PONTIFÍCIA UNIVERSIDADE CATÓLICA DO PARANÁ
ESCOLA DE DIREITO
MESTRADO EM DIREITO

GIOVANA BATISTI VIEIRA

O CADASTRO BASE DO CIDADÃO COMO TECNOPOLÍTICA À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

CURITIBA
2022

GIOVANA BATISTI VIEIRA

O CADASTRO BASE DO CIDADÃO COMO TECNOPOLÍTICA À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica do Paraná como requisito parcial à obtenção do título de Mestre.

Área de Concentração: Direito Socioambiental e Sustentabilidade.

Linha de Pesquisa: Estado, Sociedades, Povos e Meio Ambiente.

Orientadora: Profa. Dra. Cinthia Obladen de Almendra Freitas.

CURITIBA

2022

Dados da Catalogação na Publicação
Pontifícia Universidade Católica do Paraná
Sistema Integrado de Bibliotecas – SIBI/PUCPR
Biblioteca Central
Sônia Maria Magalhães da Silva – CRB 9/1191

Vieira, Giovana Batisti
V658c 2022 O cadastro base do cidadão como tecnopolítica à luz da Lei Geral de Proteção de Dados Pessoais / Giovana Batisti Vieira ; orientadora: Cinthia Obladen de Almendra Freitas. – 2022.
158 f. ; 30 cm

Dissertação (mestrado) – Pontifícia Universidade Católica do Paraná, Curitiba, 2022
Bibliografia: 149-158

1. Brasil. Lei Geral de Proteção de Dados Pessoais (2018). 2. Cidadão. I. Freitas, Cinthia Obladen de Almendra. II. Pontifícia Universidade Católica do Paraná. Programa de Pós-Graduação em Direito. III. Título.

Dóris 3. ed. – 340

AGRADECIMENTOS

Aos meus pais, Inês Batisti Dantas Vieira e Geraldo Edson Dantas Vieira, por todo o apoio, carinho e ensinamentos. Obrigada por sempre me incentivarem a ir em frente, segurarem a minha mão durante os obstáculos que surgiram pelo caminho e comemorarem minhas vitórias.

Ao meu irmão, Gabriel Batisti Vieira, por estar sempre ao meu lado e me animar nas horas difíceis.

Ao Emanuel Augusto de Castro, companheiro, amor e amigo, por me ouvir, me incentivar e me apoiar durante essa trajetória.

À Profa. Dra. Cinthia Obladen de Almendra Freitas, por acreditar na minha capacidade e pela dedicação incansável na orientação prestada durante o Mestrado. Obrigada pelos ensinamentos, pelas críticas construtivas e pelo esforço para meu desenvolvimento como pesquisadora.

Às minhas amigas, Juliane Tedesco Andretta e Amanda de Meirelles Belliard e às minhas primas Isabelle Batisti Riato Navarro e Talita Vieira Volpato, por estarem sempre ao meu lado, ouvindo meus desabafos, me consolando e me dando ânimo para continuar.

Aos meus amigos e companheiros de Mestrado e Doutorado da PUCPR, em especial à Ana Carolina Fontana de Mattos e Nicolas Addor, pelo companheirismo tanto na vida pessoal, quanto acadêmica.

À Pontifícia Universidade Católica do Paraná (PUCPR), à Escola de Direito e a todos os professores e demais funcionários que fazem seu funcionamento possível, por me acolherem há 7 anos (desde a graduação), me formando não só como profissional e acadêmica, mas como uma pessoa melhor. Ainda, agradeço ao Programa de Pós-graduação em Direito (PPGD) da Escola de Direito da PUCPR e à equipe responsável, pela formação e experiência proporcionadas durante esses dois anos, as quais me tornaram uma pesquisadora.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES).

“O amor à servidão não pode ser instituído senão como fruto de uma profunda revolução pessoal nas mentes e nos corpos humanos”

(HUXLEY, 2014, p. 16)

“O novo objetivo do poder não consiste na administração do passado, mas no controle psicopolítico do futuro”

(HAN, 2018, p. 56)

RESUMO

A vigilância é hoje líquida, distribuída e ubíqua e, embora seja por vezes necessária, pode apresentar riscos significativos à diversos direitos fundamentais e até mesmo à democracia. Diante desse contexto, questiona-se se a Lei Geral de Proteção de Dados Pessoais é capaz de mitigar os riscos apresentados pelo Cadastro Base do Cidadão, tecnopolítica de vigilância implementada no Brasil. A hipótese de pesquisa consiste em uma resposta negativa ao questionamento apresentado, isto é, na insuficiência do ordenamento jurídico brasileiro – leia-se a ineficácia da LGPD em conjunto com a Constituição Federal de 1988 -, em frear e/ou mitigar os riscos aos direitos à proteção de dados pessoas e à privacidade derivados da Cadastro Base do Cidadão. Assim, determinou-se como objetivo geral da pesquisa analisar o Cadastro Base do Cidadão (CBC), uma tecnopolítica de vigilância atualmente implementada no Brasil, e sua adequação à Lei Geral de Proteção de Dados Pessoais, no intuito de avaliar se a lei é capaz frear e mitigar os riscos apresentados pela implementação do Cadastro. O objetivo geral se subdivide em três objetivos específicos, quais sejam: i) estabelecer o contexto do tema por meio da análise da teoria da psicopolítica neoliberal de Byung-Chul Han, evidenciando seus riscos para a sociedade; ii) analisar a Lei Geral de Proteção de Dados Pessoais (LGPD) e seus alcances no que diz respeito ao tema, verificando sua capacidade para proteção dos direitos à proteção de dados pessoais e à privacidade contra os riscos criados pelas tecnopolíticas; iii) analisar o Cadastro Base do Cidadão como uma tecnopolítica de vigilância com o intuito de verificar quais os riscos aos direitos à proteção de dados pessoais e à privacidade são criados por esse sistema. O método de pesquisa foi o hipotético-dedutivo, com técnica bibliográfica e documental. Partindo da problemática determinada e tendo como marco teórico as teorias de Byung-Chul Han sobre a Psicopolítica Neoliberal, o panóptico digital e a Sociedade de Controle, a pesquisa se desenvolveu primeiramente travando uma discussão sobre a vigilância como instrumento de poder, sobre o conceito de vigilância, suas características e peculiaridades, bem como sobre a forma como ela se configura na sociedade contemporânea. Em seguida, realizou-se um delineamento dos balizadores legais e principiológicos que devem reger a implementação de um sistema de vigilância, os quais são garantidos pela LGPD. E, por fim, considerando o embasamento teórico-científico, realizou-se a análise do Cadastro Base do Cidadão. Conclui-se que a Lei Geral de Proteção de Dados Pessoais é perfeitamente capaz de mitigar os riscos mais prementes de uma tecnopolítica de vigilância, não obstante, o problema é de outra ordem, já que os sistemas e práticas vigilantistas implementados no Brasil são feitos, muitas vezes, às margens da lei e da justiça, como demonstrado durante a análise do Cadastro Base do Cidadão.

Palavras-chave: Sociedade de Controle. Novas tecnologias. Lei Geral de Proteção de Dados Pessoais. Tecnopolíticas de Vigilância. Cadastro Base do Cidadão.

