13] Disponível em: https://www.themoscowtimes.com/2020/03/25/coronavirus-outbreak-is-major-test-for-russias-facial-recognition-network-a69736

[14] Conferir a reportagem em: https://www.newyorker.com/news/news-desk/seouls-radical-experiment-in-digital-contact-tracing

Conforme demonstrado, são vários os países que se valem da coleta de dados para o monitoramento da população em decorrência da pandemia, todavia, como observado por Rondon, já há “pesquisas e estudos relatando que este tipo de dado é pouco efetivo no combate de uma epidemia” (RONDON, 2020).

Devido à natureza rotinizada e administrativa liderada pelo Estado, a vigilância em massa é normalizada.

> Em outras palavras, o conjunto de ações associadas às políticas de prevenção e tratamento da pandemia poderia se estender *ad infinitum* e, com isso, gerar um Estado de exceção permanente ao lado de novas formas de socialização, tendo como justificativa moral a proteção da vida, no sentido de “vida biológica” (LACERDA, 2020, p. 75).

Assim, os mecanismos de controle demonstram a necessidade de estabelecer critérios objetivos para evitar que determinadas externalidades limitem de forma drástica o direito à privacidade, à intimidade e à proteção de dados.

3 BREVES REFLEXÕES ACERCA DA PROTEÇÃO DE DADOS PESSOAIS E O DIREITO À PRIVACIDADE

O tema de proteção de dados surge muito antes das legislações que dele tratam. Há uma falsa percepção de se estar vivendo uma grande revolução, de ser o século XXI e, mais particularmente a segunda década deste século, o momento histórico de ruptura paradigmática em que grandes movimentos, inclusive legislativos que rompem os tecidos clássicos da estrutura social.

Urge ressaltar que temas relacionados ao direito digital e à proteção de dados, especialmente no contexto em que a Sociologia vê a manifestação daquilo que seria uma sociedade de vigilância, se defronta com a disparidade inegável entre o ritmo de desenvolvimento tecnológico e a capacidade do Estado de atuar no contraponto a essa galopante e inevitável inovação. A tecnologia, ao mesmo tempo que nos ajuda e dinamiza a vida em sociedade, também pode ensejar novas situações violadoras de direitos.

Quando se tem discussões doutrinárias emergindo, especialmente ao longo da década de 1980 e 1990 sobre conceitos como vigilância e sociedade de vigilância, surge efetivamente uma dogmática relacionada ao Direito e a interação com esse novo universo que a tecnologia nos traz notadamente após o surgimento e a popularização da *internet*.

Nesse sentido, os dados passam a serem vistos como instrumento de poder e controle da sociedade, uma vez que podem sofrer manipulações para persuasões que vão além daquilo que seria razoável, tornando-se primordial conhecer e analisar os riscos frequentemente denunciados de um estado de vigilância, incubados em nossa sociedade por certos usos da tecnologia da informação.

Dessa forma, é inegável a necessidade de se compreender toda a complexidade dos impactos desse novo cenário e, de que maneira o avanço na ordem jurídica se faz necessário para disciplinar a inovação.

3.1 OS PARADIGMAS NORTEADORES DA PROTEÇÃO DE DADOS

O tema da proteção de dados e a necessidade de sua regulação surge a partir do Estado Moderno, isso porque após a Segunda Guerra Mundial, com o avanço da ciência computacional, o Estado passa a compreender que as informações pessoais dos cidadãos são de grande valia no planejamento de suas ações para um crescimento ordenado (BIONI, 2019, p. 174).

Conforme destaca Laura Schertel Mendes (2014, p. 33)

> [...] a utilização massiva de dados pessoais a partir da segunda metade do Século XX pode ser associada a duas características principais do Estado pós-industrial: a burocratização (dos setores público e privado) e o desenvolvimento da tecnologia da informação. Ambos os fenômenos, que podem ser considerados transnacionais, suscitaram o processamento dos dados pessoais por governos das mais variadas ideologias políticas e por grandes corporações empresariais, com finalidades estatísticas, administrativas, negociais e investigativas.

Nesse contexto, em 1965 o escritório do orçamento norte-americano (*Bureau of Budget*) apresentou proposta para a estruturação de uma central única que reuniria informações de caráter pessoal dos cidadãos disponíveis em vários órgãos da administração federal, denominada de *National Data Center*, como: unificação dos cadastros do CENSO – registros trabalhistas, fisco e previdência em um único banco de dados (MENDES, 2014, p. 37-38).

Em razão da criação desses grandes bancos centralizadores houve um receio generalizado de que essa concentração nas mãos da administração pública implicasse em um excessivo crescimento de poder, representando uma afronta à tradição liberal norte-americana que, eventualmente, poderia gerar uma ameaça à própria democracia.

Dessa forma, surgiram iniciativas semelhantes em outros países, tanto nos Estados Unidos quanto na Europa, visando a proteção de dados dos cidadãos. Pode-se citar, a título de exemplificação, as Leis do Estado Alemão de Hesse (1970), Lei de Dados da Suécia (1973), Estatuto de Proteção de Dados do Estado Alemão de *Rheinland-*

Pfalz (1974) e a Lei Federal de Proteção de Dados da Alemanha (1977). Já nos EUA, o *Fair Credit Reporting Act* (1970) e o *Privacy Act* (1974) (MENDES, 2014, p. 45).

Essas normas tinham por finalidade a descrição de procedimentos a serem adotados por bancos de dados (MENDES, 2014, p. 38-39) e marcam a primeira geração de proteção dos dados pessoais[15]. Além disso, havia o controle na criação desses bancos de dados, em que eram necessárias autorizações para seu funcionamento (BIONI, 2019, p. 174). Contudo, tais legislações se mostraram insuficientes, ao não regularem, por exemplo, situações em que os dados poderiam ser coletados.

Em 1979 a Organização das Nações Unidas (ONU) começa a impulsionar um movimento para a proteção de dados em âmbito internacional a partir da organização de ações e conferências relativas ao tema, notadamente a *International Conference of Data Protection and Privacy Commissiners*, que acontece anualmente e possibilitou que diversas nações europeias desenvolvessem suas legislações acerca da proteção de dados, é o caso das Constituições de Portugal, Espanha e Áustria que incluíram o direito à privacidade de dados em seu texto constitucional.

Já na década de 1980 emergem dois instrumentos internacionais importantes, a saber: as Diretrizes da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais[16] e a Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, também conhecida como Convenção n.º 108, do Conselho da Europa[17], primeiro instrumento internacional referente à proteção das pessoas quanto à eventuais abusos ocorridos no tratamento de dados pessoais.

Assim, é possível vislumbrar que a segunda geração de leis destinadas à proteção de dados passa a se preocupar não somente com a base de dados estatais, mas, de

[15] Taxonomia desenhada por Viktor Mayer-Schoneberger.
[16] Disponível em: https://www.oecd.org/sti/ieconomy/15590254.pdf
[17] Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37

igual forma, a proteção recai sobre bases de dados na esfera privada (BIONI, 2019, p. 175). Com isso,

> A segunda geração de leis transfere para o próprio titular dos dados a responsabilidade de protegê-los. Se antes o fluxo das informações pessoais deveria ser autorizado pelo Estado, agora cabe ao próprio cidadão tal ingerência que, por meio do consentimento, estabelece as suas escolhas no tocante à coleta, uso e compartilhamento dos seus dados pessoais (BIONI, 2019, p.174).

Desse modo, o indivíduo passa a ter maior controle e autonomia sobre o fluxo de suas informações pessoais. Tal protagonismo ganha ainda mais espaço na terceira geração de leis, que busca assegurar a participação e controle do indivíduo sobre todo percurso realizado por seus dados pessoais, isto é, desde a coleta, passando pelo armazenamento até o compartilhamento de dados (BIONI, 2019, p. 175-176).

Nesse sentido, destaca-se a Resolução nº 45/1995 que estabelecia as Diretrizes para a Regulação de Ficheiros Informatizados de Dados de Caráter Pessoal e tinha por objetivo escolher os princípios relativos às garantias que devem ser aplicados na legislação nacional: princípio da legalidade e equidade; princípio da exatidão; princípio da finalidade especificada; princípio da não discriminação[18].

A partir dos anos 2000, a revolução digital e seus desdobramentos tornou-se um dos principais assuntos debatidos pela União Europeia, haja vista que, a integração econômica e social dos países que compõe a comunidade fomentou um maior fluxo transfronteiriço de dados pessoais, tornando-se necessária à regulação do uso dos meios digitais e as repercussões da Internet na privacidade das pessoas no mundo *online*.

Este cenário propiciou a promulgação do Regulamento Geral de Proteção de Dados Pessoais Europeu nº 679 (GDPR)[19], aprovado em 27 de abril de 2016, cujo objetivo segundo o preâmbulo do GDPR, é:

---

[18] Para acesso ao documento completo: https://gddc.ministeriopublico.pt/sites/default/files/diretrizes-protecaodados.pdf

[19] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT

> a) contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união econômica, para o progresso econômico e social, a consolidação e a convergência das economias no nível do mercado interno e para o bem-estar das pessoas físicas; b) assegurar um nível coerente de proteção das pessoas físicas no âmbito da União e evitar que as divergências constituam um obstáculo à livre circulação de dados pessoais no mercado interno; c) garantir a segurança jurídica e a transparência aos envolvidos no tratamento de dados pessoais, aos órgãos públicos e à sociedade como um todo; d) impor obrigações e responsabilidades iguais aos controladores e processadores, que assegurem um controle coerente do tratamento dos dados pessoais; e) possibilitar uma cooperação efetiva entre as autoridades de controle dos diferentes Estados-Membros (PINHEIRO, 2018).

Outrossim, este Regulamento reforçou a ideia de controle pelos titulares sobre os seus dados pessoais. Neste sentido, cumpre destacar que a propriedade sobre os dados pessoais é diferente de controle pelos titulares dos dados, como explica Lorenzon (2021, p. 44)

> É importante ressaltar que a GDPR não fornece aos indivíduos (titular dos dados) propriedade sobre seus dados, mas, sim, o controle sobre o que irá acontecer com eles — como serão armazenados, para que fim serão utilizados e com quem serão compartilhados. Nesse sentido, algumas das garantias da lei aos titulares são o direito de exigir que empresas deletem seus dados pessoais (desde que não sejam necessários para fins científicos, históricos, de saúde pública e estatísticos); direito de acessar e transferir seus dados pessoais de um serviço para o outro sem deixar rastros; e direito à transparência total sobre qualquer operação realizada com seus dados.

Assim, a intenção da GDPR foi aumentar a confiança dos consumidores na tentativa de impulsionar o crescimento econômico, emprego e inovação tecnológica na União Europeia.

Vê-se que a tutela de dados não está ligada apenas a uma história política, cultural e jurídica de determinados países, mas uma grande questão global. De fato, existem hoje diversas propostas para o que se pode chamar de “Declaração de Direitos na Internet” ou, como chama Tim Berners-Lee, criador da Web, uma Carta Magna da Internet[20].

Sob esta ótica, Stefano Rodotà é enfático ao afirmar que “a proteção de dados pode ser vista como a soma de um conjunto de direitos que configuram a cidadania do novo milênio” (RODOTÀ, 2008. p. 14).

[20] Sobre o tema, Berners-Lee escreveu o artigo “We need a Magna Carta for The Internet”’ publicado na revista New Perspectives Quarterly.

Nesta, como em outras matérias, a construção de normas comuns se dá por meio da consolidação e harmonização entre diversas iniciativas nacionais, que possuem as mesmas características.

Nos últimos tempos, confrontam-se dois modelos de proteção de dados – o primeiro deles baseado na autorregulamentação e em uma certa confiança nos instrumentos de mercado e um segundo modelo que, por sua vez, considerou desde o início que tal tutela era constitucionalmente relevante.

3.2 A PROTEÇÃO DE DADOS PARA ALÉM DA PRIVACIDADE

Normalmente, quando se fala sobre dados pessoais associa-se a ideia de privacidade de dados. Mas, afinal o que é a privacidade? E qual a relação entre privacidade e dados pessoais?

A noção de privacidade surge a partir da dicotomia entre a esfera pública e privada, "sendo a sua lógica centrada na liberdade negativa de o indivíduo não sofrer interferência alheia" (BIONI, 2019), isto é, como exigência de ausência de intervenção do Estado na vida privada. Stefano Rodotà explicita que a privacidade era considerada um privilégio de determinado grupo, notadamente a burguesia:

> O isolamento era privilégio de pouquíssimos eleitos ou daqueles que, por necessidade ou opção, viviam distantes da comunidade – místicos ou monges, pastores ou bandidos. Esta possibilidade depois se estendeu a todos que dispunham dos meios materiais que lhe permitissem reproduzir, mesmo no ambiente urbano, condições que satisfaziam a esta nova necessidade de intimidade [...].
> A privacidade configura-se assim como uma possibilidade da classe burguesa, que consegue realizá-la sobretudo graças às transformações socioeconômicas relacionadas à Revolução Industrial. [...] (RODOTÀ, 2008, p. 26-27).

Assim, a tutela à privacidade se desenvolve de maneira mais acentuada no final do século XIX, a partir da obra "*A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract"* do juiz Cooley, considerada um marco nos Estados Unidos

ao criar o “direito de ser deixado só”[21] (COOLEY, 1879, p. 29), expressão que foi repetidamente utilizada ao longo do tempo.

Mais adiante, em 1890, os advogados Samuel Dennis Warren e Louis Demitz Brandeis escrevem o artigo intitulado “*The right to privacy*”[22], escrito que expõem que o direito de propriedade, quando invocado para proteger os bens imateriais, já não seria suficiente no mundo moderno, de modo que, a proteção da vida privada se relacionaria com o direito à privacidade que, por sua vez, era considerado o direito mais amplo da personalidade (OLIVEIRA; LOPES, 2019), sendo o indivíduo responsável por decidir quais informações de sua vida privada poderiam ser compartilhadas.

Ademais, Leonardo Zanini sugere que Warren e Brandeis ao tratarem do direito à privacidade estabelecem como garantia do indivíduo “[...] uma ampla liberdade contra intromissões não desejadas em sua vida, tutelando seus pensamentos, sentimentos, emoções, dados pessoais e até mesmo o nome” (ZANINI, 2015, p. 11).

Em outro sentido, Alan Westin afirma que a privacidade deve ser entendida como a retirada voluntária e temporária do indivíduo do convívio social, que se recolhe em sua solitude ou se resguarda ao convívio com pequenos grupos. Alerta ainda Westin sobre os perigos das tecnologias de vigilância e possíveis interferências, sendo uma das grandes preocupações da sociedade americana do final da década de sessenta (ZANINI, 2015, p. 07).

Entretanto, o conceito de privacidade não é um conceito fechado, pelo contrário, pode variar, por exemplo, com o tempo, com a cultura. Nesse sentido, com a chegada da *internet* e a convergência tecnológica, a privacidade se distancia da ideia inicial, ligada ao direito de ser deixado só, para se aproximar do pensamento acerca da necessidade de proteção do indivíduo contra interferências alheias e, revelando ao mundo somente

[21] Podendo-se também usar a expressão “o direito de ser deixado em paz”. No original: “the right to be let alone”.
[22] WARREN, Samuel Dennis; BRANDEIS, Louis Demitz. The right to privacy. Disponível em < http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html >

aquilo que deseja, de modo a controlar e dispor de suas informações pessoais (MOLINARO; SARLET, 2019, p. 202).

Assim, o discurso sobre privacidade acaba, cada vez mais, girando em torno de questões relacionadas a informações e dados pessoais que passam a ser violados com acessos indevidos. Nessa perspectiva, o direito fundamental à privacidade já não é suficiente para garantir a integral proteção aos dados pessoais, de modo que, a proteção de dados emerge como direito autônomo, podendo, contudo, ser complementar à privacidade (DONEDA, 2011). Como sintetiza Doneda "A proteção de dados é uma espécie de herdeira, atualizando-a e impondo características próprias" (2011, p.95).