ABSTRACT

Surveillance is now liquid, distributed and ubiquitous and, although it is sometimes necessary, it can pose significant risks to various fundamental rights and even to democracy. In this context, the question is whether the General Law on the Protection of Personal Data is able to mitigate the risks presented by the Citizen's Base Register, a surveillance technopolitics implemented in Brazil. The research hypothesis consists of a negative answer to the question presented, that is, the insufficiency of the Brazilian legal system - read the ineffectiveness of the LGPD in conjunction with the Federal Constitution of 1988 -, to curb and/or mitigate the risks to the rights to data protection and privacy derived from the Citizen's Base Register. Thus, it was determined as a general research objective to analyze the Citizen's Base Register (CBC), a surveillance technopolitics currently implemented in Brazil, and its adequacy to the General Law on Personal Data Protection, in order to assess whether the law is able to curb and mitigate the risks presented by the implementation of the Register. The general objective is subdivided into three specific objectives, namely: i) establish the context of the theme through the analysis of Byung-Chul Han's theory of neoliberal psychopolitics, highlighting its risks to society; ii) analyze the General Law of Personal Data Protection (LGPD) and its scope with regard to the theme, verifying its ability to protect the rights to the protection of personal data and privacy against the risks created by technopolitics; iii) analyze the Citizen's Base Register as a technopolitics of surveillance in order to verify which risks to the rights to the protection of personal data and privacy are created by this system. The research method was hypothetical-deductive, with bibliographic and documental techniques. Starting from the determined problematic and having as theoretical framework the theories of Byung-Chul Han about the Neoliberal Psychopolitics, the digital panopticon and the Control Society, the research was developed firstly by discussing surveillance as an instrument of power, about the concept of surveillance, its characteristics and peculiarities, as well as how it is configured in contemporary society. Then, an outline of the legal and principles that should govern the implementation of a surveillance system, which are guaranteed by the LGPD was performed. And, finally, considering the theoretical and scientific basis, the analysis of the Citizen's Base Register was carried out. It is concluded that the General Law on Personal Data Protection is perfectly able to mitigate the most pressing risks of a technopolitics of surveillance, however, the problem is of another order, since the surveillance systems and practices implemented in Brazil are often made at the margins of law and justice, as demonstrated during the analysis of the Citizen's Base Register

Key-words: Control society**.** New Technologies. General Law on Personal Data Protection. Surveillance Technopolitics. Citizen's Base Register.

LISTA DE SIGLAS E ABREVIATURAS

ABIN – Agência brasileira de inteligência

ABI - Solução Automatizada de Identificação Biométrica

ADI - Ação Direta de Inconstitucionalidade

ADPF - Arguição de Descumprimento de Preceito Fundamental

AEB - Agência Espacial Brasileira

AGU - Advocacia-Geral da União

ANCINE - Agência Nacional de Cinema

ANEEL - Agência Nacional de Energia Elétrica

ANM - Agência Nacional de Mineração

ANPD - Autoridade Nacional de Proteção de Dados

ANS - Agência Nacional de Saúde Suplementar

ANTAQ - Agência Nacional de Transportes Aquaviários

ANTT - Agência Nacional de Transportes Terrestres

ANVISA - Agência Nacional de Vigilância Sanitária

CADE - Conselho Administrativo de Defesa Econômica

CAPES - Coordenação de Aperfeiçoamento de Pessoal de Nível Superior

CBC – Cadastro Base do Cidadão

CCTV - *Closed-circuit television*

CEX - Comando do Exército

CF – Constituição Federal de 1988

CFOAB – Conselho Federal da Ordem dos Advogados do Brasil

CFTV - Câmeras de Circuito Fechado de Televisão

CGU - Controladoria-Geral da Uniã

CNAE – Classificação Nacional de Atividades Econômicas

CNH – Carteira Nacional de Habilitação

CNPJ – Cadastro Nacional de Pessoas Jurídicas

CNPQ - Conselho Nacional de Desenvolvimento Científico e Tecnológico

CPF – Cadastro de Pessoas Físicas

DATASUS - Departamento de informática do Sistema Único de Saúde do Brasil

DENATRAN - Departamento Nacional de Trânsito

DINT/SEOPI - Diretoria de Inteligência da Secretaria de Operações Integradas

DNIT - Departamento Nacional de Infraestrutura de Transportes

ENAP - Escola Nacional de Administração Pública

FIOCRUZ – Fundação Oswaldo Cruz

FNDE - Fundo Nacional de Desenvolvimento da Educação

GDPR - *General Data Protection Regulation*

GSI - Gabinete de Segurança Institucional

IBAMA - Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis

IBGE - Instituto Brasileiro de Geografia e Estatística

ICMBio - Instituto Chico Mendes de Conservação da Biodiversidade

IFAM - Instituto Federal de Educação, Ciência e Tecnologia do Amazonas

IFG - Instituto Federal de Educação, Ciência e Tecnologia Goiano

IFRN - Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte

IFRO - Instituto Federal de Educação, Ciência e Tecnologia de Rondônia

IFRS - Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul

IFSC - Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina

IFSP - Instituto Federal de Educação, Ciência e Tecnologia de São Paulo

IFSul - Instituto Federal de Educação, Ciência e Tecnologia Sul Rio-Grandense

INCRA - Instituto Nacional de Colonização e Reforma Agrária

INEP - Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira

INMETRO - Instituto Nacional de Metrologia, Qualidade e Tecnologia

INPI - Instituto Nacional da Propriedade Industrial

ITI - Instituto Nacional de Tecnologia da Informação

LGBTQIA+ -

LGPD – Lei Geral de Proteção de Dados Pessoais (Lei n 13.709/2018)

MAPA - Ministério da Agricultura, Pecuária e Abastecimento

MC - Ministério da Cidadania

MCTIC - Ministério da Ciência, Tecnologia, Inovações e Comunicações

MD - Ministério da Defesa

MDR - Ministério do Desenvolvimento Regional

ME - Ministério da Economia

MEC - Ministério da Educação

ME/SEGES - Secretaria de Gestão do Ministério da Economia

MINFRA - Ministério da Infraestrutura

MJSP - Ministério da Justiça e Segurança Pública

MMFDH - Ministério da Mulher, da Família e dos Direitos Humanos

MS - Ministério da Saúde

MTUR - Ministério do Turismo

NIS - Número de Identificação Social

OCDE - Organização para a Cooperação e Desenvolvimento Econômico

OCR - *Optical Character Recognition*

PASEP – Programa de Formação de Patrimônio do Servidor Público

PEC - Proposta de Emenda à Constituição

PGFN - Procuradoria-Geral da Fazenda Nacional

PIS – Programa de Integração Social

PREVIC - Superintendência Nacional de Previdência Complementar

PRF - Polícia Rodoviária Federal

PSB – Partido Socialista Brasileiro

RAIS – Relação Anual de Informações Sociais

SAFARI - *Système Automatisé pour les Fichiers Administratifs et le Rèpertoire des Individus*

SEOPI - Secretaria de Operações Integradas

SGD/DEOPC - Departamento de Operações Compartilhadas da Secretaria do Governo Digital

SGD/DESPD - Departamento de Serviços Públicos Digitais da Secretaria do Governo Digital

SGD/ME - Secretaria de Governo Digital do Ministério da Economia

SINESP - Sistema Nacional de Informações de Segurança Pública

SINIVEM - Sistema Integrado Nacional de Identificação de Veículos em Movimento

STF – Supremo Tribunal Federal

STN - Secretaria do Tesouro Nacional

SUDAM - Superintendência do Desenvolvimento da Amazônia

SUFRAMA - Superintendência da Zona Franca de Manaus

SUSEP - Superintendência de Seguros Privados

TIC – Tecnologia de Informação e Comunicação

UFLA - Universidade Federal de Lavras

UFPR - Universidade Federal do Paraná

UFSC - Universidade Federal de Santa Catarina

UFU - Universidade Federal de Uberlândia

SUMÁRIO

1 INTRODUÇÃO

A proliferação de dispositivos móveis de comunicação, plataformas digitais de compartilhamento de conteúdo, a multiplicação de objetos conectados à Internet que fazem parte da vida cotidiana de grande parte da população mundial e a expansão da videovigilância em grandes centros urbanos; tudo isso vem transformando gradualmente o modo de vida em sociedade, produzindo mudanças de ordem estética, social, política, ambiental e cultural. Ao mesmo tempo em que a comunicação e a liberdade de expressão são potencializadas nos meios digitais, os dispositivos de monitoramento tornam-se cada vez mais presentes no dia a dia de todos. Toda ação cotidiana torna-se sujeita à coleta, registro, monitoramento e classificação.

O mundo vive, atualmente, sob constante vigilância, a qual pode ser exercida de diversas formas, para muitas finalidades e em muitas esferas diferentes – policiamento, administração pública, comercial, militar, entre outras -, esferas essas que podem coexistir e, até mesmo, se inter-relacionar. Independentement da finalidade exata para a qual é exercida, no entanto, a prática de vigiar sempre busca a obtenção de um conhecimento sobre o vigiado, o qual será posteriormente utilizado para a construção de relação de dominação ou para a manutenção de poder já existente, para a manutenção da ordem social, a racionalização e a classificação de indivíduos, objetos ou fatos.