A era digital inaugura uma série de novos questionamentos relacionadas ao direito fundamental à proteção de dados e sua violação. Atualmente, o tema da proteção de dados necessariamente traz desdobramentos relacionados a todas as possibilidades que a tecnologia proporciona para o tratamento e processamento de dados. Assim, ao se falar em 5G, inteligência artificial, computação em nuvem, *Big Data*, tais elementos integram o contexto no qual se insere a sociedade hiperconectada, com um governo movido a dados. Acrescenta-se ainda que as tecnologias digitais cada vez mais inseridas no cotidiano que refletem estruturas de poder com todos os seus desequilíbrios, discriminações e seus vieses implícitos e explícitos.

O entendimento da proteção de dados como direito fundamental e autônomo ganha relevância a partir do julgamento conjunto pelo Supremo Tribunal Federal (STF) das ADIN's nº 6.387, 6.388, 6.389, 6.390 e 6.393 referentes à inconstitucionalidade da Medida Provisória nº 954/2020[23] que versava sobre o compartilhamento de dados por empresas de telecomunicações com a Administração Pública, revela o amadurecimento do ordenamento jurídico e da Corte Constitucional brasileira quanto à essa questão.

Verificou o STF, na referida decisão considerada histórica, a necessidade de se reconhecer, de forma inédita, o direito à proteção de dados como um corolário da

[23] Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm

Constituição e independente em relação à privacidade e ao sigilo dos dados, com fulcro nos artigos 1º, inciso III e 5º, *caput*, e incisos X, XII e LXXII, da Constituição Federal:

> Nesta histórica decisão do STF, foi superado antigo paradigma da própria Corte, com o reconhecimento do direito à proteção de dados pessoais e à autodeterminação informacional como um novo direito fundamental, destacado e independente do direito à privacidade, com a identificação de uma série de liberdades individuais, atreladas ao direito à proteção de dados pessoais, que não são abraçadas pelo direito à privacidade - na concepção da privacidade como uma garantia de abstenção do Estado na esfera privada individual (BRASIL, 2020).

A partir dessa decisão, é possível vislumbrar a superação de um paradigma pela Corte Constitucional de que apenas as informações privadas eram protegidas, bem como, somente aquilo que é comunicado. Logo, o dado por si só torna-se digno da tutela constitucional.

Cumpre destacar, que o referido direito fundamental comporta duas dimensões: a dimensão subjetiva, relacionada a um direito subjetivo do cidadão, como forma de expressão de sua liberdade individual, e uma dimensão objetiva, na medida em que o Estado tem o dever de garantir o direito à proteção de dados nas relações privadas (SCHERTEL, 2019, p. 205).

Ao se admitir o direito fundamental à proteção de dados pessoais deve-se compreender não apenas a dimensão negativa de proteção, isto é, de não intervenção indevida pelo Estado, mas, de igual forma, o aspecto positivo de tal direito, que acarreta no dever de proteção por parte do próprio Estado face aos setores público e privado, estabelecendo medidas de segurança necessárias para a manipulação e o tratamento de dados por intermédio de órgãos de supervisão (SCHERTEL, 2019, p. 206-207).

Nesse sentido, a proteção de dados pessoais sugere não apenas uma dimensão individual, mas, também o reconhecimento de uma dimensão social e coletiva desse direito, posto que a proteção de dados pessoais se revela como instrumental e essencial para a concepção de muitos outros direitos fundamentais, como a liberdade de expressão, de associação e até mesmo a liberdade de locomoção.

Já no âmbito legislativo, há discussão da Proposta de Emenda Constitucional (PEC) nº 17/2019[24], que embora ainda sujeita à apreciação do Plenário, visa assegurar o direito fundamental à proteção de dados pessoais de forma expressa na Constituição Federal com a inclusão do inciso XII-A, no art. 5º, que passaria a ter a seguinte redação:

> Art. 5º […]
> XII – 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, bem como é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais; […] (NR).

A ideia de um direito fundamental de proteção a dados pessoais vem como uma chave interpretativa alicerçada na autodeterminação informativa que busca reconhecer o pensamento de que o indivíduo deve ser protagonista sobre seus dados pessoais, na medida em que mantem o domínio sobre suas informações e sob a forma como sua personalidade se projeta no mundo (EHRHARDT JÚNIOR; CATALAN; MALHEIROS, 2020, p. 580).

3.3 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – LGPD: *OVERVIEW*

Cumpre analisar, neste momento, a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais.

Cumpre ressaltar que até a promulgação da Lei Geral de Proteção de Dados Pessoais, não havia no ordenamento jurídico pátrio uma legislação que disciplinasse de forma direta e pormenorizada a proteção de dados pessoais (DONEDA, 2011, p. 103). Havendo apenas uma legislação esparsa em que tal proteção era direta ou indiretamente associada às garantias constitucionais da liberdade, vida privada e intimidade, estipuladas no artigo 5º, inciso X, do texto constitucional:

---

[24] Proposta de Emenda à Constituição nº 17, de 2019. Disponível em: < https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node013z74yoyqfhribjhxy5ac27ic29697723.node0?codteor=1773684&filename=PEC+17/2019 >. Acesso em: 03 jul. 2020.

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> [...]
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação. (BRASIL, 1988)

De igual forma, o inciso XII do mesmo artigo 5º da CF, veda a interceptação de comunicações telefônicas, telegráfica ou de dados, já o inciso XXXIII assegura o direito fundamental de acesso às informações que estejam sob o domínio do poder público. Logo, esse direito fundamental de acesso gera um dever essencial de transparência.

Assim, a LGPD chega para integralizar o microssistema de normas que regem a proteção de dados pessoais, como, por exemplo, o Código de Defesa do Consumidor (Lei nº 8.078/1990), a Lei do Cadastro Positivo (Lei nº 12.414/2011) e o Marco Civil da Internet (Lei nº 12.965/2014), tendo relevância não apenas local, como também reforça a tutela à nível global dos dados pessoais.

Com relação ao novo arcabouço regulatório de proteção de dados no Brasil concretizado pela Lei nº 13.709/2018, Laura Schertel Mendes e Danilo Doneda (p. 557, 2018) comentam

> A grande inovação que a LGPD operou no ordenamento jurídico brasileiro pode ser compreendida na instituição de um modelo *ex ante* de proteção de dados, baseado no conceito de que não existem mais dados irrelevantes diante do processamento eletrônico e ubíquo de dados na sociedade da informação. Os dados pessoais são projeções diretas da personalidade e como tais devem ser considerados. Assim, qualquer tratamento de dados, por influenciar na representação da pessoa na sociedade, pode afetar a sua personalidade e, portanto, tem o potencial de violar os seus direitos fundamentais.

Insta salientar que a LGPD brasileira foi inspirada na *General Data Protection Regulation* (GDPR) europeia cuja finalidade era impulsionar o desenvolvimento econômico e tecnólogo, por meio da flexibilização de regras pertinentes ao uso de dados pessoais em modelos de negócios inovadores, ao mesmo tempo que, proporciona um maior controle e proteção desses dados pelos usuários (MONTEIRO, 2018).

Apesar de uma legislação tímida e tangencial, quando o acesso e o compartilhamento de informações se tornam algo fundamental para a vida em sociedade, é inevitável que a proteção aos dados receba maior atenção.

Por esse motivo “[...] a ideia de tratamento é relevante, porque é justamente essa possibilidade de trabalhar os dados e informações, por meio da tecnologia da informática e das telecomunicações que lhes agrega elevado valor político e econômico” (GEDIEL; CORRÊA, 2008, p. 144), de modo que, surge a necessidade de oferecer um tratamento adequado de manipulação de dados pessoais.

Nessa perspectiva, a Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei nº 13.709/2018, foi promulgada em 14 de agosto de 2018, entrando em vigor quase dois anos depois, no dia 18 de setembro de 2020 e, pretende “proporcionar segurança para que informações pessoais circulem adequadamente, ao buscar estabelecer várias instâncias de controle de forma responsável e tutelada, proporcionando meios claros e seguros para a sua proteção” (SOUSA; BARRANCOS; MAIA, 2019, p. 243).

Nesse contexto, a proteção de dados compreende não só a normatização quanto ao processamento desses dados, mas, principalmente, regulamentar a geração de informações e conhecimentos obtidos por meio daqueles, vez que podem influenciar na tomada de decisões e gerar consequências adversas para os indivíduos afetados (ALBERS, p. 43, 2016).

Assim, ao longo dos seus 65 artigos, 10 capítulos e diversos parágrafos e incisos estão disciplinadas as regras atinentes à operação de tratamento de dados pessoais, físicos ou digitais, “por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (art. 1º, da LGPD)”.

Portanto, “independentemente do meio, do país de sede ou do país onde estejam localizados os dados” (art. 3º, *caput*, LGPD), a Lei Geral de Proteção de Dados Pessoais será aplicável, conforme o art. 3º, sempre que: a) a operação de tratamento

for realizada em território brasileiro; b) o tratamento de dados tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou c) os dados pessoais tratados tenham sido coletados no Brasil.

De todo modo, importante destacar que a Lei não é aplicável a todo e qualquer tratamento de dados pessoais, pois conforme disposição do art. 4º, da Lei, não é necessária a observância de seus ditames, quando o tratamento for:

> 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.

Quando se observa os fundamentos da proteção de dados assinalados pela Lei (artigo 2º) que guardam maior relevância com o objeto deste estudo, cumpre destacar principalmente o respeito à privacidade e à inviolabilidade da intimidade, da honra e da imagem, tendo em vista que, como se verá adiante, a Medida Provisória nº 954, tratava exatamente sobre o compartilhamento de dados pessoais por empresas de telecomunicações com o Instituto Brasileiro de Geografia e Estatística (IBGE).

Outrossim, em seu artigo 2º, a Lei ainda enumera dentre seus fundamentos basilares, a “autodeterminação informativa”, expressão inaugurada na LGPD e que garante um maior controle por parte dos titulares, não apenas sobre o conteúdo dos dados pessoais, mas, principalmente, o que deles pode ser feito “ao participar do tratamento de dados, desde o consentimento para o início do tratamento até o compartilhamento com terceiros” (LUGATI; ALMEIDA, 2020, p. 23).

Além disso, importa destacar que a Lei adotou um conceito bastante amplo para caracterizar o que é tratamento de dados, de modo que toda operação realizada com

dados pessoais é assim considerada. Neste sentido, aponta a Lei, em seu art. 5º, inciso X, que tratamento de dados 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.

O que se observa da leitura do inciso é que o tratamento envolve todo e qualquer tipo de contato e processo do dado, desde as atividades mais simples até as mais complexas. Outrossim, cumpre esclarecer que "as hipóteses não são cumulativas, ou seja, uma única atividade da lista já se inclui no conceito de tratamento, por mais simples que ela seja" (COTS; OLIVEIRA: 2019, p. 72).

Nessa perspectiva, a relevância jurídica da proteção de dados vai além dos dados considerados em si, devendo abranger todo e qualquer processo que vise a coleta, armazenamento, utilização ou transferência de informações pessoais extraídas para serem utilizadas em um determinado contexto e para determinados fins (SCHERTEL, 2019, p. 204).

Dito isso, é importante destacar que o tratamento de dados pessoais precisa observar os princípios da boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas (art. 6º, LGPD).

A observância de tais princípios tem o "[...] objetivo de restringir a atividade de tratamento de dados pessoais, exigindo-se que haja o seu cumprimento para que seja reconhecida a licitude da atividade legitimada" (MULHOLLAND, 2018, p.163).

Assim, no que tange à finalidade e à adequação, o tratamento de dados pessoais somente poderá ocorrer para "propósitos legítimos, específicos, explícitos e informados ao titular dos dados" (art. 6º, inciso I da LGPD) de modo que qualquer tratamento incompatível com a finalidade informada ao titular viola os ditames legais, sujeitando os infratores às sanções previstas em lei.

Outrossim, pelo princípio da segurança, as pessoas jurídicas públicas ou privadas, ou as pessoas físicas que utilizam dados para fins econômicos, deverão demonstrar 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” (art. 6º, VII da LGPD) e a adoção de medidas capazes de prevenir incidentes de segurança em decorrência do tratamento de dados pessoais.

Já no que concerne ao princípio da boa-fé, verifica-se que este consiste na adoção de padrões de conduta éticos, honestos, leais, transparentes, probos e adequados entre os agentes de tratamento e os titulares dos dados.

Além disso, a boa-fé deve pautar todas as fases do tratamento de dados, obrigando não apenas os agentes de tratamento, mas, também, toda e qualquer pessoa que venha a intervir em uma das fases, a garantir a segurança dos dados pessoais, mesmo após o término do tratamento.

Nessa perspectiva, “O titular dos dados pessoais tem, portanto, a confiança de que as suas informações serão eventualmente utilizadas ou, até mesmo, tratadas em conformidade com as suas legítimas expectativas, em razão da esfera social de seu relacionamento pregresso” (LISBOA, p. 10, 2019).

Quanto aos agentes de tratamento, ainda prevê a lei que estes adotem “medidas de segurança 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” (art. 46, *caput* da LGPD).

Ainda no que tange aos princípios da Lei Geral de Proteção de Dados, vale ressaltar que o princípio da necessidade, impõe “limitação ao tratamento dos dados para que este ocorra ao mínimo necessário para a realização de suas finalidades, de modo que somente sejam tratados dados pertinentes, proporcionais e não excessivos no que toca às finalidades de tratamento de dados” (art. 6º, inciso III da LGPD).

Um outro ponto importante, refere-se aos requisitos autorizadores do tratamento de dados pessoais. Isto porque, a Lei Geral de Proteção de Dados somente permite o tratamento de dados pessoais “comuns” (leia-se, não sensíveis) nas seguintes situações:

> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

No que tange ao consentimento, tido por muitos como o principal requisito autorizativo do tratamento de dados, cumpre destacar algumas particularidades.

Inicialmente, insta salientar que este não é obrigatório para os dados tornados públicos pelo titular, resguardados, entretanto os seus direitos e os princípios previstos na Lei Geral de Proteção de Dados (art. 7º, §4º da LGPD). Além disso, o consentimento “deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular” (art. 8º, *caput* da LGPD) e, quando fornecido por escrito, precisará constar de forma destacada das demais cláusulas do contrato, sendo expressamente vedado o tratamento de dados pessoais mediante vício de consentimento (art. 8º, §1º da LGPD).

Assim, cumpre destacar que, embora a comunidade jurídica, em linhas gerais, tenha enaltecido a ideia de necessidade de consentimento prévio e expresso dos usuários

para utilização dos dados, esta é apenas uma das 10 (dez) hipóteses que autorizam o tratamento dos dados pessoais.

Ademais, o consentimento deverá concernir às finalidades determinadas e poderá ser revogado a qualquer tempo mediante manifestação expressa do titular dos dados pessoais (art. 8, §§4º e 5º da LGPD). Autorizações genéricas serão nulas, tendo o titular direito ao acesso facilitado às informações sobre o tratamento de seus dados (art. 8, §§4º e 5º da LGPD).

Já em relação aos agentes de tratamento (controlador e operador de dados), a Lei Geral de Proteção de Dados, estabelece que ambos "devem manter o registro das operações de tratamento de dados que realizem, especialmente quando baseado no legítimo interesse" (art. 37, *caput* da LGPD). Além disso, conforme aponta o art. 39, da Lei nº 13.709/2018 – LGPD, o operador de dados "deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria".

Outro ponto que merece destaque refere-se ao encarregado, que vem a ser a pessoa escolhida "pelo controlador e operador para funcionar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)", conforme prescreve o artigo 5º, inciso VIII da LGPD.

Neste aspecto, importante ressaltar que tanto controlador quanto operador que violarem os ditames da lei brasileira de proteção de dados pessoais são solidariamente responsáveis pelos danos causados em decorrência das atividades de tratamento de dados pessoais que realizam, sendo obrigados a repará-los (art. 42, incisos I e II da LGPD)[25].

[25]Art. 42, § 1º § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
II - 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.

É oportuno mencionar ainda as sanções administrativas tratadas na Lei Geral de Proteção de Dados brasileira. Neste aspecto, insta salientar que apesar da Lei já estar em vigor desde setembro de 2020, o capítulo que trata sobre as sanções administrativas (artigos 52, 53 e 54) somente passou a vigorar em 1º de agosto de 2021, conforme art. 20, da Lei nº 14.010/2020, que dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET)[26] no período da pandemia do coronavírus (Covid-19).

De todo modo, conforme art. 52, da Lei Geral de Proteção de Dados, os agentes de tratamento de dados que violarem os preceitos da norma, estarão sujeitos a diversas sanções administrativas a serem aplicadas pela Autoridade Nacional de Proteção de Dados, como:

> 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.

Além disso, verifica-se que as sanções serão aplicadas após processo administrativo respeitada a ampla defesa e as peculiaridades do caso concreto, de acordo com a gravidade e natureza das infrações, a boa-fé do infrator, o grau do dano, a adoção de política de boas práticas e governança e demais parâmetros e critérios estabelecidos nos incisos do § 1º, do art. 52, da Lei Geral de Proteção de Dados.

3.4 DADOS: DELIMITAÇÃO DO CONCEITO JURÍDICO

[26] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14010.htm

Para que se avance nos estudos acerca da problemática que envolve o empoderamento tecnológico em um estado de vigilância frente aos direitos fundamentais, notadamente a privacidade e a proteção de dados pessoais, há de se resgatar conceitos elementares que fundamentam a questão.

Comumente quando se iniciam os estudos sobre a proteção de dados, surge expressão "Dados são o novo petróleo"[27] em alusão ao papel semelhante desempenhado por esse recurso natural no último século. Assim, atualmente os dados tem um valor econômico extremamente relevante, fazendo com que haja um interesse cada vez maior de acesso e manipulação destes.

Conceitualmente falando, dados "são fatos ou observações brutas, em geral sobre fenômenos físicos ou transações de negócios" (O'BRIEN; MARAKAS, 2013, p. 32), representando, portando, objetos reais. Deste modo, embora possam ser apresentados de forma estruturada - textual, visual ou numérica, o dado por si só não possui valor agregado significativo e útil, sendo a matéria-prima bruta da informação, que após um processo de tratamento extrai esse valor (BOTELHO, 2020, p. 198).

Assim, ao analisar os dados e seu conteúdo, importante trazer à baila a distinção entre dado e informação estabelecida por Danilo Doneda (2001, p. 94)

> Em relação à utilização dos termos "dado" e "informação", vale uma especificação. [...] Assim, o "dado" apresenta conotação um pouco mais primitiva e fragmentada, como observamos em um autor que o entende como uma informação em estado potencial, antes de ser transmitida, o dado estaria associado a uma espécie de "pré-informação", anterior à interpretação e ao processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição. Sem aludir ao seu significado ou conteúdo em si, na informação já se pressupõe uma fase inicial de depuração de seu conteúdo – daí que a informação carrega também um sentido instrumental, no sentido da redução de um estado de incerteza.

Logo, "a informação é o resultado do tratamento dos dados, a transformação do fato bruto, da representação de um fato da realidade, em valor para a organização"

[27] Creditada pioneiramente ao matemático britânico Clive Humby, popularizou-se a máxima de que "informação é o novo petróleo" (HUMBY, Clive. Data is the new oil. Proc. ANA Sr. Marketer's Summit, Evanston, 2006).

(BOTELHO, 2020, p. 198), em outras palavras, a informação é composta por dado e contexto, isto é, um dado contextualizado.

Conquanto "no campo da tecnologia e segurança da informação dado e informação sejam conceitos distintos, a LGPD não teve essa preocupação" (BOTELHO, 2020, p. 201), isto é, os "dados pessoais" dispostos no art. 5º, inciso I, da Lei nº 13.709/2018 - LGPD se referem tanto aos dados em si como às informações resultantes do tratamento daqueles.

Sob essa perspectiva, o mencionado texto legal conceitua os dados pessoais como todo e qualquer tipo de informação relacionada a uma pessoa natural identificada ou identificável, como o nome e endereço residencial, número do Registro Geral de Identificação (RG) e do Cadastro de Pessoas Físicas (CPF), contudo, a lei não se restringe apenas a esses dados, pois inclui também, por exemplo, o *Internet Protocol* (IP) e os dados de geolocalização do indivíduo, logo, a Lei Geral de Proteção de Dados Pessoais adota o critério expansionista para definição de dados pessoais (COTS; OLIVEIRA, 2019, p. 71).

Neste sentido, não há um rol taxativo do que ou quais seriam considerados dados pessoais, qualquer dado que esteja vinculado, de forma direta ou indireta, a determinada pessoa e, no contexto inserido, revelam algo sobre ela deve ser entendido como dado pessoal.

> [...] observa-se que nem a LGPD nem o GDPR trazem uma listagem do que poderia constituir um dado pessoal, na medida em que a avaliação deve sempre ser levada a efeito de maneira contextual. Se uma determinada informação potencialmente é capaz de tornar uma pessoa identificável, então ela pode vir a caracterizar-se como dado pessoal naquele específico contexto (MALDONADO, 2019, p. 15).

Assim, ao se falar sobre dados pessoais deve-se pensar em um quebra-cabeça em que há várias peças soltas e dispostas de forma aleatória, que sozinhas não são capazes de mostrar a imagem a ser montada, contudo, ao se encaixar as peças, é possível identificar uma figura. De igual forma acontece com os dados pessoais, um dado sozinho talvez não seja capaz de identificar uma pessoa, mas ao juntá-las um

dado no outro é possível identificar determinada pessoa, é o que chamamos de efeito mosaico (BIONI, 2020, p. 191).

A LGPD menciona também os dados ditos anonimizados, isto é, dados que se tornaram anônimos e cujo titular não é possível identificar, "considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento", conforme dispõe o artigo 5º, inciso III, da LGPD, não sendo aqueles abarcados pela proteção preconizada pela lei em comento. Contudo, cumpre ressaltar que a própria Lei Geral de Proteção de Dados, traz uma distinção entre dados anonimizados e pseudoanonimizados, estes, por sua vez, se referem à dados aos quais o processo de anonimização permite a reversão (art. 12, LGPD), de modo que, a estes é garantida a proteção.

Ademais, a Lei Geral de Proteção de Dados Pessoais ainda classifica no mesmo artigo 5º, citado anteriormente, agora no inciso II[28], os dados pessoais considerados sensíveis, relacionados às opções e características basilares do indivíduo e que podem levar a uma situação de discriminação contra o titular dos dados, como dados relacionados à orientação sexual, religiosa e política, etnia, ou seja, dados que necessitam de tratamento diferenciado, pois poderão acarretar na discriminação dos seus titulares e, por isso, merecem atenção especial.

Os dados de saúde, como tipo sanguíneo, existência de doença hereditária ou informações relacionadas à vacinação de determinada pessoa, também são classificados como sensíveis. Já os dados genéticos e biométricos são considerados sensíveis em razão da sua imutabilidade, haja vista não ser possível alterar a impressão digital ou a íris dos olhos, por exemplo. Uma vez coletado esse dado é possível identificar seu titular para o resto da vida, por isso a necessidade de um tratamento diferenciado/especial.

[28] Artigo 5º, inciso II, Lei nº 13.709/2018: "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".

Cumpre ressaltar ainda a possibilidade de um dado pessoal originalmente não sensível, que a depender do contexto em que está inserido, passe a ser assim considerado. É o caso, por exemplo, de um dado de geolocalização, que por si só é um dado pessoal, e que na sua origem não é um dado sensível, contudo, se a geolocalização indicar alguma questão discriminatória – como a sede de um partido político ou determinada igreja ou templo, ele poderá passar a ser assim considerado.

Sob outro prisma, os dados ainda podem ser divididos em dois grupos: dados públicos e privados. Dados públicos compreendem aqueles de conhecimento geral, incluídos os cadastros de dados registrais não sigilosos em cartórios e repartições públicas e que estão à disposição do público. Já os dados privados são dados relativos tanto à pessoa física como jurídica restritos à esfera privada, como informações confidenciais e sigilosas (VEIGA; ROVER, 2004).

Por outro lado, existem dados privados cujos titulares liberam para cadastramento e disponibilização. Esses dados podem ser chamados de dados privados autorizados, considerada aqui a autorização como permissão à inclusão em bancos de dados.

Ademais, considerando-se o contexto tecnológico em que os dados estão inseridos, é imperioso reconhecer que os dados pessoais servem de insumos para as mais variadas atividades econômicas e governamentais. Nessa perspectiva, aquele que tem acesso e controle sobre dados tem condições de exercer poder, político, econômico e intelectual sobre os indivíduos com grande eficácia.

À vista disso, é possível vislumbrar que o acesso a dados pessoais se torna um fator produtivo econômico importante ao permitir o controle sobre as pessoas.

4 O DEBATE EM TORNO DA MEDIDA PROVISÓRIA Nº 954/2020 E A PROBLEMÁTICA QUANTO AO COMPARTILHAMENTO DE DADOS COM A ADMINISTRAÇÃO PÚBLICA

O contexto pandêmico acelerou a prática de coleta de dados pessoais e seu uso para a elaboração de políticas públicas, notadamente aquelas referentes à saúde e à pesquisas científicas de combate à Covid-19, o que acaba por evidenciar a fragilidade da proteção de dados.

Dentro dessa estratégia de isolamento social forçada, entre outras medidas, de igual forma necessárias, é possível vislumbrar uma série de desdobramentos e, como se verá adiante, o compartilhamento de dados pessoais é uma das medidas recorrentes aplicadas no momento atual e, ao mesmo tempo que pode contribuir para uma atuação mais efetiva (e rápida) do Estado, não poderá ocorrer a qualquer custo, devendo ser respeitados não apenas os princípios previstos na Lei Geral de Proteção de Dados, mas, também, os direitos garantidos aos titulares, evitando-se, assim, abusos advindos de utilização e compartilhamento indevidos de dados e ameaças aos direitos e garantias fundamentais.

Em outras palavras

> A questão da "proteção da vida" como justificativa para a constituição de um regime de Estado de exceção, ainda que provisório, ganha mais complexidade, já que a instauração de tal Estado se deve a uma reação de urgência diante das consequências do conjunto de políticas francamente contrárias à proteção da vida, em todas as suas dimensões, políticas que intencionalmente destruíram sistemas de proteção social, entre eles os sistemas de saúde, tudo com o argumento da necessidade de fazer a economia funcionar, nas décadas de hegemonia neoliberal (LACERDA, 2020, 78).

Sob esta ótica, a Lei nº 13.979[29], apelidada de Lei da Pandemia, foi promulgada em 6 de fevereiro de 2020 e, "dispõe sobre as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019" (BRASIL, 2019).

[29] Disponível em http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l13979.htm

Dentre os 9 artigos previstos na lei, chama a atenção o artigo 6º[30] que torna obrigatório o compartilhamento de dados pessoais entre órgãos e entidades da administração pública federal, estadual, distrital e municipal na tentativa de identificar pessoas infectadas ou com suspeita de infecção pelo coronavírus, cuja finalidade exclusiva é evitar a propagação da doença. Tal obrigação ainda é estendida às pessoas jurídicas de direito privado quando os dados forem solicitados por autoridade sanitária (art. 6º, §1º, Lei 13.979).

Nesse contexto, quais os desdobramentos dessa lei? É possível vislumbrar o risco à privacidade e à proteção de dados pessoais que, se impõe como princípios relacionais, porém distintos e, igualmente, pode apresentar um risco à segurança, uma vez que o Estado passa a monitorar seus cidadãos.

4.1 A INCONSTITUCIONALIDADE DA MEDIDA PROVISÓRIA Nº 954/2020

Medidas provisórias são espécies normativas infraconstitucionais de caráter excepcional, cuja previsão encontra-se no artigo 62 da Constituição Federal[31]. Tem como principal característica a ausência de um processo legislativo para sua elaboração, visto que é editada por um ato monocrático de vontade do representante do Poder Executivo, que no exercício de sua função atípica, se apodera da atividade legislativa para regular situações em casos de relevância e urgência.

> A justificativa para o Presidente da República editar medidas provisórias, com força de lei, é a existência de um *estado de necessidade*, que impõe ao Poder Público a adoção imediata de providências, de caráter legislativo, inalcançáveis segundo as regras ordinárias de legiferação, em face do próprio *periculum in mora* que fatalmente decorreria do atraso na concretização da prestação legislativa – grifos no original (BULOS, 2018, p. 1182).

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

[31] Art. 62. Em caso de relevância e urgência, o Presidente da República poderá adotar medidas provisórias, com força de lei, devendo submetê-las de imediato ao Congresso Nacional.

Ponto importante e sempre destacado pela doutrina se refere aos requisitos fundamentais da MP, como dito - relevância e urgência -, visto que constituem conceitos jurídicos indeterminados, dotados de imprecisão e vagueza. Logo, a análise desses requisitos envolve juízos de valor atinentes ao caso concreto (BULOS, 2018, p.1187).

Sob esta ótica, vislumbra-se na atual conjuntura brasileira de um cenário pandêmico, uma inflação legislativa com uma proliferação de MP's[32]. A que recebe destaque nesse estudo é a Medida Provisória nº 954, sancionada no dia 17 de abril de 2020 pelo Presidente da República, e tratava sobre o compartilhamento de dados pessoais (nome, número telefônico e endereço) dos consumidores pelas empresas de telecomunicações com o Instituto Brasileiro de Geografia e Estatística (IBGE), para o desenvolvimento de estatística oficial, de modo não presencial, durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (Covid-19) (artigo 2º, da MP 954).

Desse modo, os dados deveriam ser transmitidos ao IBGE em até 07 (sete) dias contados da publicação da MP e, sua vigência duraria até o final da situação de emergência de saúde pública (art. 2, §3º, inciso I, MP 954). Superada a situação de emergência, as informações compartilhadas pelas empresas de telecomunicações ao IBGE seriam excluídas automaticamente. Caso houvesse necessidade de conclusão de produção de estatística oficial, o Instituto poderia utilizar os dados por mais 30 (trinta) dias contados a partir do fim da situação de emergência (artigo 4º, p. único, MP 954).

A medida ainda previa que os dados repassados teriam caráter sigiloso, ou seja, seriam de uso exclusivo do IBGE para a produção de estatística, ficando proibido o repasse dos dados para empresas públicas e privadas ou com órgãos ou entidades da administração pública direta ou indireta de quaisquer dos entes federativos (artigo 3º, da MP 954).

[32] Nos quatro primeiros meses de 2020 já se somavam 42 medidas provisórias; a média registrada desde 2001 era de 50 para o ano todo. Desde março de 2020 já foram 35 medidas provisórias ligadas à pandemia, número correspondente a 75% de todo o volume de 2019 e que se iguala ou supera a quantidade em três dos últimos 11 anos (AGÊNCIA SENADO, 2020).

Ademais, o § 2º do referido artigo, estabeleceu, ainda, a obrigação do Instituto em informar em quais situações os dados fornecidos seriam utilizados e divulgar relatório de impacto à proteção de dados pessoais, em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), que por sua vez, indica no art. 23 que o tratamento de dados pessoais realizado pelas pessoas jurídicas de direito público deverá atender a finalidade pública.