A vigilância aparece como parte da política econômica do capitalismo (Marx), como produto da organização burocrática (Weber) e como ferramenta para imposição da autodisciplina (Foucault). A busca pela racionalização e a classificação torna-se cada vez mais forte a partir da modernidade e, combinada com a cultura do individualismo pós-moderno e os conflitos globais, a ordem produzida pela vigilância é bem recebida em todas as áreas da vida em sociedade. Em conjunto com o desenvolvimento tecnológico, é que o exercício da vigilância se torna distribuído, líquido e ubíquo nas sociedades contemporâneas, tido como necessário e, portanto, um fato imutável.

É por meio dessa vigilância que se consuma o psicopoder na Sociedade de Controle, conforme descrito por Byung-Chul Han, dentro da qual a liberdade e a comunicação transformam-se em monitoramento e controle, pois tudo que pertence às práticas de liberdade é explorado pelo psicopoder, que possui a capacidade de intervir nos processos psicológicos, modulando-os. A vigilância, especialmente aquela realizada por meio da coleta e tratamento de dados pessoais, é o que dá suporte ao psicopoder, produzindo as informações e o conhecimento necessário para o exercício do controle e da modulação. É por meio do tratamento de grandes quantidades de dados (incluindo-se os dados pessoais) que se pode obter informações e,

portanto, conhecimento, sobre as dinâmicas e comportamentos sociais, tornando quantificáveis, mensuráveis e controláveis os sujeitos vigiados. Assim, a vigilância distribuída é característica da sociedade contemporânea, sendo ela um instrumento para controle e administração da sociedade, necessária para a manutenção da ordem e da organização social.

A vigilância, portanto, apesar de assumir um caráter negativo em variados contextos, é necessária, inclusive para garantir o correto funcionamento do Estado e a correta distribuição de direitos e garantias fundamentais aos cidadãos. Os Estados necessitam de informações detalhadas sobre os cidadãos e sobre o funcionamento da sociedade para fins de discriminação entre quem possui ou não determinado direito ou benefício, quem deve pagar determinado imposto, bem como quais políticas públicas são necessárias. A vigilância se faz necessária também para fins de segurança pública e nacional, comercial, para fins estatísticos e assim por diante. Portanto, não é uma prática exclusiva de Estados totalitários, mas está presente, também, em países institucionalmente democráticos. Em suma, o exercício da vigilância é um aspecto inevitável da sociedade do Século XXI. No entanto, a vigilância nunca é neutra, e quando exercida de forma massiva e distribuída torna-se, por sua própria natureza, invasiva, podendo, dessa forma, vir a ameaçar direitos e liberdades fundamentais. Diversos elementos dessa vigilância são considerados preocupantes do ponto de vista democrático, como a objetificação e o controle de indivíduos de uma forma que perpetua desigualdades sociais; a falta de transparência de muitos sistemas e práticas; a falta de consciência dos indivíduos vigiados sobre o monitoramento que está ocorrendo; a falta de participação social em decisões sobre esses processos, entre outros. Justamente por apresentar esses aspectos, toda vigilância requer uma avaliação cuidadosa.

A despeito dos inúmeros riscos apresentados pelo exercício massificado da vigilância, o que se tem hoje é a construção de um conglomerado cada vez maior de dispositivos tecnopolíticos de vigilância operadas pelos Estados, em conjunto com corporações. Por dispositivos tecnopolíticos leia-se um conjunto de políticas, técnicas, sistemas e práticas de monitoramento e controle, mediados por Tecnologias de Informação e Comunicação (TIC), que realizam a coleta, processamento e análise de dados com a finalidade de controle e regulação das relações humanas. Essas tecnopolíticas rearranjam as relações de poder, influenciando diretamente nas vidas dos cidadãos, consumando a Sociedade de Controle descrita por Byung-Chul Han. Diante desse cenário, os estudos sobre a vigilância levantam inúmeras questões sobre privacidade, proteção de dados pessoais, direitos e liberdades fundamentais, e democracia, no sentido de buscar compreender como as práticas de vigilância podem ser limitadas de forma que não venham a representar riscos reais aos cidadãos.

Um exemplo muito real desse debate é o que acontece em relação ao Cadastro Base do Cidadão (CBC), uma tecnopolítica de vigilância brasileira, consistente em uma base de dados centralizada criada para reunir ao longo do tempo dados pessoais de cidadãos brasileiros que estão em posse de órgãos estatais. O CBC foi criado em 2019, por meio da publicação do Decreto 10.046/2019, sem qualquer consulta pública ou participação da sociedade ou de partes interessadas em seu desenvolvimento, e, desde então, vem causando acaloradas discussões tanto no âmbito acadêmico quanto no âmbito jurídico, sendo objeto de Ação Direta de Inconstitucionalidade nº 6.649.

Diante do problema apresentado, é evidenciada a necessidade de regulação do uso dessas tecnologias com potencialidade para a vigilância e consequente classificação social e automatização de discriminações em espaços de poder e controle – como é o caso desses sistemas criados pelo Estado. A diversidade de riscos de violação de direitos advindos de processos de vigilância e automatização de tomadas de decisão pelo Estado somada à falta de conhecimento dos cidadãos a respeito desses processos tecnopolíticos de vigilância, bem como a respeito das complexas facetas da tecnologia em si, evidenciam a relevância da investigação e pesquisa aqui propostas.

Diante desse contexto, questiona-se se a Lei Geral de Proteção de Dados Pessoais (LGPD - Lei n 13.709/2018), em conjunto com a Constituição Federal de 1988, é eficiente em mitigar os riscos apresentados pelo Cadastro Base do Cidadão, tecnopolítica de vigilância implementada no Brasil, sendo esse o problema de pesquisa. A hipótese de pesquisa consiste em uma resposta negativa ao questionamento apresentado, isto é, na insuficiência do ordenamento jurídico brasileiro – leia-se a ineficácia da LGPD em conjunto com a Constituição Federal de 1988 -, em frear e/ou mitigar os riscos aos direitos à proteção de dados pessoas e à privacidade derivados da Cadastro Base do Cidadão.

Desse modo, o objetivo geral da pesquisa consistiu em analisar o Cadastro Base do Cidadão (CBC), uma tecnopolítica de vigilância atualmente implementada no Brasil, e sua adequação à Lei Geral de Proteção de Dados Pessoais, no intuito de avaliar se a lei é capaz frear e mitigar os riscos apresentados pela implementação do Cadastro. Esse subdivide-se, ainda, em três objetivos específicos: i) estabelecer o contexto do tema por meio da análise da teoria da psicopolítica neoliberal de Byung-Chul Han, evidenciando seus riscos para a sociedade; ii) analisar a Lei Geral de Proteção de Dados Pessoais (LGPD) e seus alcances no que diz respeito ao tema, verificando sua capacidade para proteção dos direitos à proteção de dados pessoais e à privacidade contra os riscos criados pelas tecnopolíticas; iii) analisar o Cadastro Base do

Cidadão como uma tecnopolítica de vigilância com o intuito de verificar quais os riscos aos direitos à proteção de dados pessoais e à privacidade são criados por esse sistema.

A pesquisa se enquadra no viés social da Área de Concentração "Direito Socioambiental e Sustentabilidade" do Programa de Pós-Graduação em Direito da PUCPR, refletindo o estudo da proteção de bens e direitos sociais por meio do Direito, buscando promover a sustentabilidade social, isto é, a redução das desigualdades sociais e a promoção de valores como equidade e justiça social. Ao buscar estudar como o Direito – no presente caso, por meio da LGPD -, pode proteger os direitos de coletividades, especialmente de minorias sociais, frente aos riscos advindos das tecnopolíticas da vigilância, a presente pesquisa volta-se ao estudo do Direito Socioambiental, especialmente as interfaces do direito com o ser humano, a tecnologia, as condições para o exercício democrático do direito, o Estado, grupos sociais vulneráveis e a Sociedade de Controle. Portanto, a pesquisa volta-se ao estudo dos direitos fundamentais, tecnologia e democracia dentro do contexto de implementação de tecnopolíticas de vigilância por parte do Estado no Brasil e, nesse sentido, enquadra-se na Linha de Pesquisa "Estado, Sociedades, Povos e Meio Ambiente" da Área de Concentração mencionada, na medida em que busca investigar a relação do Estado e do Direito na promoção da dignidade, liberdade, justiça e democracia na complexa Sociedade de Controle, analisando as perspectivas e soluções jurídicas face aos riscos que os sistemas sociotécnicos vigilantistas apresentam dentro dessa sociedade. Nesse sentido, desenvolveu-se a pesquisa dentro do tema Novas Tecnologias, Vigilância e Sociedade de Controle.

A metodologia utilizada para o desenvolvimento da pesquisa consistiu no método hipotético-dedutivo, que pressupõe o conhecimento prévio da teoria e do problema existente e busca o delineamento de uma hipótese, a qual será testada durante a pesquisa. A pesquisa tem técnica bibliográfica – consistente no marco teórico e outras bibliografias relevantes para o tema - e documental – consistente nos documentos legislativos brasileiros -, com objetivos exploratórios e descritivos. Ressalta-se que o marco teórico da pesquisa diz respeito à teoria da Psicopolítica Neoliberal e do Panóptico Digital de Byung-Chul Han, da qual partiu o tema de pesquisa, uma vez que a complexa rede de processos sociotécnicos que dá origem às tecnopolíticas de vigilância, objeto da pesquisa, são parte essencial na consolidação da Sociedade de Controle descrita por Han.

Com o desenvolvimento da pesquisa, espera-se desenvolver uma base teórica para o âmbito acadêmico e jurídico, para que se passe a questionar mais abertamente o papel do Direito na proteção dos direitos fundamentais dos cidadãos contra os abusos advindos das tecnopolíticas de vigilância implementadas pelo Estado, bem como para que se passe a

investigar mais profundamente em que medida esses sistemas vigilantistas realmente são necessários e benéficos para a sociedade, em busca de estabelecer certo equilíbrio entre seus benefícios e seus riscos, para que o cidadão não tenha seus direitos fundamentais prejudicados em prol da vigilância.

A dissertação divide-se em três capítulos. No primeiro capítulo delineia-se o desenvolvimento das Sociedades de Soberania, Disciplinar, Biopolítica e de Controle Neoliberal, dentro das quais a vigilância é sempre utilizada como um instrumento para manutenção do poder. Ainda, realiza-se breve análise da literatura sobre o tema em busca de definir um conceito de vigilância; descreve-se as tecnopolíticas de vigilância na sociedade de controle – isto é, na sociedade contemporânea -, elencando suas peculiaridades e características com base, principalmente, na obra de Byung-Chul Han; e, por fim, são discutidos riscos das tecnopolíticas de vigilância para os direitos à proteção de dados pessoais, à privacidade e direitos à liberdade derivados dos dois primeiros, no contexto da sociedade contemporânea.

No segundo capítulo são delineadas as questões necessárias para a análise da legitimidade de uma tecnopolítica de vigilância dentro do ordenamento jurídico brasileiro, para que posteriormente possa ser realizada a análise do Cadastro Base do Cidadão. Aqui realizou-se uma escolha metodológica no sentido de delimitar a discussão aos direitos à proteção de dados pessoais e à privacidade, uma vez que são os dois direitos que são violados de forma mais direta e evidente pelos sistemas de vigilância e que, quando protegidos, podem evitar a violação de outros direitos e liberdades fundamentais. Assim, na primeira e na segunda seções discorre-se sobre a garantia do direito fundamental à privacidade e a garantia da proteção de dados pessoais, respectivamente, e sua importância face ao exercício da vigilância. Na terceira seção discorre-se sobre a necessidade de realização de análise de proporcionalidade entre os direitos do indivíduo que está sob vigilância e a finalidade dessa. E, por fim, na última seção discorre-se sobre a necessidade de análise contextual da aplicação de uma tecnopolítica de vigilância.

Por fim, no terceiro e último capítulo é realizada a análise do Cadastro Base do Cidadão. A escolha pela realização da análise do Cadastro Base do Cidadão se deu tendo em vista que os riscos advindos da centralização de todos os dados dos cidadãos brasileiros coletados por órgãos do poder público para serem utilizados para finalidades diversas daquelas inicialmente propostas e sem o conhecimento dos titulares é significativo, permitindo acesso mais amplo e intrusivo aos dados pessoais dos cidadãos a grande parte dos órgãos públicos e construindo um aparato de vigilância massiva e totalizante, sendo esse, portanto, uma das tecnopolíticas

potencialmente mais perigosas já implementadas no Brasil, conforme restará demonstrado durante o desenvolvimento da pesquisa.

Assim, no primeiro subtópico analisa-se o Decreto 10.046/2019 que cria o Cadastro Base do Cidadão para explicar seu funcionamento. No segundo, analisa-se o contexto de implementação do CBC tendo em vista o interesse vigilantista do atual governo, citando exemplos de tecnopolíticas de vigilância já implementados, bem como tentativas de compartilhamento de dados entre entes públicos. No terceiro elucida-se como e por que o CBC pode ser entendido como um sistema de vigilância com base na discussão teórica desenvolvida no primeiro capítulo. No quarto, é realizado uma análise da (in)adequação do Decreto e do Cadastro em relação à Lei Geral de Proteção de Dados Pessoais (LGPD), com base na discussão desenvolvida no capítulo anterior. E, por fim, no quinto e último subtópico elenca-se os riscos de violação aos direitos à proteção de dados pessoas, à privacidade e às liberdades derivadas dos dois primeiros direitos, advindos da implementação do CBC.

2 TECNOPOLÍTICAS DE VIGILÂNCIA E A SOCIEDADE DE CONTROLE

Inicialmente, ressalta-se que, ainda que a vigilância estatal contemporânea não possa ser plenamente compreendida se for dissociada da vigilância comercial privada, como dois exercícios totalmente distintos, tendo em vista que elas usam as mesmas tecnologias e operam por meio de parcerias[1], o foco principal do presente estudo está direcionado à vigilância exercida por setores públicos, na medida em que governos possuem maior capacidade para contornar muitas restrições legais em relação à vigilância em nome da segurança e administração pública, por exemplo, por meio das chamadas "tecnopolíticas de vigilância".

O significado do termo tecnopolítica pode variar de acordo com o contexto, mas, de forma geral, refere-se às dinâmicas que envolvem o desenvolvimento tecnológico e as práticas políticas, isto é, refere-se às práticas de projetar ou utilizar a tecnologia para constituir, incorporar ou cumprir objetivos ou finalidades políticas.[2] Nesse sentido, pode-se definir "tecnopolíticas de vigilância" como o conjunto de técnicas e dispositivos de controle e vigilância exercidos – e moldados - por meio de tecnologias, especialmente as Tecnologias de Informação e Comunicação (TICs).

A ideia de vigilância implica que o observador está em uma posição de dominância em relação ao observado. Atualmente, processos de vigilância são realizados por Estados, pelo setor privado e, por vezes, por indivíduos em suas relações interpessoais[3], dando origem ao que David Lyon denomina de Cultura da Vigilância.[4] Desse modo, seja a vigilância exercida por agências de inteligência para a segurança nacional ou por corporações, comerciantes, empregadores ou pais - para exercício de controle parental[5] -, o relacionamento em que essa vigilância se dá possui uma relação de poder entre o observador – o qual terá o instrumento para proteger e controlar - e o observado.

Portanto, independente do contexto em que está inserida, a vigilância foi e ainda é tanto uma expressão, quanto um instrumento de poder, utilizado para organizar, controlar e proteger

---

[1] RICHARDS, Neil M. The danger of surveillance. In: **Harvard Law Review**, v. 126, 2013. p. 1934-1965. p. 1958-1959.

[2] HECHT, Gabrielle. Technology, politics, and national identity in France. In: ALLEN, Michael Thad; HECHT, Gabrielle (Ed). **Technologies of Power**: Essays in honor of Thomas Parke Hughes and Agatha Chipley Hughes. Cambridge/London: The MIT Press, 2011. p. 253-293. p. 256-257.

[3] MARX, Gary T. Surveillance Studies. In: **International Encyclopedia of the Social & Behavioral Sciences**, 2nd ed., v. 23. Oxford: Elsevier, 2015. p. 733-741. P. 733.

[4] LYON, David. **The Culture of Surveillance**: Watching as a Way of Life. Cambridge: Polity, 2018. p. 15.