Nessa toada, a referida MP, de forma genérica e sem nenhuma medida de segurança, controle e gerenciamento de acesso, permitia o compartilhamento de dados pessoais, sem, contudo, especificar o escopo e o contexto da produção dessas estatísticas a partir do acesso total a base de dados das empresas de telecomunicações.

Logo, passou-se a questionar qual a real finalidade da transmissão dessas informações, uma vez que, como esclareceu o próprio IBGE, a coleta de dados da Pesquisa Nacional por Amostra de Domicílios (PNAD) Contínua é realizada exclusivamente de forma presencial nos domicílios selecionados; contudo, devido à situação de excepcionalidade enfrentada, a coleta de informações segue sendo realizada por meio de contato telefônico (IBGE, 2020), logo as estatísticas realizadas pelo IBGE são amostrais.

Em contrapartida, se considerarmos os dados abrangidos pelas empresas de telecomunicações temos que, segundo a Agência Nacional de Telecomunicações (ANATEL), que publica mensalmente a quantidade de acessos relativos aos principais serviços de telecomunicação, cerca de 234,1 milhões de brasileiros utilizam a telefonia móvel, e 30,2 milhões a telefonia fixa (ANATEL, 2020), isto é, dados que seriam alcançados pela referida MP e que divergem com a quantidade divulgada pelo IBGE.

Assim, ao nos atentarmos para o princípio da necessidade destacado na LGPD é preciso questionar: é necessário e proporcional, para a finalidade de uma pesquisa amostral, ter acesso a base de dados completa dos telefones dos brasileiros? Acrescente-se a isso, sob a ótica do princípio da adequação, como garantir que esses dados não seriam utilizados no futuro para outros fins não especificados?

Outra problemática que emerge a partir da publicação da MP nº 954 é a de que, como visto anteriormente, dados de saúde são considerados dados sensíveis. Assim, uma vez que o IBGE se utiliza de uma base de dados genérica e esses dados forem utilizados para o desenvolvimento de pesquisas em torno da Covid-19, estes passam a ser considerados dados sensíveis e a medida não aborda acerca dos cuidados para o tratamento desses dados em específico, tornando os usuários totalmente vulneráveis.

Não há também especificado na MP a indicação do encarregado pelo tratamento dos dados pessoais compartilhados e nem quem elaborará, por exemplo, o relatório de impacto à proteção de dados pessoais, igualmente mencionado na Medida.

De igual modo, outra questão que pode surgir a partir da edição de medidas provisórias como essa seria em relação ao armazenamento dos dados, se ocorreria de forma centralizada ou descentralizada.

Nesse contexto, após a publicação da MP, entendendo existir um vício de inconstitucionalidade formal e material do texto normativo, partidos políticos - Partido da Social Democracia Brasileira – PSDB; Partido Socialista Brasileiro – PSB; Partido Socialismo e Liberdade – PSOL; e Partido Comunista do Brasil - PCdoB, bem como o Conselho Federal da Ordem dos Advogados do Brasil – OAB, propuseram 05 Ações Diretas de Inconstitucionalidade perante o Supremo Tribunal Federal a fim de suspender a eficácia da MP[33].

A ADI ajuizada pela Ordem dos Advogados justifica o seu ajuizamento, haja vista que:

> A Medida Provisória padece, nesse sentido, de a) inconstitucionalidade formal, no tocante à ausência de preenchimento dos pressupostos constitucionais de urgência e relevância, nos termos do art. 62, caput, da CF; e b) inconstitucionalidade material, por violação direta aos artigos 1º, inciso III e 5º, incisos X e XII da Constituição Federal, os quais asseguram, respectivamente a dignidade da pessoa humana; a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas; o sigilo dos dados e o direito à autodeterminação informativa, bem como por violação ao princípio da proporcionalidade. A violação constitucional ao artigo 5º, incisos X e XII da Constituição Federal que cita a inviolabilidade do sigilo de correspondência e das comunicações telegráficas de dados e das

[33]ADI's nº 6.387; 6.388; 6.389; 6.390 e 6.393.

> comunicações telefônicas, salvo, em último caso, por decisão judicial. Além disso, ainda na esfera constitucional, a MP ao permitir o acesso aos dados pessoais dos usuários violaria também o direito à intimidade, à vida privada, à honra e à imagem e à autodeterminação informativa (BRASIL, 2020).

Em julgamento conjunto das ADI's nº 6.387; 6.388; 6.389; 6.390 e 6.393, o STF por meio do voto da relatora, ministra Rosa Weber, concedeu as medidas liminares para suspender a eficácia da Medida Provisória nº 954/2020 e determinar o impedimento do IBGE em solicitar dados pessoais dos consumidores abrangidos pela MP, sob o argumento de que a "crise sanitária emergencial não pode justificar a coleta desmedida de dados pelo Estado, sob risco de atropelo dos direitos fundamentais" (BRASIL, 2020).

A decisão foi submetida a referendo do Plenário, em sessão por videoconferência e, confirmada, por quase unanimidade dos ministros, com 10 (dez) votos favoráveis, sendo divergente apenas o voto do Ministro Marco Aurélio. Em seguida a ementa da decisão:

> MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA Nº 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. *FUMUS BONI JURIS. PERICULUM IN MORA*. DEFERIMENTO.
> 1. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais.
> 2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos**. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados**.
> 3. **O Regulamento Sanitário Internacional (RSI 2005) adotado no âmbito da Organização Mundial de Saúde exige, quando essencial o tratamento de dados pessoais para a avaliação e o manejo de um risco para a saúde pública, a garantia de que os dados pessoais manipulados sejam "adequados, relevantes e não excessivos em relação a esse propósito" e "conservados apenas pelo tempo necessário." (artigo 45, § 2º, alíneas "b" e "d"**).
> 4. Consideradas **a necessidade, a adequação e a proporcionalidade da medida, não emerge da Medida Provisória nº 954/2020**, nos moldes em que editada, **interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia**.

> 5. Ao **não definir apropriadamente como e para que serão utilizados os dados coletados, a MP nº 954/2020 desatende a garantia do devido processo legal (art. 5º, LIV, da CF)**, na dimensão substantiva, por não oferecer condições de avaliação quanto à sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades.
> 6. Ao não apresentar mecanismo técnico ou administrativo apto a proteger, de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados pessoais compartilhados, a MP nº 954/2020 descumpre as exigências que exsurgem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros.
> 7. Mostra-se **excessiva a conservação de dados pessoais coletados, pelo ente público, por trinta dias após a decretação do fim da situação de emergência de saúde pública, tempo manifestamente excedente ao estritamente necessário para o atendimento da sua finalidade declarada**.
> 8. Agrava a ausência de garantias de tratamento adequado e seguro dos dados compartilhados a circunstância de que, embora aprovada, ainda não vigora a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), definidora dos critérios para a responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais. O fragilizado ambiente protetivo impõe cuidadoso escrutínio sobre medidas como a implementada na MP nº 954/2020.
> 9. **O cenário de urgência decorrente da crise sanitária deflagrada pela pandemia global da COVID-19 e a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento não podem ser invocadas como pretextos para justificar investidas visando ao enfraquecimento de direitos e atropelo de garantias fundamentais consagradas na Constituição**.
> 10. Fumus boni juris e periculum in mora demonstrados. Deferimento da medida cautelar para suspender a eficácia da Medida Provisória nº 954/2020, a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel.
> 11. Medida cautelar referendada (grifou-se) (BRASIL, 2020).

Nessa perspectiva, a ministra Rosa Weber firmou o entendimento de que há limites para o acesso e tratamento de dados pelo Estado e que a MP deveria demonstrar "interesse público legítimo que justificasse o acesso dessas informações, devendo o Poder Executivo se atentar aos critérios de necessidade, adequação e proporcionalidade da medida" (BRASIL, 2020). Bem como, não se prestou a demonstrar a "forma como esta pesquisa contribuirá na formulação das políticas públicas de enfrentamento da crise sanitária" (BRASIL, 2020).

Assim como os demais princípios constitucionais, a proteção de dados não é absoluta como pontuou o voto do Ministro Alexandre de Moraes:

> Portanto, também nas hipóteses de proteção ao sigilo de dados com base na intimidade e na privacidade, previstas nos já referidos inc. X e XII do art. 5º,

> existe a possibilidade de relativização, inclusive em relação a possível compartilhamento com outros órgãos que manterão sigilo, lógico que dentro desse contexto e de toda interpretação dos direitos e garantias individuais.
> (...)
> Dessa maneira, desde que as hipóteses legais que relativizem o sigilo de dados sejam adequadas, razoáveis, proporcionais e específicas, somente nessas hipóteses, não haverá, a meu ver, inconstitucionalidade ou suspeita de inconstitucionalidade (BRASIL, 2020).

Apesar da possibilidade de relativização da proteção de dados, este não parece ser o caso a ser aplicado em relação à MP nº 954/2020, isto porque, como destacado pelo Ministro Alexandre de Moraes "não estão presentes, na disciplina dessas hipóteses, as necessárias adequação, razoabilidade e proporcionalidade para, excepcionalmente, relativizar-se a proteção constitucional ao sigilo de dados" (BRASIL, 2020).

Ao suspender a eficácia da Medida Provisória nº 954/2020, o STF dá indícios de como se dará a proteção de dados pessoais no Brasil. A proteção desse direito é procedimental, no sentido de que o uso de dados deve respeitar a transparência, ter uma finalidade específica explícita e que o processamento ocorrerá de forma adequada. Também demostra na perspectiva paradigmática que as informações íntimas da vida privada merecem proteção de não divulgação.

Cumpre destacar que, em 14 de agosto de 2020 por meio de Ato Declaratório nº 112 do Presidente da Mesa do Congresso Nacional, a Medida Provisória nº 954 teve seu prazo de vigência encerrado.

Contudo, a discussão iniciada pela promulgação da medida não se encerra após a suspensão dos seus efeitos e expirado seu prazo de vigência, para além do debate específico do abuso e da desproporcionalidade da MP que deixa vulnerável o cidadão e a privacidade dos seus dados, imprescindível o aprofundamento dos estudos quanto aos desdobramentos políticos que tal medida possa representar: um estado de vigilância.

4.2 OUTRAS ESPÉCIES NORMATIVAS QUE TRATAM SOBRE O COMPARTILHAMENTO DE DADOS NO ORDENAMENTO JURÍDICO BRASILEIRO

A discussão quanto ao perigo e à fragilidade de normas que dispõem sobre o compartilhamento de dados no Brasil é anterior à Medida Provisória nº 954/2020. Antes mesmo da entrada em vigor da LGPD, o ordenamento jurídico brasileiro já autorizava, o tratamento de dados em diversas leis e decretos[34]. Como exemplo: (i) Lei nº 9.507/1997, que regula o direito ao acesso à informação e disciplina o rito processual do *habeas data*; (ii) Lei nº 9.784/1999, que prescreve sobre o processo administrativo no âmbito da Administração Pública Federal; (iii) Lei nº 12.965/2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil; e (iv) Lei nº 13.460/2017, que dispõe sobre a participação, proteção e defesa dos direitos do usuário dos serviços públicos da Administração Pública.

A Lei nº 12.965/2014, popularmente conhecida como "Marco Civil da Internet", "estabelece os princípios, garantias, direitos e deveres para o uso da *internet* no Brasil e determinar as diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios" (art. 1º, Lei 12.965/2014) relacionadas ao tema[35].

O "Marco Civil" estabelece que o uso da internet do Brasil tem entre seus princípios a proteção da privacidade e a proteção dos dados pessoais, garantindo aos titulares de dados que sejam fornecidas informações claras e completas sobre a coleta, o uso, o armazenamento, o tratamento e a proteção de seus dados pessoais, os quais somente poderão ser utilizados para finalidades legítimas, específicas e justificadas (art. 7º, Lei 12.965/2014).

No que tange especificamente ao compartilhamento de dados, observa-se pela leitura da lei em questão, que o acesso à internet é essencial ao exercício da cidadania, sendo garantidos aos usuários o direito que seus dados pessoais não sejam fornecidos a terceiros, incluindo-se nessa regra, os registros de conexão e de acesso a aplicações de internet (art. 7º, Lei 12.965/2014).

De todo modo, a regra disposta acima poderá ser afastada, quando i) houver consentimento livre, expresso e informado do titular ou ii) em hipóteses previstas em lei, como nos casos de ordem judicial (art. 7º, inciso VII, Lei 12.965/2014).

---

[34] Disponível em*:* https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf
[35] Disponível em: L12965 (planalto.gov.br)

Além disso, aponta o “Marco Civil da Internet”, em seu art. 10, § 3º, que, excepcionalmente, poderão ser fornecidos acessos a dados pessoais cadastrais, como qualificação pessoal, filiação e endereço, por autoridades administrativas que detenham competência legal e necessitem do acesso para o desempenho de suas atribuições.

Em relação ao assunto em tela, observa-se a edição do Decreto nº 8.771/2016[36], que veio para regulamentar o “Marco Civil da Internet” e disciplinar, entre outros assuntos, sobre a proteção aos registros, aos dados pessoais e às comunicações privadas.

Neste sentido, verifica-se que são considerados dados cadastrais aqueles relativos a i) filiação; ii) endereço e iii) qualificação pessoal, compreendidos aqui o nome, o prenome, o estado civil e a profissão do titular.

No que tange às autoridades administrativas, aponta o decreto que que estas indicarão o fundamento legal para o acesso e a motivação do pedido de acesso aos dados cadastrais.

Ainda nesse aspecto, de acordo com o decreto, observa-se que a autoridade máxima de cada órgão da administração pública federal deverá publicar anualmente em seu sítio eletrônico, os relatórios estatísticos contendo dados relativos à requisição de dados cadastrais, contendo, entre outros, o número de pedidos realizados; o número de pedidos deferidos e indeferidos pelos provedores e o número de usuários afetados.

Por outro lado, o Decreto Presidencial nº 8.789/2016 assinado durante o governo de Michel Temer se apresentava como uma inovação da administração pública na promoção de eficiência na gestão de políticas públicas, isto porque o art. 6º dispensava expressamente a celebração de acordos e convênios entre órgãos e entidades para o compartilhamento de bases de dados.

Com a edição do Decreto, os mecanismos de compartilhamento e cruzamento de banco de dados foram simplificados e, assim, os dados cadastrais sob a gestão dos

[36] Disponível em: Decreto nº 8771 (planalto.gov.br)

órgãos e das entidades da administração pública federal direta ou indireta seriam compartilhados entre as bases de dados oficiais, preferencialmente de forma automática (art. 3º). Já o acesso aos dados individualizados não cadastrais dependeria da comprovação de necessidade dos órgãos interessados (art. 4º).

Cumpre ressaltar que o artigo 8º, § 2º do referido Decreto previa a possibilidade de retransmissão das informações compartilhadas, desde que houvesse expressa autorização do órgão responsável pela base de dados. Ademais, ao estabelecer as condições normativas para o compartilhamento e cruzamento de bancos de dados, o Decreto falhou ao não prever limitações a tais usos, bem como foi silente quanto aos riscos à segurança e à proteção de dados.

O Decreto nº 8.789/2016 foi revogado pelo Decreto nº 10.046, de 9 de outubro de 2019, que "dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados" (BRASIL, 2019).

O primeiro fato que chama a atenção no Decreto é a supressão do termo "dados pessoais", e a escolha pelos termos: atributos biográficos - "dados de pessoa natural relativos aos fatos da sua vida, tais como nome civil ou social, data de nascimento, filiação, naturalidade, nacionalidade, sexo, estado civil, grupo familiar, endereço e vínculos empregatícios" (art. 2º, inciso II, Decreto nº 10.046/2019); e atributos biométricos – "características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar;" (art. 2º, III, Decreto nº 10.046/2019).