[5] Ressalta-se que o exercício de controle parental por meio de programas de computador é permitido pelo artigo 29 do Marco Civil da Internet (Lei nº 12.965/2014), desde que respeitados os princípios do próprio Marco Civil da Internet e do Estatuto da Criança e do Adolescente (Lei nº 8.069/1990).

populações.[6] Isso significa que a vigilância pode ser experimentada pelos observados tanto positiva quando negativamente. As finalidades e os meios da vigilância, bem como a forma como ela é experimentada e entendida pelos seus receptores, são influenciados pela forma como o poder se manifesta no contexto da vigilância e, de forma geral, pelo contexto social, político e econômico. Isso porque a vigilância em si não é inerentemente boa ou ruim, sendo sempre imbuída de certa ambiguidade, isto é, o contexto em que está inserida e suas finalidades que a imbuem de um valor ou outro.[7]

Conforme observado por Lyon, as questões sobre quem está observando, quem e quais são as consequências dessa observação para o observado, ou para a sociedade em geral, não podem ser entendidas sem que se faça referência ao contexto específico em que essa vigilância ocorreu ou está ocorrendo.[8] A estrutura e os processos de vigilância sofreram mudanças ao longo da história, alterando, consequentemente, como este fenômeno era entendido em sua época. A vigilância sistêmica, pervasiva e ubíqua[9] que se conhece hoje advém de um processo histórico em que os processos da vigilância foram se alterando conforme grandes mudanças sociais, econômicas e políticas ocorriam nas sociedades, sendo que o fenômeno em sua forma atual foi influenciado pelo advento de indústrias, crescimento das cidades, advento do capitalismo, advento da democracia, bem como por organização militar.[10]

Desse modo, para os fins dessa pesquisa, fez-se necessário entender o termo vigilância, como as tecnopolíticas de vigilância são exercidas no contexto atual e quais os seus riscos para a democracia. Para isso, esse capítulo está divido em 4 partes: na primeira é feita uma breve e

---

[6] GILLIOM, John. Overseers of the poor: Surveillance, resistance, and the limits of privacy. In: MONAHAN, Torin; WOOD, David Murakami (Ed.). **Surveillance Studies**: a reader. New York: Oxford University Press, 2018. p. 230-233. p. 231

[7] MARX, Gary T. Surveillance Studies. In: **International Encyclopedia of the Social & Behavioral Sciences**, 2nd ed., v. 23. Oxford: Elsevier, 2015. p. 733-741. p. 733.

[8] LYON, David. **The Electronic Eye**: The rise of surveillance society. Cambridge: Polity, 1994 (Kindle Edition). p. 24

[9] O termo "pervasiva" refere-se a algo que se infiltra, se penetra, se espalha facilmente. Algo que é ubíquo e universal. Já "ubíquo" se refere à essa característica de universalidade, algo que é omnipresente, está ao mesmo tempo em toda parte. Ambos os termos são muito utilizados para descrever a omnipresença da tecnologia no cotidiano do ser-humano. Foi usado pela primeira vez por Mark Weiser, para o qual a computação ubíqua seria aquela que se integra na vida cotidiana de tal forma que se torna indistinguível, invisível para a consciência comum, tendo em vista que as pessoas os usarão a tecnologia inconscientemente para a realização de tarefas diárias. O termo refere-se, portanto, à tecnologia que é distribuída e integrada ao ambiente, está em toda parte, é universal e omnipresente. (WEISER, Mark. The computer for the 21st Century. In: **Scientific American**, sep. 1991). Essa característica da tecnologia na sociedade pós-moderna também pode ser descrita pelo "paradigma everyware" cunhado por Adam Greenfield. Referindo-se à um poder de processamento tão distribuído que se torna invisível. Para o autor, toda informação disponível por meio da Internet se torna acessível de qualquer lugar, a qualquer tempo, podendo ser acessada da maneira mais apropriada para a localização ou contexto (GREENFIELD, Adam. Everyware: The dawning age of ubiquitous computing. Berkeley: New Riders, 2006).

[10] LYON, David. **The Electronic Eye**: The rise of surveillance society. Cambridge: Polity, 1994 (Kindle Edition). p. 24

simplificada revisão histórica dos principais contextos em que a vigilância aparece como um instrumento de poder, utilizando-se, para isso, das obras de Foucault, Deleuze e Byung-Chul Han; na segunda parte, analisa-se literatura de vigilância em busca de uma definição para o fenômeno; na terceira parte, descreve-se as tecnopolíticas de vigilância na sociedade de controle – isto é, na sociedade contemporânea -, elencando suas peculiaridades e características com base, principalmente, na obra de Byung-Chul Han; e, por fim, na quarta e última parte são discutidos os riscos das tecnopolíticas de vigilância para a democracia de forma geral, e mais especificamente para os direitos à privacidade e à proteção de dados pessoais, no contexto da sociedade contemporânea.

2.1 SOCIEDADES E VIGILÂNCIA: DE MICHEL FOUCAULT (1926-1984) À BYUNG-CHUL HAN (1959)

Os estudos sobre a vigilância se intensificaram após os acontecimentos de 11 de setembro de 2001 em Nova Iorque nos Estados Unidos da América. Mas a questão já vinha sendo tema de estudo desde pelo menos 1950, devido a crescente preocupação com os abusos de direitos humanos cometidos pelo colonialismo, fascismo e processos anti-democráticos em geral no pós-guerra.[11] Muitos autores modernos ofereceram suas contribuições para o estudo da vigilância, incluindo Hobbes, Rousseau, Bentham, Marx, Nietzsche, Weber, Taylor e Foucault, sendo que este último pode ser considerado como o avô dos estudos contemporâneos sobre vigilância, que apesar de ter seu trabalho contextualizado temporalmente distante do Século XXI, pode-se considerar que seus entendimentos e conclusões sobre o panóptico e os poderes disciplinar e biopolítico ainda possuem profundas implicações nos estudos da vigilância pós-moderna.[12]

A figura do panóptico, uma prisão caracterizada pela total transparência de suas celas em relação ao olhar do vigia, é utilizada há anos para representar o poder de instituições em administrar populações. Esta prisão foi concebida por Jeremy Bentham, filósofo utilitarista, que se baseou no conceito original criado por seu irmão Samuel Bentham, engenheiro naval, que concebera um projeto de vigilância generalizada de portos e docas construídos para Catarina II

[11] MARX, Gary T. Surveillance Studies. In: **International Encyclopedia of the Social & Behavioral Sciences**, 2nd ed., v. 23. Oxford: Elsevier, 2015. p. 733-741. p. 734.
[12] MARX, Gary T. Surveillance Studies. In: **International Encyclopedia of the Social & Behavioral Sciences**, 2nd ed., v. 23. Oxford: Elsevier, 2015. p. 733-741. p. 734.

da Rússia; e foi popularizada pelas análises de Foucault, que representam um dos estudos mais importantes para o tema da vigilância até os dias atuais.[13] [14]

Conforme descrito por Bentham, o panóptico seria um prédio circular, em sua forma ideal, contendo uma torre central, com grandes janelas que se abrem para o interior dessa estrutura circular, de onde o inspetor teria a visão completa de todas as celas localizadas na periferia do prédio.[15] Cada cela possui duas janelas, uma para o interior e outra para o exterior, permitindo que a luz atravesse a cela, para que, com o efeito da contraluz, o inspetor possa observar as silhuetas dos internos em cada cela da periferia. Ainda, a estrutura do prédio permite que os internos tenham apenas uma visão axial, impedindo a visão lateral e, consequentemente, qualquer tipo de contato entre os internos.[16] A essência do panóptico consiste na posição central do inspetor, local em que pode ver sem ser visto. Nesse sentido, o inspetor assume a aparência de ser omnipresente, já que os internos do panóptico, por não terem comprovações absolutas da presença do inspetor em nenhum momento, sempre assumiriam que estariam sendo observados.[17]

Foucault considera o panóptico o "ponto de eclosão" do poder disciplinar, que vinha evoluindo desde seu desenvolvimento, por volta dos séculos XIV-XV, até sua penetração em larga escala na sociedade do século XVI e, especialmente, dos séculos XVII e XVIII. Segundo Foucault, essa evolução do poder disciplinar culmina com o desenvolvimento do Panóptico por Bentham em 1791, sendo este o momento em que o poder disciplinar passa a se tornar uma forma social generalizada, tendo em vista que o dispositivo de vigilância representado pelo panóptico é essencial para que a disciplina se mantenha.[18] A vigilância para Foucault, portanto, é um instrumento para a manutenção do poder, o qual, a partir do século XVII, passou a se manifestar mais concretamente por meio da disciplina, poder este, como já dito, denominado de poder disciplinar. Para explicar no que consistia essa manifestação de poder, Foucault o

---

[13] FOUCAULT, Michel. **A sociedade punitiva**: curso no Collège de France (1972-1973). Tradução de Ivone C. Benedetti. São Paulo: WMF Martins Fontes, 2015. p. 59-60.
[14] MONAHAN, Torin; WOOD, David Murakami (Ed.). **Surveillance Studies**: a reader. New York: Oxford University Press, 2018. p. 27-30.
[15] BENTHAM, Jeremy. The Panopticon. In: MONAHAN, Torin; WOOD, David Murakami (Ed.). **Surveillance Studies**: a reader. New York: Oxford University Press, 2018. p. 31-35.
[16] FOUCAULT, Michel. **Vigiar e Punir**: Nascimento da Prisão. Tradução de Pedro Elói Duarte. Lisboa: 70, 2013. p. 286.
[17] BENTHAM, Jeremy. The Panopticon. In: MONAHAN, Torin; WOOD, David Murakami (Ed.). **Surveillance Studies**: a reader. New York: Oxford University Press, 2018. p. 31-35.
[18] FOUCAULT, Michel. **O poder psiquiátrico**. Curso dado no Collège de France (1973-1974). Tradução de Eduardo Brandão. São Paulo: Martins Fontes, 2006. p. 51-52.

diferencia de um poder que o precedeu e que, por um longo tempo, se misturou com ele – o poder de soberania[19].

O poder de soberania é marcado pela assimetria na relação entre soberano e súdito, bem como por uma anterioridade, como um direito divino, uma vitória, um ato de submissão, por exemplo. Para que essa relação de soberania se mantivesse, fazia-se sempre necessário um suplemento de violência ou ameaça de violência,[20] pois "é na violência que a soberania faz valer seus direitos e vai impô-los à força a alguém que ela subjuga".[21] Desse modo, o direito de vida e morte – ou seja, o direito de causar a morte ou deixar viver –, foi, por muito tempo, um dos privilégios do poder soberano, seja este direito absoluto ou não.[22] Como explica Foucault, este poder se manifestava na sociedade como dispositivo de confisco, de subtração, como um direito de apropriação de bens, de trabalho, dos corpos e da vida. No entanto, com o avanço da industrialização esse poder é substituído por outro – o poder disciplinar - que possui a função de gerir a vida e não mais causar a morte. A partir deste momento, o poder passa a fixar-se no desenrolar da vida, sendo a morte o limite do poder, o momento que lhe escapa. [23]

Voltando à questão do poder disciplinar, a partir do desenvolvimento do poder de gerir a vida, o mecanismo de confisco deixa de ser a peça principal de manifestação do poder, sendo substituído por outros como o reforço, o controle, a vigilância, a organização de forças etc. Esse poder tem sua centralidade no corpo como máquina, deixando de implicar na apropriação de um serviço, trabalho ou bem, e passando a implicar na apropriação total do corpo, do tempo e do comportamento do indivíduo, o que torna este poder contínuo.[2425] Nas palavras de Foucault "no sistema disciplinar, não se está à eventual disposição de alguém, está-se perpetuamente sob o olhar de alguém ou, em todo o caso, na situação de ser olhado".[26]

Como já mencionado, para que esse poder se mantenha é necessária a utilização de mecanismos de vigilância, sendo a escrita o mecanismo inicialmente mencionado por Foucault,

---

[19] FOUCAULT, Michel. **O poder psiquiátrico**. Curso dado no Collège de France (1973-1974). Tradução de Eduardo Brandão. São Paulo: Martins Fontes, 2006. p. 52-53

[20] FOUCAULT, Michel. **O poder psiquiátrico**. Curso dado no Collège de France (1973-1974). Tradução de Eduardo Brandão. São Paulo: Martins Fontes, 2006. p. 53-54

[21] FOUCAULT, Michel. **O poder psiquiátrico**. Curso dado no Collège de France (1973-1974). Tradução de Eduardo Brandão. São Paulo: Martins Fontes, 2006. p. 56

[22] FOUCAULT, Michel. **História da sexualidade I**: A vontade de saber. Tradução de Maria Thereza da Costa Albuquerque e J. A. Guilhon Albuquerque. 11ª ed. Rio de Janeiro/São Paulo: Paz e Terra, 2011. p. 145

[23] FOUCAULT, Michel. **História da sexualidade I**: A vontade de saber. Tradução de Maria Thereza da Costa Albuquerque e J. A. Guilhon Albuquerque. 11ª ed. Rio de Janeiro/São Paulo: Paz e Terra, 2011. p. 146, 149.

[24] FOUCAULT, Michel. **História da sexualidade I**: A vontade de saber. Tradução de Maria Thereza da Costa Albuquerque e J. A. Guilhon Albuquerque. 11ª ed. Rio de Janeiro/São Paulo: Paz e Terra, 2011. p. 146

[25] FOUCAULT, Michel. **O poder psiquiátrico**. Curso dado no Collège de France (1973-1974). Tradução de Eduardo Brandão. São Paulo: Martins Fontes, 2006. p.57-59.

[26] FOUCAULT, Michel. **O poder psiquiátrico**. Curso dado no Collège de France (1973-1974). Tradução de Eduardo Brandão. São Paulo: Martins Fontes, 2006. p.59

para que se possa garantir o registro de tudo que diz respeito ao indivíduo o qual o poder subjuga, tornando essas informações sempre acessíveis e assegurando a "onivisibilidade", ou seja, a total transparência, uma grande característica da disciplina.[27] A vigilância, a transparência contínua e perpétua, se faz essencial para o poder disciplinar, por possibilitar que este tenha uma reação rápida, desde o primeiro instante, e, por vezes, até antes do próprio ato se realizar, "no momento em que a virtualidade está se tornando realidade".[28] Essa questão da virtualidade do comportamento, ou seja, do gesto antes mesmo dele se realizar, é explicado por Foucault como sendo o nível da alma, diferente daquela definida pela teoria cristã, sendo como uma psiquê.[29] É nesse ponto que Foucault traz a figura do panóptico para estabelecer uma relação com o poder disciplinar, já que, segundo ele, esse poder possui um caráter panóptico na medida em que depende da visibilidade absoluta e constante para que possa realizar ações punitivas sobre as virtualidades de comportamento.[30] Nas palavras de Foucault:

> O dispositivo panóptico organiza unidades espaciais que permitem ver constantemente e reconhecer de imediato. Em suma, inverte-se o princípio da masmorra; ou melhor, das suas três funções – encerrar, privar de luz e esconder -, só se conserva a primeira e suprimem-se as outras duas. A luz e o olhar do vigia captam melhor que a escuridão, que antes protegia. A visibilidade é uma armadilha.[31]

Nesse sentido, a eficiência do panóptico encontra-se justamente no fato de que o sujeito está sob o olhar omnipresente do vigia e é impedido de ver ou comunicar-se com seus companheiros, o que garante um funcionamento automático do poder e uma sujeição real, não sendo necessário o uso de força para subjugação do indivíduo ao bom comportamento. [32] O panóptico provoca no recluso um estado de constante visibilidade, assegurando o efeito permanente da vigilância, ainda que não haja, em realidade, um vigia a observar os reclusos permanentemente. Foucault o descreve como uma "máquina de criar e sustentar uma relação de poder independente de quem o exerce".[33] Para Foucault, portanto, o panoptismo representava

---

[27] FOUCAULT, Michel. **O poder psiquiátrico**. Curso dado no Collège de France (1973-1974). Tradução de Eduardo Brandão. São Paulo: Martins Fontes, 2006. p. 61

[28] FOUCAULT, Michel. **O poder psiquiátrico**. Curso dado no Collège de France (1973-1974). Tradução de Eduardo Brandão. São Paulo: Martins Fontes, 2006. p. 63-64

[29] FOUCAULT, Michel. **O poder psiquiátrico**. Curso dado no Collège de France (1973-1974). Traduçãode Eduardo Brandão. São Paulo: Martins Fontes, 2006. p. 63-64

[30] FOUCAULT, Michel. **O poder psiquiátrico**. Curso dado no Collège de France (1973-1974). Tradução de Eduardo Brandão. São Paulo: Martins Fontes, 2006. p. 65

[31] FOUCAULT, Michel. **Vigiar e Punir**: Nascimento da Prisão. Tradução de Pedro Elói Duarte. Lisboa: 70, 2013. p. 286

[32] FOUCAULT, Michel. **Vigiar e Punir**: Nascimento da Prisão. Tradução de Pedro Elói Duarte. Lisboa: 70, 2013. p. 287-288.