Ademais, há uma abrangência da incidência da norma em relação ao Decreto de 2016 ao incluir os demais Poderes da União (Legislativo e Judiciário), visto que anteriormente, o compartilhamento de dados restringia-se aos órgãos e às entidades da administração pública federal direta, autárquica e fundacional.

> Art. 1º Este Decreto 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**, com a finalidade de:
> I - simplificar a oferta de serviços públicos;
> II - orientar e otimizar a formulação, a implementação, a avaliação e o monitoramento de políticas públicas;
> III - possibilitar a análise das condições de acesso e manutenção de benefícios sociais e fiscais;
> IV - promover a melhoria da qualidade e da fidedignidade dos dados custodiados pela administração pública federal; e
> V - aumentar a qualidade e a eficiência das operações internas da administração pública federal. (grifos nossos) (BRASIL, 2019)

Outrossim, ao adicionar uma quinta finalidade para o compartilhamento de dados (art. 1º, inciso V), o Decreto Presidencial esbarra na Lei Geral de Proteção de Dados Pessoais, que prevê em seu art. 7º, inciso III, o tratamento e compartilhamento de dados pela administração pública quando necessários à execução de políticas públicas.

Apenas por esses aspectos é possível concluir que as inovações trazidas pelo Decreto nº 10.046/2019 vão em sentido contrário às regras e garantias de proteção e à segurança dos dados dos cidadãos ao não incorporar princípios centrais e diretrizes consolidadas na LGPD, dando ensejo à propositura da Ação Direta de Inconstitucionalidade nº 6.649 pelo Conselho Federal da OAB, sob o argumento de que com o Decreto nº 10.046/2019:

> [...] está sendo erigida uma **ferramenta de vigilância estatal extremamente poderosa**, que inclui informações pessoais, familiares e laborais básicas de todos os brasileiros, mas também dados pessoais sensíveis, como dados biométricos, tanto quanto "características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar" (art. 2º, inciso II, do Decreto nº 10.046/2019). (grifos nossos) (BRASIL, 2020)

Precedente importante relacionado ao compartilhamento de dados na Administração Pública se refere ao episódio em que a Procuradoria Jurídica do Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep) se negou a compartilhar dados dos estudantes brasileiros coletados pelo Censo da Educação com o Ministério da Educação, que os requisitou sob a justificativa de que pretendia confeccionar as carteiras dos estudantes. Nesse sentido, a Procuradoria entendeu que se tratavam de dados sigilosos coletadas para uma finalidade específica diversas e que por isso não deveriam ser compartilhados.

Tal situação criou um impasse dentro do próprio instituto, entre o Presidente e o Procurador Federal que emitiu o parecer[37] e acabou por ser exonerado.

O imbróglio chegou ao Supremo Tribunal Federal por intermédio do Mandado de Segurança 36150 impetrado pelo Inep contra o acórdão do Tribunal de Contas da União que determinou a entrega de dados individualizados do Censo Escolar e do ENEM para auditoria do Programa Bolsa Família sob o argumento de que a "decisão da corte de contas "fere sensivelmente" o sigilo estatístico" e viola o art. 5º, incisos X, XIV e XXXIII da Constituição Federal; o art. 23 da Lei nº 12.527/2011 – Lei de Acesso à Informação; o art. 6º do Decreto nº 6.425/2008, que trata sobre o sigilo dos dados do censo educacional e a Resolução da Assembleia da ONU nº 68/261/2014, que dispõe sobre o sigilo estatístico (BRASIL, 2018).

A liminar foi deferida pelo Ministro Luís Roberto Barroso para suspender a disponibilização dos dados individualizados do Censo Educacional e do ENEM do período entre os anos de 2013 a 2016, requisitados pelo Tribunal de Contas da União (TCU), bem como as sanções impostas à autoridade responsável pela entrega dos dados.

O Ministro Relator ponderou que a finalidade declarada no ato da coleta dos dados deveria ser observada, do mesmo modo, a garantia de sigilo quanto às informações pessoais prestadas.

> Nesse aspecto, a transmissão a outro órgão do Estado dessas informações e para uma finalidade diversa daquela inicialmente declarada subverte a autorização daqueles que forneceram seus dados pessoais, em aparente violação do dever de sigilo e da garantia de inviolabilidade da intimidade (BRASIL, 2018).

Após a interposição de agravo regimental contra a decisão liminar deferida e a manifestação da Procuradoria-Geral da República (PGR), o Mandado de Segurança encontra-se concluso ao relator.

---

[37] Veja a reportagem: https://g1.globo.com/educacao/noticia/2019/05/17/disputa-sobre-acesso-a-dados-sigilosos-de-alunos-pesou-na-demissao-do-presidente-do-inep.ghtml

Constata-se que os objetos dessas normativas são, pura e simplesmente, direitos e deveres, positivados sob a forma de regras e princípios que deverão ser respeitados pelos agentes públicos, não tendo o legislador pátrio, até então, se ocupado em procedimentalizar a efetivação destes direitos e deveres, ditando quando, onde e como fazê-lo (processos e ferramentas de gestão, que deverão funcionar de forma harmônica e suportados por um patrocínio ético ostensivo – bem exemplificado e comunicado – por parte das lideranças de cada repartição e, sobretudo, pelos integrantes da alta administração das instituições).

Por isso, essas leis, que não foram revogadas mesmo com a entrada em vigor da Lei Geral de Proteção de Dados Pessoais, deverão, sempre, ser interpretadas e obedecidas à luz dos preceitos gerais desta, de maneira a viabilizar, conglobadamente, o início da jornada de maturidade a qual a Administração Pública brasileira precisará percorrer para fins de concretização – não apenas em Proteção de Dados, mas, sobretudo, em Governança de Dados.

4.3 AS INTERFACES ENTRE A LEI DE ACESSO À INFORMAÇÃO E A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

A ideia de proteção e acesso a informações prevista no âmbito constitucional na forma expressa no art. 5º, XXXIII com ordem ao legislador infraconstitucional de que regulamentasse a previsão vem à tona em 2011 com o advento da Lei de Acesso à Informação – Lei nº 12.527, de 18 de novembro de 2011 e, posteriormente, com a Lei Geral de Proteção de Dados, destinada a proteger o titular dos dados pessoais.

Nesse contexto, a Lei de Acesso à Informação, conhecida como LAI, concretiza a ideia de que “[...] o direito à informação é uma garantia constitucional e sua efetivação pressupõe a participação ativa do cidadão no Estado Democrático de Direito.” (BARROS; RODRIGUES, 2017, p. 294), em que se tem a transparência como um dos princípios norteadores da Administração Pública.

A LAI, apesar de não ter como escopo principal o tratamento de dados pessoais, possui uma certa zona de sobreposição de escopos. Nesse sentido, a Lei de Acesso

à Informação apresenta o conceito de “informação pessoal” como sendo toda informação relacionada à pessoa natural identificada ou identificável relativa à intimidade, vida privada, honra e imagem (art. 4º, inciso III c/c art. 31), logo vislumbra-se um ponto de contato entre o conceito de “informação pessoal” abordado pela LAI e os de “dado pessoal” e “dado pessoal sensível” da LGPD, isso porque

> […] embora não haja na referida lei um conceito possível de ser associado ao de “dado pessoal sensível”, entendemos que sua definição na LGPD abre espaço para o relacionarmos com o conceito de “informação pessoal” da LAI, visto que os dados pessoais de origem racial, convicção religiosa, opinião política, saúde, vida sexual, etc. têm direta ligação com a intimidade, vida privada, honra e imagem das pessoas naturais (BARROS; SILVA; SCHMIDT, 2019, p. 30).

Desse modo, deve-se compreender que não há um antagonismo entres os dois marcos jurídicos, isto é, a LAI e a LGPD não são normas colidentes e sim complementares para a necessária proteção de direitos constitucionalmente assegurados, sendo inclusive acolhidos pelo mesmo artigo, qual seja o artigo 5º, da CF.

De certo modo, a LAI pode ser considerada como precursora da LGPD na medida em que estabeleceu um mini estatuto de dados pessoais ao dispor, por exemplo, sobre consentimento e acesso, já “a LGPD parece preencher essa lacuna ao explicar qual a origem dos dados ou informações de caráter sensível” (BARROS; SILVA; SCHMIDT, 2019, p. 30).

Ademais, a Lei de Acesso à Informação não disciplina pormenorizadamente o tratamento de informações pessoais pelos entes públicos, o *caput* do seu artigo 31[38] cuida de alguns tratamentos específicos e estabelece *standards* para o tratamento de dados da vida privada respeitando a transparência e a intimidade.

> A ideia de “tratamento” presente em ambas as definições remete a todo o processo que envolve o trato de um dado ou informação. O que se pode observar é que a operação que envolve o tratamento de dados parece mais ampla que o conjunto de ações que envolvem o tratamento de informações. (BARROS; SILVA; SCHMIDT, 2019, p. 31).

[38] 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.

Posteriormente, os parágrafos do mencionado artigo 31 tratam acerca da divulgação e acesso a informações pessoais. Ainda neste mesmo artigo, o parágrafo 5º remete à regulamentação a tarefa de estabelecer em minúcias sobre o tratamento de informações pessoais. De fato, essa regulamentação mais detalhada é identificada na Lei Geral de Proteção de Dados que se aprofunda na temática dos dados pessoais em si tanto para o setor público quanto para o setor privado, com exceções previstas no artigo 4º, da LGPD.

O tratamento desse tipo de informação continua sujeito exclusivamente a Lei de Acesso à Informação ou então a legislação especial pertinente. Ademais, a própria LGPD no § 3º, do artigo 23, ressalta que:

> Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data) , da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo) , e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) (BRASIL, 2018).

Ainda em relação a LAI, cumpre ressaltar a recente alteração sofrida pela Lei por intermédio da edição da Medida Provisória nº 928/2020 que restringiu a possibilidade de o cidadão solicitar informações sobre os atos do Governo Federal e em seu artigo 6º-B prevê:

> Art. 6º-B. Serão atendidos prioritariamente os pedidos de acesso à informação, de que trata a Lei nº 12.527, de 2011, relacionados com medidas de enfrentamento da emergência de saúde pública de que trata esta Lei.
> § 1º Ficarão suspensos 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:
> I – acesso presencial de agentes públicos encarregados da resposta; ou
> II – agente público ou setor prioritariamente envolvido com as medidas de enfrentamento da situação de emergência de que trata esta Lei.
> § 2º Os pedidos de acesso à informação pendentes de resposta com fundamento no disposto no § 1º deverão ser reiterados no prazo de dez dias, contado da data em que for encerrado o prazo de reconhecimento de calamidade pública a que se refere o Decreto Legislativo nº 6, de 20 de março de 2020.
> § 3º Não serão conhecidos os recursos interpostos contra negativa de resposta a pedido de informação negados com fundamento no disposto no § 1º.
> § 4º Durante a vigência desta Lei, o meio legítimo de apresentação de pedido de acesso a informações de que trata o art. 10 da Lei nº 12.527, de 2011, será exclusivamente o sistema disponível na internet. § 5º Fica suspenso o

> atendimento presencial a requerentes relativos aos pedidos de acesso à informação de que trata a Lei nº 12.527, de 2011.

Logo após a entrada em vigor da referida MP, foi ajuizada a Ação Direta de Inconstitucionalidade nº 6.351 para ser declarada a inconstitucionalidade da MP em razão da limitação ao direito à informação, à transparência e à publicidade. Em sede de decisão liminar, o Ministro Relator Alexandre de Moraes suspendeu a eficácia da MP, decisão que foi posteriormente referendada por unanimidade pelo Plenário. Nas palavras do relator:

> [...] o artigo impugnado pretende TRANSFORMAR A EXCEÇÃO – sigilo de informações – EM REGRA, afastando a plena incidência dos princípios da publicidade e da transparência.
> A Constituição da República Federativa do Brasil, de 5 de outubro de 1988, consagrou expressamente o princípio da publicidade como um dos vetores imprescindíveis à Administração Pública, conferindo-lhe absoluta prioridade na gestão administrativa e garantindo pleno acesso às informações a toda a Sociedade. [...]
>
> A participação política dos cidadãos em uma Democracia representativa somente se fortalece em um ambiente de total visibilidade e possibilidade de exposição crítica das diversas opiniões sobre as políticas públicas adotadas pelos governantes, como lembrado pelo JUSTICE HOLMES ao afirmar, com seu conhecido pragmatismo, a necessidade do exercício da política de desconfiança (politics of distrust) na formação do pensamento individual e na autodeterminação democrática, para o livre exercício dos direitos de sufrágio e oposição; além da necessária fiscalização dos órgãos governamentais, que somente se torna efetivamente possível com a garantia de publicidade e transparência. (BRASIL, 2020c, grifos do autor)

Assim como a MP nº 954, a Medida Provisória nº 928 também representou uma violação à proteção de dados ao impulsionar restrições de acesso à informação nos entes federativos. Nessa perspectiva, Gargarella e Roa Roa (2020) argumentam que medidas de emergência deflagradas pela crise sanitária da Covid-19 podem representar uma erosão democrática em governos latino-americanos e, esclarecem que em momentos de crise institucional é mais prudente adotar decisões que garantam a estabilidade e o controle.

Contudo, o que se vê reiteradamente é o uso abusivo de medidas que reforçam o poder presidencial, como a legislação pela via de medidas protetivas e decretos e, de forma alarmante, a decretação de estados de exceção, sem nenhuma transparência.

5 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS COMO FERRAMENTA DE BOAS PRÁTICAS E GOVERNANÇA DA ADMINISTRAÇÃO PÚBLICA

O Estado tem se tornado cada vez mais aparelhado tecnologicamente com sistemas sofisticados para a coleta, processamento e armazenamento de dados pessoais, exigindo novas maneiras de lidar com as informações. Como aponta Agambem

> O que preocupa não é tanto, ou não somente, o presente, mas o depois. Assim como as guerras deixaram de herança à paz uma série de tecnologias nefastas, dos arames farpados às centrais nucleares, também é muito provável que se tente dar continuidade, mesmo após a emergência sanitária, aos experimentos que antes os governos não conseguiam realizar: [...] (AGAMBEN, 2020, p. 11).

Assim, diante das fragilidades e receios já tratados anteriormente no que tange ao tratamento de dados pessoais, especialmente em momentos de crises, é inevitável indagar sobre a possibilidade de se implementar, de modo efetivo, um sistema de Governança de Dados.

As melhores práticas de Governança indicam a compreensão, o respeito e o atendimento às expectativas das partes interessadas[39], sejam elas direitos e deveres que repercutam em suas esferas patrimoniais ou íntimas, ligadas à sua privacidade e intimidade e, possibilitam a estruturação de um ambiente pautado na confiança, transparência e responsabilidade, especialmente, na lida com os direitos fundamentais e visando a integridade.

Neste viés particular à proteção de dados, as autoridades internacionais vêm se debruçando, dentre diversos outros pontos relevantes que ainda carecem da adequada tutela estatal, sobre a construção de um sistema de regulamentação e fiscalização do uso de dados pessoais pelas empresas e órgãos da Administração Pública, visando ao que se denomina “Governança de Dados”.

---

[39] De acordo com a ISO (*International Organization for Stardardization*), item 3.2 da Norma 37301:2021 “parte interessada (termo preferido), stakeholder (termo admitido), pessoa ou *organização* (3.1) que pode afetar, ser afetada ou se perceber afetada por uma decisão ou atividade.”

Sem embargo, falar em Governança de Dados pressupõe, antes de tudo, o fomento, na Administração Pública, da cultura de Governança e Integridade em seu sentido mais abrangente, abalizada pelos princípios da transparência, equidade, prestação de contas e responsabilidade.