[33] FOUCAULT, Michel. **Vigiar e Punir**: Nascimento da Prisão. Tradução de Pedro Elói Duarte. Lisboa: 70, 2013. p. 287.

um dispositivo que melhoraria a eficácia do poder, tornando-o mais leve, mais rápido e mais sutil.[34] Assim:

> O panoptismo é um dos traços característicos de nossa sociedade. É uma forma de poder que se exerce sobre os indivíduos em forma de vigilância individual e contínua, em forma de controle de punição e recompensa e em forma de correção, isto é, de formação e transformação dos indivíduos em função de certas normas. Este tríplice aspecto do panoptismo – vigilância, controle e correção – parece ser uma dimensão fundamental e característica das relações de poder que existem em nossa sociedade. [...] Vivemos hoje numa sociedade programada, no fundo, por Bentham, uma sociedade panóptica, sociedade onde reina o panoptismo.[35]

Ressalta-se que o Panóptico não deve ser entendido como uma utopia ou um edifício onírico. Ele representa "um mecanismo de poder levado à sua forma ideal"[36], pois possibilita que aquele que possui o poder intervenha incessantemente, bem como que a pressão constante exercida sob aqueles que assumem que estão sendo vigiados age preventivamente, antes que faltas, erros e crimes sejam cometidos, sendo assim, o panóptico intensifica qualquer manifestação de poder.[37] Portanto, de acordo com o autor:

> O panóptico funciona como uma espécie de laboratório de poder. Graças aos seus mecanismos de observação, ganha em eficácia e em capacidade de penetração no comportamento dos homens; um aumento de saber estabelece-se sobre todos os avanços do poder e descobre objetos de conhecimento em todas as superfícies onde este se exerce.[38]

Ainda, Foucault entende que, tendo em vista que qualquer um pode exercer a função de vigia na torre central, não haveria risco de esse aumento de poder ser corrompido, transformando-se em tirania, pois o panóptico, como dispositivo disciplinar, seria democraticamente controlado, tendo em vista que estaria sempre acessível à sociedade, ao "grande comité do tribunal do mundo". O dispositivo panóptico tem a função de organizar o

---

[34] FOUCAULT, Michel. **Vigiar e Punir**: Nascimento da Prisão. Tradução de Pedro Elói Duarte. Lisboa: 70, 2013. p. 296

[35] FOUCAULT, Michel. **A verdade e as formas jurídicas**. Conferências de Michel Foucault na PUC-Rio de 21 a 25 de maio de 1973. Tradução de Roberto Cabral de Melo Machado e Eduardo Jardim Morais. Rio de Janeiro: NAU, 2002. p. 103

[36] FOUCAULT, Michel. **Vigiar e Punir**: Nascimento da Prisão. Tradução de Pedro Elói Duarte. Lisboa: 70, 2013. p. 291

[37] FOUCAULT, Michel. **Vigiar e Punir**: Nascimento da Prisão. Tradução de Pedro Elói Duarte. Lisboa: 70, 2013. p. 292

[38] FOUCAULT, Michel. **Vigiar e Punir**: Nascimento da Prisão. Tradução de Pedro Elói Duarte. Lisboa: 70, 2013. p. 291

poder, tornando-o mais eficaz e econômico e, consequentemente, aumentando a produção, desenvolvendo a economia, difundindo educação, elevando o nível da moral pública.[39]

Existem, portanto, 02 (dois) extremos do poder disciplinar, a saber: (i) a "disciplina-bloqueio", caracterizada por instituições precisas e relativamente fechadas – casernas, escolas, oficinas, hospitais, prisões - e voltada para funções negativas – "travar o mal, romper as comunicações, suspender o tempo" -, e (ii) a "disciplina-mecanismo", inaugurada com o panoptismo, e consistente em um dispositivo de melhoria do exercício do poder. Para Foucault, o movimento de um extremo ao outro consiste em uma transformação histórica que ocorre durante os séculos XVII e XVIII, na qual o poder disciplinar passa de um esquema de exceção à uma vigilância total e generalizada por meio da multiplicação dos dispositivos de disciplina e sua distribuição por toda a sociedade e a formação do que Foucault denomina de "sociedade disciplinar".[40] Assim, o dispositivo panóptico "trata-se de mostrar como se pode «reabrir» as disciplinas e fazê-las funcionar de forma difusa, múltipla e polivalente em todo o corpo social. [...] A organização panóptica fornece a fórmula desta generalização".[41] Por ter concebido a ideia do panóptico, Foucault considera Jeremy Bentham um dos pensadores mais importantes da história – afirmando ser ainda mais relevante que Kant e Hegel -, tendo em vista que, segundo ele, Bentham definiu de modo mais exato as formas de poder existentes nas sociedades dos séculos XIX e XX por meio do "maravilhoso e célebre modelo desta sociedade da ortopedia generalizada", sendo esse uma "utopia que efetivamente se realizou". [42]

Avançando em seus estudos a respeito do poder sobre a vida, Foucault conclui que a partir do século XVII esse poder se desenvolve em duas formas principais e interligadas, sendo uma delas centrada no corpo como máquina, em seu adestramento, aumento de aptidões, extorsão de forças, ampliação da utilidade e docilidade dos corpos e em sua integração com sistemas de controle, sendo este o poder disciplinar, a "anátomo-política do corpo humano". A segunda forma de desenvolvimento desse poder se formou um pouco mais tarde, na metade do século XVIII, e centrava-se no corpo-espécie, isto é, no corpo como suporte dos processos biológicos – proliferação, nascimento, mortalidade, saúde, longevidade -, intervindo nesses

[39] FOUCAULT, Michel. **Vigiar e Punir**: Nascimento da Prisão. Tradução de Pedro Elói Duarte. Lisboa: 70, 2013. p. 294
[40] FOUCAULT, Michel. **Vigiar e Punir**: Nascimento da Prisão. Tradução de Pedro Elói Duarte. Lisboa: 70, 2013. p. 296
[41] FOUCAULT, Michel. **Vigiar e Punir**: Nascimento da Prisão. Tradução de Pedro Elói Duarte. Lisboa: 70, 2013. p. 295
[42] FOUCAULT, Michel. **A verdade e as formas jurídicas**. Conferências de Michel Foucault na PUC-Rio de 21 a 25 de maio de 1973. Tradução de Roberto Cabral de Melo Machado e Eduardo Jardim Morais. Rio de Janeiro: NAU, 2002. p. 86-87.

processos e controlando-os a partir de uma "bio-política da população".[43] O biopoder foi indispensável ao desenvolvimento do capitalismo, uma vez que esse dependia da inserção controlada de corpos no aparelho de produção, bem como da adaptação de fenômenos de população aos processos econômicos. Mas essa nova técnica de poder não é suficiente ao capitalismo, portanto, não substitui a técnica disciplinar, mas atua juntamente com ela, a integrando e a modificando parcialmente.[44][45] Nesse sentido, Foucault observa:

> Mais precisamente, eu diria isto: a disciplina tenta reger a multiplicidade dos homens na medida em que essa multiplicidade pode e deve redundar em corpos individuais que devem ser vigiados, treinados, utilizados, eventualmente punidos. E, depois, a nova tecnologia que se instala se dirige à multiplicidade dos homens, não na medida em que eles se resumem em corpos, mas na medida em que ela forma, ao contrário, uma massa global, afetada por processos de conjuntos que são próprios da vida, que são processos como o nascimento, a morte, a produção, a doença, etc.[46]