Logo, impõe-se como necessária a reflexão acerca do posicionamento da Administração Pública em relação à governança de dados e o que precisa ser institucionalizado a partir da experiência atual e para além do contexto pandêmico e suas implicações sobre a gestão de crises, em que várias medidas são implementadas às pressas, sem um debate e supervisão apropriados e, dificilmente serão reversíveis.

A crise sanitária ressalta os desafios e os benefícios do acesso aos dados no auxilio aos Administradores quanto a tomada de decisões. Coerência na tomada de decisão requer boa governança de dados.

“A governança responsável de dados inclui também a descrição das metodologias de processamento e análise dos dados, pois dados têm valor de prova, de evidência, na tomada de decisão tanto para políticas públicas quanto para ciência” (ALMEIDA, 2020, p. 2490).

A crise sanitária trouxe à tona as limitações do atual estado de acesso e compartilhamento de dados e, a necessidade de se aprimorar as habilidades e ferramentas de sistema de dados do país.

5.1 A BOA GOVERNANÇA: CONCEITO E PRINCÍPIOS

A expressão Governança pode ser conceituada “como a maneira na qual o poder é exercido na gestão dos recursos econômicos e sociais para o desenvolvimento”[40] (WORLD BANK, 1992).

[40] No original: Governance is defined as the manner in which power is exercised in the management of a country’s economic and social resources for development.

Nessa senda, a busca pelo desenvolvimento econômico-social horizontal, ético e inclusivo, sedimentou-se o que, hoje, denominamos Governança Corporativa ou Governança Pública.

Cumpre ressaltar que governo e governança não devem ser entendidos como sinônimos, em que pese o primeiro estar contido no segundo, isto porque

> Governo sugere atividades sustentadas por uma autoridade formal, pelo poder de polícia que garante a implementação das políticas devidamente instituídas, enquanto governança refere-se a atividades apoiadas em objetivos comuns, que podem ou não derivar de responsabilidades legais e formalmente prescritas e não dependem, necessariamente, do poder de polícia para que sejam aceitas e vençam resistências (ROSENAU, 2000, p. 15).

Nesse sentido, o governo é personificado na figura do governante, sendo parte de um conjunto maior de elementos, a governança que contempla ritos e processos que devem funcionar de forma harmônica.

Assim, a boa governança pode ser traduzida na capacidade do Estado em governar de forma responsável e deve incorporar ao menos três dimensões: política, econômica e institucional. A dimensão política na medida em que se observa o processo eleitoral das autoridades políticas; uma dimensão econômica que reflete a capacidade governamental de gerir de forma eficaz os recursos e implementar políticas públicas e, uma dimensão institucional que emerge do respeito aos cidadãos e ao Estado pelas instituições (KAUFMANN, 2015).

Os principais regramentos de abrangência internacional sobre governança são de autoria da *Organisation for Economic Co-operation and Development* (OECD) intitulado “Princípios da OCDE sobre o Governo das Sociedades” (1999); a Lei “Sarbanes-Oxley” (2002), dos senadores norte-americanos Paul Sarbanes e Michael Oxley e; a “*ICGN Statement On Global Corporate Governance Principles*” (2005) da *International Corporate Governance Network* (ICGN).

Outrossim, a Comissão das Comunidades Europeias elaborou o Livro Branco sobre a governança europeia e estabeleceu cinco princípios políticos fundados na boa governança: a) Abertura: as instituições deverão adotar formas mais transparentes

sobre suas tarefas e decisões; b) Participação: a participação aberta e abrangente no desenvolvimento e aplicação das políticas das instituições, desde o início até sua execução; c) Responsabilização: assumir responsabilidades a todos que participam da elaboração e aplicação das políticas; d) Eficácia: as políticas deverão ser eficazes e aplicadas de forma que proporcione os objetivos e que as decisões sejam adotadas em níveis mais adequados; e) Coerência: as políticas e as medidas utilizadas deverão ser coerentes e compreensíveis, estabelecendo uma liderança política com forte responsabilidade por parte das instituições (COMISSÃO DAS COMUNIDADES EUROPEIAS, 2015).

No Brasil, o marco teórico sobre o tema é o “Código das Melhores Práticas de Governança Corporativa”, do Instituto Brasileiro de Governança Corporativa (IBGC), datado de 1999.

Segundo o IBGC,

> Governança Corporativa é o 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 (IBGC, 2015. p. 20-21).

Embora definidos e consolidados em regramentos e diretrizes voltados ao aprimoramento da gestão de negócios privados, é certo que os princípios da boa governança, não só podem, como devem, ser aplicados à Administração Pública.

Sob esta ótica, a governança de dados deve ser entendida como ponto de partida para o gerenciamento dados e deve fornecer respostas a perguntas referentes à disponibilidade, possibilidades de acesso, proveniência, significado e confiabilidade, isto é: Quais são os dados disponíveis e como seu conteúdo pode ser compartilhado? Poderia os dados rastreados serem compartilhados com demais pessoas, incluindo aquelas fora da Administração Pública? Como pode o processo ser mais transparente?

Os mecanismos de governança devem colaborar para que os governantes implementam estratégias de longo prazo e, justamente por serem de longo prazo, não

devem se limitar a projetos de um ou outro governante, suscetíveis a variações de direção ao sabor do grupo mandatário momentaneamente empossado. Logo, as diretrizes do Estado devem estar dispostas nas políticas públicas desenvolvidas pelos órgãos competentes e aprovadas pelas instâncias constitucionalmente responsáveis.

A governança passa a ser um elemento chave para que os mandatários tenham autonomia e dinâmica necessárias para tomar decisões sem ferir os limites que lhes foram impostos, especialmente os direitos fundamentais.

Sob esse prisma, para que ocorra a transformação necessária à boa governança pública, a OCDE destaca ações que transponham a esfera do Poder Executivo, envolvendo os Poderes Legislativo e Judiciário (dados os papéis de regulação e fiscalização que desempenham, indispensáveis à integridade de um país).

Ao compilar as medidas e controles sugeridos pela OCDE à boa Governança Pública, é possível perceber uma simetria com os princípios da Governança Corporativa, conforme se vê: (i) demonstração do compromisso nos mais altos níveis políticos e administrativos do setor público para aumentar a transparência, a equidade e a integridade; (ii) capacitação e profissionalização do setor público, implementação de meritocracia e esclarecimento dos papéis e responsabilidades institucionais em todos os setores, visando à sua plena eficiência; (iii) desenvolvimento de uma abordagem estratégica para o setor público, que se baseie em evidências e vise atenuar os riscos de não-conformidade, através de mecanismos de gerenciamento e controle interno; (iv) definição de altos padrões de conduta para funcionários públicos, que engaje e gere aderência de toda a sociedade (setor privado, sociedade civil e indivíduos, como partes interessadas que são); (v) incentivo à transparência e ao envolvimento das partes interessadas em todas as etapas do processo político e do ciclo político, para promover a prestação de contas e o interesse público, reforçando o papel de fiscalização e controle externo (OCDE, 2017).

A boa governança, seja ela privada ou pública, necessita de uma visão mais ampliada e sistêmica: a gestão se organiza e executa em retroalimentação, facilitando que agentes e partes interessadas *(stakeholders*) interajam de forma coordenada e

transparente, contribuindo para o aperfeiçoamento e valorização de todo o contexto que é administrado e legitimando, de modo equânime, a todos os que, direta ou indiretamente, são por ela impactados.

Mais do que atender a objetivos dos donos e/ou responsáveis pela propriedade administrada, como ditavam os antigos modelos de gestão, a boa governança requer a compreensão, o respeito e o atendimento às expectativas dos *stakeholders* – expectativas estas que se traduzem em direitos e prerrogativas, positivados na Constituição e em tratados, convenções, leis, decretos, sentenças e contratos.

Nesse sentido, cumpre ressaltar que "A legitimidade de coleta, processamento, compartilhamento e uso de dados pessoais não advém do acesso aos dados, mas da confiança em quem os detém, tratando-os com transparência e dentro dos parâmetros legais" (ALMEIDA, 2020, p. 2490).

E é com esse propósito, de atenção ao direito à intimidade e privacidade dos indivíduos, que autoridades internacionais do mundo todo, encabeçadas por potências da América do Norte e da União Europeia, vêm se debruçando, dentre diversos outros pontos relevantes que ainda carecem da adequada tutela jurídica, sobre a construção de um sistema de regulamentação e fiscalização do uso de dados pessoais pelas empresas e órgãos da Administração Pública, visando ao que se denomina Governança de Dados.

Na linha dos *standards* internacionais de Governança de TI e Dados Pessoais, como o exemplo do COBIT, as leis propriamente ditas – emanadas das autoridades legislativas de cada país, ou da união de países – têm, cada vez mais, deixado de ser instrumento, pura e simplesmente, de regulamentação da conduta de indivíduos para assumirem o importante papel de ferramentas de gestão ética, inovadora e eficiente de negócios públicos e privados.

Ao atestar o que ora se afirma, sobreleve-se a entrada em vigor, em 25 de maio de 2018, do Regulamento Geral de Proteção de Dados da União Europeia, que serviu a

atualizar a “Diretiva Europeia de Proteção de Dados” (*Directive 95/46/EC*)[41] – regramento cuja vigência datava de 1995 – para, além de alterar as relações estabelecidas no próprio continente, impactar aquelas entabuladas com outros países, inclusive o Brasil.

Um aspecto relevante refere-se à autodeterminação informacional, que empodera o titular dos dados em detrimento do agente que lhes esteja requisitando para uso e compartilhamento. Logo “a autodeterminação informativa é, indubitavelmente, um aspecto fundamental a ser levado em consideração para o uso de dados pessoais, conjuntamente com as garantias de transparência, segurança e minimização no uso de dados” (ALMEIDA, 2020, p. 2489).

Além disso, observa-se que a LGPD impõe a Governança de Dados não apenas às empresas privadas, como, também, à Administração Pública, propondo uma mudança profunda e sensível de paradigma às instituições que, desde sempre, são as principais requisitantes e mantenedoras de dados pessoais – os Poderes Executivo, Legislativo e Judiciário – a partir do momento em que condiciona a coleta, uso e compartilhamento de informações relevantes à identificação dos administrados (notadamente, aquelas ligadas às suas características pessoais, financeiras, políticas, religiosas e de saúde) ao consentimento e monitoramento destes.

Inobstante seja a autodeterminação informativa um direito a ser observado, há de se ressaltar que, em casos excepcionais, o consentimento pode ser suprimido em razão do interesse público.

> Entretanto, existem situações em casos de emergência e de interesse público, como a saúde pública, em que o uso de dados pessoais é permitido, mesmo sem o consentimento do seu titular, desde que haja salvaguardas, proporcionalidade no uso dos dados para alcance das finalidades e especificidades relacionadas às credenciais dos órgãos autorizados a processar esses dados, conforme estabelecido na Lei Geral de Proteção de Dados brasileira e no Regulamento Geral de Proteção de Dados da União Europeia (ALMEIDA, 2020, p. 2489).

[41] In: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046

Nesse sentido, a Lei de Proteção de Dados Pessoais estabelece os alicerces mínimos a serem erigidos nas estruturas de gestão para uma arquitetura de Governança de Dados, isto é, políticas, modelos, processos, posturas alinhadas e concatenadas, e, por fim, capacitação para uso ético e consciente de infraestrutura de Tecnologia da Informação).

5.2 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E A GOVERNANÇA PÚBLICA

Como dito, a Administração Pública sempre foi a principal requisitante e mantenedora de dados pessoais do país e, com o advento da LGPD, o tratamento de dados a ser realizado pelo Poder Público passa a observar obrigatoriamente os preceitos da legislação em comento.

Desse modo, observando-se a lei, para que o tratamento de dados possa ser realizado pela Administração Pública, deverão ser informadas as hipóteses em que ocorrerão, bem como serem fornecidas 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 no *site* dos órgãos e entidades), como, também, a indicação do encarregado que ficará responsável pela operação de tratamento.

A Lei Geral de Proteção de Dados Pessoais brasileira concebeu-se, tal qual a Europeia, sob as premissas de respeito aos direitos dos indivíduos, com foco na obtenção de seu prévio consentimento, que deve ser solicitado de forma clara e pode ser retirado a qualquer momento.

Para consecução deste objetivo, a lei estabelece às organizações públicas e privadas uma série de processos, procedimentos e controles internos preventivos – formulários de consentimento, contratos de coleta e processamento, implementação de infraestrutura e mecanismos de segurança adequados aos riscos específicos a que cada uma está exposta (a depender do local onde se situa, número de servidores ou colaboradores, nível de sofisticação de suas ferramentas de gestão interna e grau de

sensibilidade dos dados recebidos e tratados), além da obrigação de comunicação de vazamento aos titulares, quando houver.

Logo,

> Ao considerar que dados podem ser utilizados e compartilhados por diferentes pessoas e organizações simultaneamente, as questões principais a serem harmonizadas giram em torno da governança responsável dos dados baseada na transparência e empoderamento dos cidadãos para que haja confiança e estabelecimento de relacionamentos equilibrados e justos entre indivíduos e organizações (ALMEIDA, 2020, p. 2490).

Neste diapasão, e como se não bastasse, simplesmente, a alusão a posturas éticas, transparentes e responsáveis, o legislador, no artigo 49, menciona expressamente a imperiosidade de se tratar dados conforme as melhores práticas de Governança:

> Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Especificamente no que toca às posturas e ferramentas que deverão permear a modelagem de Governança de Dados a se implementar, a Lei Geral de Proteção de Dados Pessoais, pontuou-os no artigo 50, § 2º, inciso I:

> Art. 50. [...].
>
> § 2º. Na aplicação dos princípios indicados nos incisos VII e VIII do *caput* do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:
> 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. [...]. (Grifou-se).

Já o Decreto nº 10.046/2019[42] 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. Em relação ao Comitê, observa-se que, de acordo com o artigo 21 do supracitado Decreto, este possui competência para deliberar, entre outros assuntos, sobre:

> Art. 21. [...].
> I - as orientações e as diretrizes para a categorização de compartilhamento amplo, restrito e específico, e a forma e o meio de publicação dessa categorização, observada a legislação pertinente, referente à proteção de dados pessoais;
> II - as regras e os parâmetros para o compartilhamento restrito, incluídos os padrões relativos à preservação do sigilo e da segurança;
> III - a compatibilidade entre as políticas de segurança da informação e as comunicações efetuadas pelos órgãos e entidades de que trata o art. 1º, no âmbito das atividades relativas ao compartilhamento de dados;
> IV - a forma de avaliação da integridade, da qualidade e da consistência de bases de dados derivadas da integração de diferentes bases com o Cadastro Base do Cidadão;
> VI - as orientações e as diretrizes para a integração dos órgãos e das entidades de que trata o art. 1º com o Cadastro Base do Cidadão [...].

Com efeito, além dos dados que são condicionados à utilização de serviços públicos, a finalidade primordial do tratamento de dados refere-se à execução de políticas públicas que estejam previstas em leis e regulamentos, ou que estejam respaldadas em contratos, convênios ou instrumentos congêneres (art. 7º, III, LGPD) – hipóteses em que, embora dispensado o consentimento do titular, obrigam a Administração a informar a finalidade e a forma como esses dados serão tratados.

No Brasil, em se tratando de Governança e Integridade Pública, apesar de signatário da convenção da OCDE de 1997, recepcionou-a no ordenamento jurídico apenas no ano 2000, por intermédio do Decreto nº 3.678.

Com os avanços tecnológicos, o Poder Público tem se tornado cada vez mais digital e, com isso, solicitado um maior volume de dados pessoais em seus aplicativos voltados ao acesso a serviços/documentos públicos – como a Carteira Nacional de

[42] *In:* http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm

Habilitação – “CNH Digital”, “Meu INSS”, solução multi-dipositivos para acesso aos serviços do INSS – e, mais recentemente o auxílio emergencial, bem como demais sites, para o preenchimento de cadastros para concessão de benefícios assistenciais, para possibilitar/autorizar a utilização do Sistema Único de Saúde – SUS, ou para desconto/isenção em transporte urbano municipal por pessoas de baixa renda e/ou com deficiência.

Nesse contexto, “[...] revela-se, como componente essencial no processo de construção de instrumentos de ação pública, a garantia da adoção de alguns direitos básicos que envolvem, hoje, o uso da criptografia, a garantia de anonimização dos dados pessoais e o consentimento informado do titular desses dados” (FREITAS; CAPIBERIBE; MONTENEGRO, 2020, p. 196-197).

Isto porque, em muitos destes casos, não são informadas ou demonstradas as medidas de segurança da informação adotadas para prevenir a ocorrência de danos aos dados, nem mesmo são informados como são realizados os tratamentos destes, o que acaba por ferir diversos princípios do tratamento de dados e coloca em risco os direitos fundamentais elencados no art. 1º, *caput*, da Lei Geral de Proteção de Dados Pessoais[43].

A especificação técnica das tecnologias a serem utilizadas deve garantir todos a observância de princípios elencados na LGPD como: minimização de dados, limitação de propósito, limitação de armazenamento, integridade e confidencialidade, legalidade, justiça e transparência, responsabilidade e precisão. O uso desses aplicativos devem ser proporcionais ao seu objetivo e limitados ao tempo de emergência.

Além disso, constata-se que raras são as situações nas quais os aplicativos do Poder Público solicitam permissões adequadas. Nesse sentido, entende-se como permissões adequadas, aquelas que guardam relação com as funcionalidades para as quais foram solicitadas, bem como as que informam aos titulares sobre o direito ao

[43] Aponta o art. 1º, *caput*, da LGPD, que são direitos fundamentais protegidos pela Lei: a liberdade, a privacidade e o livre desenvolvimento da personalidade da pessoa natural

acesso gratuito e facilitado quanto à duração do tratamento e à integridade dos seus dados.

Para corroborar tal entendimento, colaciona-se o estudo realizado pelo INTERNETLAB[44], onde foram analisadas as permissões solicitadas pelos aplicativos do Governo, a fim de verificar quais delas e guardam relação com as funcionalidades proposta por esses *softwares*. Nele, constatou-se que diversos aplicativos do governo brasileiro não observavam regras e princípios básicos da segurança da informação, como o princípio do menor privilégio[45], que estabelece que todo programa deve operar utilizando o menor número de privilégios possíveis, garantindo assim, menos vulnerabilidade e mais segurança e estabilidade aos usuários, evitando exposição a riscos desnecessários.

Como exemplo, cita-se duas permissões de acesso consideradas perigosas, como a relativa à geolocalização (GPS) do aparelho, requeridas pelos aplicativos do FGTS, CAIXA, Bolsa Família e Meu INSS, e a de acesso a contas cadastradas no dispositivo, como as requeridas pelos aplicativos do FGTS e Bolsa Família.

Extreme de dúvidas, a falta de motivação razoável à quantidade expressiva de dados solicitados aos administrados, associada à vulnerabilidade dos controles internos que permeiam os processos de gestão de grande parte das repartições públicas do país, e à falta de capacitação adequada dos servidores e colaboradores terceirizados à lida geral com as informações a que têm acesso diariamente (desde a operação correta das ferramentas tecnológicas até a falta de discernimento sobre o uso correto dos dados pessoais), decorrem da falta de diretrizes éticas claras por parte das lideranças hierarquicamente superiores, assim como da falta da devida fiscalização e punição aos infratores.

Em termos equivalentes, a tríade “prevenção, detecção e resposta”, ínsita a qualquer Sistema de Governança e Integridade, não funciona de forma efetiva e sistêmica em

---

44 *In:* https://www.internetlab.org.br/pt/privacidade-e-vigilancia/especial-as-permissoes-de-acesso-dados-em-apps-do-governo/

45 O princípio do menor privilégio, apontado pelo INTERNETLAB como princípio básico da segurança da informação, assimila-se ao “princípio da necessidade” na “Lei Geral de Proteção de Dados”.

se tratando da Administração Pública brasileira, e isto é consectário, muito mais do que da precariedade de recursos financeiros e tecnológicos, da fragilidade da cultura organizacional ética, sentida na tomada de decisões, muitas vezes, desalinhadas aos princípios da legalidade, motivação, moralidade e supremacia do interesse público, mas, por outro lado, servientes a estratégias de cunho pessoal, financeiro e, principalmente, político dos administradores públicos, de outros colegas de partido, apoiadores de campanha, familiares e amigos.

À vista disso, o Brasil, em sentido oposto às diretrizes e tendências mundiais quanto à Governança e Integridade Pública, não incluiu a Administração Pública no escopo da Lei Geral de Proteção de Dados Pessoais brasileira – LGPD, de forma que a aplicação é restrita ao setor privado.

Nesse diapasão, a implementação de Governança de Dados no Brasil representa um enorme desafio à sua Administração Pública, que transcende o aspecto legal, pois, para se falar em Governança de Dados, invariavelmente deverá preexistir, como já frisado alhures, uma cultura organizacional de Governança e Integridade Pública.

CONSIDERAÇÕES FINAIS

O embate entre os direitos fundamentais notadamente o direito à incolumidade pública *versus* a privacidade e a proteção de dados ganha destaque em pronunciamentos do Supremo Tribunal Federal com os desdobramentos da pandemia pelo Covid-19. Isto porque, sob a justificativa de garantir a contenção da propagação do vírus, o Estado desenvolveu mecanismos para o compartilhamento de dados pessoais, o que acabou por acender um alerta quanto à discussão do tema. Porém, diversas dessas medidas foram praticadas em inobservância das normas, princípios e direitos contidos na Lei Geral de Proteção de Dados – LGPD. Como exemplo, cita-se o princípio da necessidade ou da minimização de dados, elencado no art. 6º, inciso III, que prevê que o tratamento de dados deverá ocorrer ao mínimo necessário ao atingimento de suas finalidades (TORRES; AZEVEDO, 2020).

A falta de previsibilidade em relação à duração de determinado fato como a pandemia faz com que o uso de dados para efeitos de contenção da disseminação da doença seja feito com muita responsabilidade, ainda que a utilização de dados pessoais possa possibilitar a contenção de uma pandemia. Isso porque, é preciso assegurar que tais dados serão utilizados de acordo com a finalidade legítima e, ao mesmo tempo, com todas as salvaguardas para o cidadão.

O debate crescente em torno do design, implantação, regulamentação e – embora menos ainda - a eficácia dos aplicativos de rastreamento de contato digital foi permeada pela narrativa que a saúde pública é mais importante do que a privacidade quando o tempo é um problema.

O combate e enfrentamento a pandemia do Covid-19 tem sido uma justificativa para adoção de medidas controversas e que podem resvalar para um aprofundamento de uma sociedade de vigilância. Seria razoável passar por cima de todos os direitos estabelecidos sob o pretexto de enfrentar o vírus?

Logo, a coleta de dados massiva e muitas vezes irregular para finalidades vagas e não muito claras evidencia a necessidade, no âmbito brasileiro, de consolidação da

LGPD e consequentemente da proteção de dados. Igualmente, se acende um alerta sobre a questão do estado de vigilância, visto que, uma vez na posse e controle de tais dados do que o Estado seria capaz?

A pandemia representa um teste para a democracia e os direitos individuais, isto porque, o risco para a democracia se coloca em primeiro lugar diante da própria amplitude dos dados pessoais, quando falamos em proteção de dados pessoais estamos falando em proteção da individualidade, os riscos de manipulação dos cidadãos em uma série de aspectos das nossas escolhas, inclusive escolhas políticas são muito fortes.

Assim, em uma democracia quando o fluxo informacional não apenas é decidido por alguns agentes, mas também manipulado por esses agentes há um problema, porque a democracia pressupõe informação e liberdade de escolha e todos esses pilares podem ser comprometidos nessa atual sociedade movida a dados.

Ao se pensar na pandemia, acrescenta-se um outro ingrediente, também de extremo grau de periculosidade, uma vez que de fato pode ser que o Estado tenha que intervir com maior intensidade no controle da doença e, desse modo precise ter acesso a dados pessoais dos cidadãos, inclusive dados biológicos que, se bem utilizados, sem dúvida são ações legítimas mas, por outro lado, se mal utilizados poderão inclusive agravar todo esse processo pelo qual nossas liberdades e nossas individualidades crescentemente são colocadas em risco.

Ao que tudo indica, até pela completude de tecnologias disponíveis, desde que tomadas cautelas como o cumprimento de alguns pressupostos do que seria uma boa política de segurança de dados, assegurando a finalidade, proporcionalidade do meio, transparência, *accountability* e, ainda que ao término da finalidade proposta os dados serão realmente ou anonimizados ou então totalmente desconsiderados. Logo, há uma série de opções jurídicas, econômicas e tecnológicas que possibilitam a conciliação entre a incolumidade pública e o direito à privacidade e liberdades individuais dos usuários.

Sempre que se for utilizar determinada tecnologia que visa uma finalidade específica, há alguns passos relevantes em termos de proteção de dados que devem ser levados em consideração para se avaliar se a tecnologia escolhida deve ser, de fato, aplicada ou não. O primeiro deles é verificar qual a finalidade, e se essa finalidade tem evidência científica; avaliar se a coleta e o uso de dados são proporcionais e se se utiliza o mínimo de dados possíveis para que aquela finalidade seja cumprida.

O tratamento dos dados deve ser realizado proporcionalmente à finalidade desejada, não sendo admissível que informações pessoais sejam coletadas e quiçá expostas ou compartilhadas, garantindo a proteção do direito fundamental à privacidade.

A resposta ao questionamento acerca da possibilidade e viabilidade ou não de utilização de dados pessoais de forma temporária para o gerenciamento de uma crise como a pandemia de COVID-19 dependerá da forma como esses dados serão manejados, ou seja, se estes serão utilizados de forma adequada e adstrita às finalidades a que se propõem, tendo em vista que o tratamento inadequado pode acarretar danos colaterais irreparáveis no campo do direito à privacidade dos indivíduos. Logo, é necessário que sejam adotadas medidas de segurança, técnicas e administrativas para impedir o vazamento dos dados, fazendo com que terceiros tenham acesso a eles. Do mesmo modo, mostra-se necessário impedir o compartilhamento dos dados com terceiros.

A transparência não só em relação ao compartilhamento dos dados bem como, quanto à finalidade para qual esses dados são coletados e tratados e o período de retenção por meio do qual os dados permanecerão armazenados são medidas que se impõe necessárias. Uma vez encerrada essa finalidade, a manipulação daqueles dados deve ser encerrada, com a eliminação daqueles.

Nesse sentido, a Lei Geral de Proteção de Dados se mostra um mecanismo muito oportuno e adequado, na medida em que sedimenta a aplicação de princípios e diretrizes internacionais em relação ao direito à privacidade.

Não obstante, a pandemia de COVID-19 também evidenciou a importância não apenas do marco regulatório para a proteção dos dados pessoais, mas também a

atuação da Autoridade Nacional de Proteção de Dados - órgão responsável por fiscalizar o cumprimento desse marco regulatório, de modo a garantir a efetiva aplicação das normas de privacidade e proteção de dados.

É preciso buscar um equilíbrio entre os direitos fundamentais, ainda que se tenha um choque entre o interesse público e o direito à privacidade. Deve haver uma busca constante pelo equilíbrio entre as liberdades civis e o interesse coletivo, buscando uma proporcionalidade.

Portanto, os eventuais riscos advindos do estado de vigilância, apoiado no uso da tecnologia da informação devem ser detidamente analisados antes de qualquer medida extrema que usurpe o direito à privacidade, para evitar que a ampla proteção aos dados do cidadão seja afetada.

As ações tomadas pelo Estado em situações emergenciais como a provocada pela pandemia do Coronavírus devem sempre compatíveis com os princípios fundamentais da incolumidade pública e também com o direito à privacidade e liberdades individuais dos usuários.

REFERÊNCIAS

AGAMBEN, Giorgio. **Reflexões sobre a peste, ensaios em tempo de pandemia**. São Paulo: Boitempo Editorial, 2020.

ALBERS, Marion. A complexidade da Proteção de Dados. **Direitos Fundamentais & Justiça**, Porto Alegre, v. 10, n. 35, p. 19-45, jul./dez. 2016. Disponível em http://dfj.emnuvens.com.br/dfj/article/view/93.

ALMEIDA, Bethânia de Araújo et al. Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. **Ciência & Saúde Coletiva**, v. 25, p. 2487-2492, 2020.

ALMEIDA, José Rubens Mascarenhas de; MOTA, Daniel Santos. Huxley, Orwell e a realização das distopias no Brasil contemporâneo. **Lutas Sociais**, v. 23, n. 42, p. 139-155, 2019. Disponível em https://revistas.pucsp.br/index.php/ls/article/view/47442/31591

ANATEL. **Painéis de dados**: Agência Nacional de Telecomunicações. 2020. Disponível em: https://www.anatel.gov.br/paineis/acessos.

BAUMAN, Zygmunt. **Modernidade líquida**. Rio de Janeiro, Jorge Zahar Editores: 2001.

BARROS, Dirlene Santos; RODRIGUES, Georgete Medleg. Lei de Acesso à Informação: entre vozes e silêncios na divulgação pelo jornal O Estado do Maranhão. **Informação & Sociedade:** Estudos, v. 27, n. 2, 25 ago. 2017.

BARROS, Gabriel, da Silva; SILVA, Lorena, dos Santos; SCHMIDT, Clarissa. Documentos públicos e dados pessoais: o acesso sob a ótica da Lei Geral de Proteção de Dados Pessoais e da Lei de Acesso à Informação. In: **Revista do Arquivo**, São Paulo, Ano V, nº 9, p. 22-39, outubro de 2019. Disponível em http://www.arquivoestado.sp.gov.br/revista_do_arquivo/09/pdf/BARROS_S_G_et_al_-_Documentos_publicos_e_dados_pessoais_o_acesso_a_partir_da_Lei_Geral_de_Protecao_de_Dados_Pessoais_e_da_Lei_de_Acesso_a_Informacao.pdf

BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. In: **Cadernos Jurídicos** – Direito digital e proteção de dados pessoais. São Paulo: Escola Paulista de Magistratura, ano 21, n. 53, janeiro-março 2020. Disponível em https://brunobioni.com.br/wp-content/uploads/2020/04/Bioni_Anonimiza%C3%A7%C3%A3o.pdf

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

BOTELLO, Nelson Arteaga. A América Latina e o apocalipse: ícones visuais em Blade Runner e Elysium. **TECNOPOLÍTICAS**, p. 217-235, 2018. Disponível em

https://medialabufrj.net/wp-content/uploads/2020/10/Tecnopoliticas-da-vigilancia_miolo_download.pdf

BOTELHO, Marcos. A proteção de dados pessoais enquanto direito fundamental: considerações sobre a lei geral de proteção de dados pessoais. **Argumenta Journal Law**, Jacarezinho – PR, Brasil, n. 32, 2020, p. 191-207.

BULOS, Uadi Lammêgo. **Curso de direito constitucional**. 11 ed. São Paulo: Saraiva, 2018.

BRADBURY, Ray. **Fahrenheit 451**: a temperatura na qual o papel pega fogo e queima. 2ª edição. São Paulo: Globo, 2012.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. 1988. Disponível em: < http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>.

BRASIL. **Decreto nº 8.771, de 11 de maio de 2016**. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm

BRASIL. **Decreto nº 8.789, de 29 de Junho de 2016.** Dispõe sobre o compartilhamento de bases de dados na administração pública federal. Disponível em < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8789.htm>.

BRASIL. **Decreto nº 10.046, de 9 de Outubro de 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D10046.htm>.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, 18 nov. 2011. Disponível em <http//www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/ lei/l12527.htm>.

BRASIL. **Lei nº 12.965, de 23 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>.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. 2018. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>.

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: <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=17/04/2020&jornal=602&pagina=1>.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade n° 6.387/DF**. Relator: Ministra Rosa Weber. Brasília. Julgada em 24 abril 2020b. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf.

BRASIL. Supremo Tribunal Federal. **Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.351**. Relator: Alexandre de Moraes. Brasília: Supremo Tribunal Federal, 2020. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/ anexo/ADI6351.pdf.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade n° 6.649 /DF**. Relator: Ministro Gilmar Mendes. Brasília. Julgada em 28 janeiro 2020c. Disponível em: < http://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=6079238 >

BRASIL. Supremo Tribunal Federal. Habeas Corpus: **HC nº 91.867/PA**. Relator: Ministro Gilmar Mendes. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=2534858

BRÍGIDO, Edimar. Michel Foucault: uma análise do poder. **Revista de Direito Econômico e Socioambiental**, v. 4, n. 1, p. 56-75, 2013.

COOLEY, Thomas. **A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract**. Chicago: Callaghan, 1879. Disponível em: https://repository.law.umich.edu/books/11/

COHN, Marjorie. Beyond Orwell's worst nightmare, in **Huffington Post**, 31 de janeiro de 2014. Disponível em <http://www.huffingtonpost.com/marjorie-cohn/beyond-orwells-worst-nigh_b_4698242.html>.

COMISSÃO DAS COMUNIDADES EUROPEIAS. **Governança Europeia**: um livro branco. 2015. Disponível em: http://www.laicidade.org/wp-content/uploads/2006/09/ue-governanca-2001.pdf

COTS, Márcio; OLIVEIRA, Ricardo. Lei Geral de Proteção de dados pessoais comentada. 2. ed. São Paulo: **Revista dos Tribunais**, 2019.

COUTO, Carlos Agostinho de Macedo. A atualidade do panóptico de Foucault e sua relação com os meios de comunicação *in* **Revista Cambiassu**, publicação científica

do Departamento de Comunicação Social da Universidade Federal do Maranhão – UFMA – ISSN 0102-3853, São Luís - MA, vol. xvii – n º 3 - janeiro a dezembro de 2007.

DELANTY, Gerard. Seis filosofias políticas em busca de um vírus: Perspectivas críticas sobre a pandemia de Covid19. **DILEMAS**: Revista de Estudos de Conflito e Controle Social. Rio de Janeiro. Reflexões na Pandemia, 2020, pp. 1-10. Disponível em: <https://www.reflexpandemia.org/texto-13>.

DELEUZE, Gilles. Post-scriptum sobre as sociedades de controle em: DELEUZE, Gilles. **Conversações**. Trad. Peter Pál Pelbart. 1ª ed. Rio de Janeiro: Ed. 34, 1992. p. 219-226.

DILLMANN, Alexandra Tewes; PIRES FILHO, Luiz Alberto Brasil Simões. MODERNIDADE, POLICIAMENTO E VIGILÂNCIA ONIPRESENTE: 1984 NÃO É TÃO DISTANTE. In: **I Congresso Nacional de Biopolítica e Direitos Humanos**. 2018.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico, Joaçaba, v. 12, n. 2, p. 91-108, jul/dez 2011. Disponível em: http://editora.unoesc.edu.br/index.php/espacojuridico/article/download/1315/658.

EHRHARDTJÚNIOR, Marcos; CATALAN, Marcos; MALHEIROS, Pablo. **Direito Civil e Tecnologia**. Belo Horizonte/MG: Editora Fórum, 2020.

FERREIRA, Rubens da Silva. A sociedade da informação como sociedade de disciplina, vigilância e controle. **Información, cultura y sociedad**, n. 31, p. 109-120, 2014.

FOUCAULT, Michel. **A Verdade e as Formas Jurídicas** (trad. Roberto Cabral de Melo Machado e Eduardo Jardim Morais). Rio de Janeiro: Nau, 2001.

FOUCAULT, Michel. **Vigiar e Punir** (trad. Raquel Ramalhete). 28ª ed. Petrópolis: Vozes, 2002.

FREITAS, Christiana Soares de; CAPIBERIBE, Camila Luciana Góes; MONTENEGRO, Luísa Martins Barroso. Governança Tecnopolítica: Biopoder e Democracia em Tempos de Pandemia. **NAU Social**, v. 11, n. 20, p. 191-201, 2020.

GARGARELLA, Roberto; ROA ROA, Jorge. Diálogo democrático y emergencia en América Latina. (Research Paper nº 2020-21). **Heidelberg: Max Planck Institute for Comparative Public Law & International Law**, 10 jun. 2020. Disponível em: https://ssrn.com/abstract=3623812.

GEDIEL, José Antônio Peres; CORRÊA, Adriana Espíndola. Proteção Jurídica de Dados Pessoais: a intimidade sitiada entre o Estado e o Mercado. **Revista da Faculdade de Direito UFPR**, 47. Curitiba, 2008, p. 141-153.

GELLMAN, Barton; POITRAS, Laura. U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. **The Washington Post.**

Washington, 07/06/2013. Disponível em: < https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html >. Acesso em: 23 jun. 2021.

GOMES, Edivan dos Santos; ZONI, Martha. Montag e o Sabujo mecânico: poder e vigilância em Fahrenheit 451. **Megafone** – estudos de teoria e crítica literária / Marcos Paulo Torres Pereira; Rafael Senra Coelho; Willian Gonçalves da Costa (organizadores) - Macapá: UNIFAP, 2020. Disponível em https://www2.unifap.br/editora/files/2020/09/megafone.pdf#page=86

GREENWALD, Glenn. **Sem lugar para se esconder**. Rio de Janeiro: Sextante, 2014.

GREENWALD, Glenn; KAZ, Roberto; CASADO, José. **Espionagem dos EUA se espalhou pela América Latina.** O Globo. Rio de Janeiro. 09 jul, 2013. Disponível em: <https://oglobo.globo.com/mundo/espionagem-dos-eua-se-espalhou-pela-america-latina-8966619 >.

GUNDALINI, Bruno e TOMIZAWA, Guilherme. Mecanismo Disciplinar de Foucault e o Panóptico de Nenthamna Era da Informação. **ANIMA**: Revista Eletrônica do Curso de Direito das Faculdades OPET. Curitiba PR - Brasil. Ano IV, nº 9, jan/jun 2013. ISSN 2175-7119.

HAN, Byung-Chul. **O coronavírus de hoje e o mundo de amanhã**. 2020. Disponível em: <https://brasil.elpais.com/ideas/2020-03-22/o-coronavirus-de-hoje-e-o-mundo-de-amanha-segundo-o-filosofo-byung-chul-han.html>.

HARARI, Yuval Noah. O mundo depois do coronavírus. **Instituto Humanitas Unisinos online,** v. 27, n. 6, 2020. Disponível em: http://www. ihu. unisinos. br/78-noticias/597469-o-mundodepois-do-coronavirus-artigo-de-yuval-noah-harari.

HITCHENS, Christopher. **A vitória de Orwell**. São Paulo: Companhia das letras, 2010.

HUXLEY, Aldous. **Admirável mundo novo**. 24. ed. São Paulo: Globo, 1998.

IBGE. **Coleta por telefone**: Pesquisas do IBGE estão em campo com rotina ajustada à pandemia de coronavírus. 2020. Disponível em: <https://respondendo.ibge.gov.br/coleta-por-telefone.html>.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das melhores práticas de governança corporativa.** 5.ed. São Paulo, SP: IBGC, 2015

KAUFMANN, Daniel, 2005. **Myths and Realities of Governance and Corruption**. MPRA Paper 8089, University Library of Munich, Germany. Disponóvel em: https://mpra.ub.uni-muenchen.de/8089/1/MPRA_paper_8089.pdf

KOPP, Rudinei. **Comunicação e mídia na literatura distópica de meados do século 20**: Zamiatin, Huxley, Orwell, Vonnegut e Bradbury. Tese de doutorado. Porto Alegre: Programa de Pós-Graduação em Comunicação Social, PUCRS, 2011.

LACERDA, Marcos. Governança na pandemia: a ciência como regulação moral e os problemas da biopolítica. **Simbiótica. Revista Eletrônica,** 69–86, 2020. <https://doi.org/10.47456/simbitica.v7i1.30983>.

LISBOA, Roberto Senise. Boa-fé e confiança na Lei Geral de Proteção de Dados brasileira. **Revista do Advogado**, n. 144, p. 6-11, 2019.

LORENZON, Laila Neves. Análise comparada entre regulamentações de dados pessoais no brasil e na união europeia (LGPD e GDPR) e seus respectivos instrumentos de enforcement. **Revista do Programa de Direito da União Europeia**, v. 1, p. 39-52, 2021.

LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de. Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. **Revista de Direito**, v. 12, n. 02, p. 01-33, 2020.

MALDONADO, Viviane Nóbrega (coord.). **LGPD**: Lei Geral de Proteção de Dados Pessoais: manual de implementação. São Paulo: Revista dos Tribunais, 2019.

MARTINS FILHO, Altino José. Entre o visível e o invisível: reflexões acerca de um admirável mundo novo. **Revista ORG & DEMO**, v. 4, p. 97-115, 2003.

MELLO, Jamer Guterres de. Vigilância e controle na obra de Harun Farocki. **Significação**: Revista De Cultura Audiovisual, v. 45, n. 49, p. 131-148, 2018.

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da Proteção de Dados no Brasil. **Revista de Direito do Consumidor**, São Paulo, v. 27, n. 120, p. 555-587, nov./dez. 2018.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel. Habeas Data e Autodeterminação Informativa: Os Dois Lados da Mesma Moeda. Direitos Fundamentais & Justiça. **Revista Brasileira De Direitos Fundamentais & Justiça**, 12(39), 185- 216, 2019. Disponível em: <https://doi.org/10.30899/dfj.v12i39.655>

MOLINARO, Carlos Alberto; SARLET, Gabrielle Bezerra Sales. Questões tecnológicas, éticas e normativas da proteção de dados pessoais na área da saúde em um contexto de big data. In: **Direitos Fundamentais & Justiça**, a. 13, n. 41, p. 183-212, jul./dez. 2019.

MONTEIRO, Renato Leite. **Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?** Instituto Igarapé, artigo estratégico 39, dez/2018. Disponível em < https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf>.

MULHOLLAND, Caitlin. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, Vitória, v. 19, n. 3, set./dez. 2018, p. 159-180.

O'BRIEN, James A.; MARAKAS, George M. **Administração de sistemas de informação**. 15.ed. Porto Alegre: AMGH, 2013.

OLIVERA, Marco Aurélio Bellizze; LOPES, Maria Pereira. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro** / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva coordenação - 1. ed. – São Paulo: Thomson Reuters Brasil, 2019.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **Recomendação do conselho da ocde sobre integridade pública**. Disponível em: <https://www.oecd.org/gov/ethics/integrity-recommendation-brazilian-portuguese.pdf>.

ORWELL, George. **1984** (Nineteen eighty-four). Tradução: Wilson Velloso – 29. ed. – São Paulo: Companhia Editora Nacional, 2005.

PARISER, Eli. **O filtro invisível.** O que a Internet está escondendo de você. Trad. Diego Alfaro. Rio de Janeiro: Zahar, 2012. p.41.

PEREIRA, Marcelo Cardoso. **Direito à intimidade na internet**. 1. ed. 6. reimp. - Curitiba: Juruá, 2011.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais**: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

RIBEIRO, Leila Beatriz. Fahrenheit 451: sobre homens-livro e bombeiros incendiários, a oposição informação imagética x escrita. **Revista Morpheus-Estudos Interdisciplinares em Memória Social**, v. 6, n. 11, 2007. Disponível em <http://seer.unirio.br/morpheus/article/view/4796/4286>.

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

RONDON, Thiago. Não precisamos da sua geolocalização para conter a propagação da covid-19: Tecnologia Bluetooth permite alertar pessoas sobre contato com alguém infectado sem violar a privacidade dos envolvidos. **Época Negócios**, em 14 de Abril de 2020. Disponível em: <https://epocanegocios.globo.com/colunas/Multidoes/noticia/2020/04/nao-precisamos-da-suageolocalizacao-para-conter-propagacao-da-covid-19.html>.

ROPER CENTER. Princeton Survey Research Associates. **Civil Liberties and Terrorism.** 21 de setembro, 2001. Disponível em: <http://ropercenter.cornell.edu/CFIDE/cf/action/catalog/abstract.cfm?type=&start=&id=&archno=USPSRA2001-NW11&abstract=>. Acesso em: 23 jun. 2021.

ROPER CENTER. Los Angeles Times. **Terrorist Attacks in New York City and Washington.** 13-14 de setembro, 2001. Disponível em: <http://ropercenter.cornell.edu/CFIDE/cf/action/catalog/abstract.cfm?type=&start=&id=&archno=USPSRA2001-NW11&abstract=>. Acesso em: 23 jun. 2021.

ROSENAU, James N. “Governança, Ordem e Transformação na Política Mundial”. In: Rosenau, James N. e Czempiel, Ernst-Otto. **Governança sem governo**: ordem e transformação na política mundial. Brasília: Ed. Unb e São Paulo: Imprensa Oficial do Estado, 2000. p. 11-46

SCURO NETO, Pedro. **Sociologia Geral e Jurídica**, 7. ed. São Paulo: Saraiva, 2010.
SILVA, Jorge Bastos da; VIEIRA, Fátima. **George Orwell**: perspectivas contemporâneas. Faculdade de Letras da Universidade do Porto, 2005.

SOUSA, Rosilene Paiva Marinho de; BARRANCOS, Jacqueline Echeverría; MAIA, Manuela Eugênio. Acesso à informação e ao tratamento de dados pessoais pelo Poder Público. **Informação & Sociedade**, v. 29, n. 1, 2019. Disponível em: <https://media.proquest.com/media/hms/PFT/1/srgz8?_s=Wko1xNvBpYHLCsom%2FsHxWFm3kBc%3D>

TORRES, Frederico Boghossian; AZEVEDO; Raphaela. **STF e o reconhecimento da existência do direito fundamental à proteção de dados**. Clínica de Direitos Fundamentais da Faculdade De Direito da UERJ – Rio de Janeiro – RJ – Brasil, 2020. Disponível em <http://uerjdireitos.com.br/stf-e-o-reconhecimento-da-existencia-do-direito-fundamental-a-protecao-de-dados/#_ftn1>.

VEIGA, Luiz Adolfo Olsen da; ROVER, Aires J. Dados e informações na internet: é legítimo o uso de robôs para a formação de base de dados de clientes? In: ROVER, Aires José (Org.). **Direito e informática**. São Paulo: Monole, 2004, p. 27-40. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/luizvaires-livro_aires.pdf>.

VIANNA, Túlio Lima. **Transparência Pública, Opacidade Privada**: O Direito Como Instrumento de Limitação do Poder na Sociedade de Controle. Rio de Janeiro: Revan, 2007.

WORLD BANK. ***Governance and Development***. Washington: The World Bank, 1992. Disponível em: <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/604951468739447676/governance-and-development>.

ZANINI, Leonardo Estevam de Assis. O Surgimento e o desenvolvimento do *Right of Privacy* nos Estados Unidos. **Revista Brasileira de Direito Civil**, Belo Horizonte, v. 3, n. 1. p.8-27, mar. 2015. p. 11. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/107>.