A partir desse momento, do surgimento da biopolítica, passa-se a observar, vigiar, medir, com a finalidade de controlar não só os comportamentos dos corpos, sua utilidade e aptidões, como corpos produtivos, mas também os fenômenos mais ou menos espontâneos, que são os fenômenos de natalidade, adotando-se a medição estatística desses processos naturais e lançando mão da demografia. Tratava-se também de controle de endemias, doenças que subtraiam forças, diminuíam tempo de trabalho, aumento de custos econômicos pela falta de produção e pelo custo dos tratamentos, ou seja, "a doença como fenômeno de população", que se introduz na vida e a corrói. [47]

Algumas das práticas das quais a biopolítica vai extrair seu saber e exercer intervenção são a natalidade, a morbidade, as incapacidades biológicas diversas, os efeitos do meio etc. A biopolítica, portanto, lida com a população e exerce seu poder em relação aos fenômenos coletivos, aleatórios e imprevisíveis individualmente, mas que se tornam relevantes e constantes no nível da massa. Para o exercício desse poder são implantados mecanismos de previsão, estimativas estatísticas e medições globais para que se possa intervir nas determinações desses fenômenos, baixando a morbidade, encompridando a vida, estimulando a natalidade;

---

43 FOUCAULT, Michel. **História da sexualidade I**: A vontade de saber. Tradução de Maria Thereza da Costa Albuquerque e J. A. Guilhon Albuquerque. 11 ed. Rio de Janeiro/São Paulo: Paz e Terra, 2011. p. 150.

44 FOUCAULT, Michel. **História da sexualidade I**: A vontade de saber. Tradução de Maria Thereza da Costa Albuquerque e J. A. Guilhon Albuquerque. 11 ed. Rio de Janeiro/São Paulo: Paz e Terra, 2011. p. 151-152.

45 FOUCAULT, Michel. **Em defesa da sociedade**: curso no Collège de France (1975-1976). Tradução de Maria Ermantina Galvão. 2 ed. São Paulo: WMF Martins Fontes, 2010. p. 203.

46 FOUCAULT, Michel. **Em defesa da sociedade**: curso no Collège de France (1975-1976). Tradução de Maria Ermantina Galvão. 2 ed. São Paulo: WMF Martins Fontes, 2010. p. 204.

47 FOUCAULT, Michel. **Em defesa da sociedade**: curso no Collège de France (1975-1976). Tradução de Maria Ermantina Galvão. 2 ed. São Paulo: WMF Martins Fontes, 2010. p. 204-205.

otimizando o estado de vida e destinando-se a "maximizar forças e extraí-las", tal como o poder disciplinar, mas utilizando caminhos diferentes, assegurando sobre o homem-espécie uma regulamentação e não uma disciplina.[48] Assim, Foucault explica que:

> [...] tudo sucedeu como se o poder, que tinha como modalidade, como esquema organizador, a soberania, tivesse ficado inoperante para reger o corpo econômico e político de uma sociedade em via, a um só tempo, de explosão demográfica e de industrialização. [...] Foi para recuperar o detalhe que se deu uma primeira acomodação: acomodação dos mecanismos de poder sobre o corpo individual, com vigilância e treinamento – isso foi a disciplina. [...] E, depois, vocês têm em seguida, no final do século XVIII, uma segunda acomodação, sobre os fenômenos globais, sobre os fenômenos de população, com os processos biológicos ou biossociológicos das massas humanas.[49]

Desse modo, Foucault reconhece a atuação conjunta desses 02 (dois) poderes – disciplinar e biopolítico -, durante os séculos XVIII, XIX e XX, os quais se integram e, por vezes, se sobrepõem e se modificam parcialmente. No entanto, Foucault não chega à análise da biopolítica neoliberal, o que pretendia fazer em seu curso "Nascimento da biopolítica" 1978 a 1979[50], o que o impede, segundo Byung Chul-Han, de perceber que a biopolítica, como conceito próprio da sociedade disciplinar, não seria apropriado para a análise e a descrição do poder em um regime neoliberal[51], como fez Gilles Deleuze, em 1990, em breve texto denominado "*Post-scriptum* sobre as sociedade de controle".[52]

De acordo com Deleuze, a sociedade disciplinar passa por uma crise generalizada dos meios de confinamento em razão de uma nova técnica de poder que se instalava lentamente, sofrendo uma aceleração após a Segunda Guerra Mundial. A partir do século XX, portanto, a sociedade disciplinar estava sendo substituída pela sociedade de controle, na qual o poder passa a ser exercido "ao ar livre", substituindo as disciplinas que operavam em sistemas fechados.[53] Deleuze propõe uma diferenciação entre a sociedade disciplinar e a sociedade de controle por meio do uso dos conceitos "analógico" e "numérico", explicando que os meios de confinamento da sociedade disciplinar eram independentes e a linguagem comum a esses meios era analógica, por outro lado, os diferentes modos de controle são inseparáveis, formando uma geometria cuja

---

[48] FOUCAULT, Michel. **Em defesa da sociedade**: curso no Collège de France (1975-1976). Tradução de Maria Ermantina Galvão. 2 ed. São Paulo: WMF Martins Fontes, 2010. p. 206-207.
[49] FOUCAULT, Michel. **Em defesa da sociedade**: curso no Collège de France (1975-1976). Tradução de Maria Ermantina Galvão. 2 ed. São Paulo: WMF Martins Fontes, 2010. p. 210.
[50] FOUCAULT, Michel**. Nascimento da biopolítica**: curso dado no Collège de France (1978-1979). Tradução de Eduardo Brandão. São Paulo: Martins Fontes. 2008.
[51] HAN, Byung-Chul. **Psicopolítica**: O neoliberalismo e as novas técnicas de poder. Tradução de Maurício Liesen. Belo Horizonte: Âyiné, 2018. p. 37-38.
[52] DELEUZE, Gilles. **Conversações**, 1972-1990. Tradução de Peter Pál Pelbart. São Paulo: 34, 1992. p. 219-226.
[53] DELEUZE, Gilles. **Conversações**, 1972-1990. Tradução de Peter Pál Pelbart. São Paulo: 34, 1992. p. 219-220.

linguagem é numérica. Ainda, as instituições de confinamento eram moldes, ao passo que os controles são uma modulação auto-deformante, que muda constantemente, se adequando ao regime neoliberal.[54]

Na sociedade de controle os indivíduos tornam-se projetos de autoempreendedorismo. Substitui-se as fábricas pelas empresas, sujeitando os indivíduos à uma rivalidade constante, contrapondo-os entre si e os dividindo em si mesmo. Do mesmo modo, a escola é substituída pela formação permanente. Na sociedade de controle nunca se termina nada, vivendo-se em estados metaestáveis.[55] Como explica Han, "o 'eu' como projeto, que acreditava ter se libertado das coerções externas e das restrições impostas por outros, submete-se agora a coerções internas, na forma de obrigações de desempenho e otimização".[56]

Deleuze utiliza, também, as figuras da toupeira e da serpente para diferenciar as duas sociedades. Segundo ele, a sociedade disciplinar constitui-se por ambientes fechados de confinamento, o indivíduo dessa sociedade passa de um meio de confinamento a outro, cada um com suas leis, cada um uma variável independente. Esse indivíduo se movimenta, portanto, em sistemas fechados, pré-instalados, por isso, a toupeira é o animal da sociedade disciplinar. A sociedade neoliberal de controle e suas formas de produção pós-industriais, por sua vez, exigem mais abertura e dissolução de fronteira, portanto, a serpente assume o lugar da toupeira, na medida em que é um projeto, criando espaço a partir do movimento.[57][58]

Para Deleuze, o *marketing* é o instrumento do controle social, exercendo seu poder por meio da modulação, incitando nos indivíduos a meta de se enquadrar no ideal imposto pela lógica neoliberal. Esse controle é de curto prazo e alta rotação, mas contínuo e ilimitado.[59] Assim, segundo o autor:

> As sociedades disciplinares têm dois pólos: a assinatura que indica o indivíduo, e o número de matrícula que indica sua posição numa massa. É que as disciplinas nunca viram incompatibilidade entre os dois, e é ao mesmo tempo que o poder massificante e individuante, isto é, constitui num corpo único aqueles sobre os quais se exerce, e molda a individualidade de cada membro do corpo [...] Nas sociedade de controle, ao contrário, o mais essencial [...] [é] uma cifra [...] A linguagem numérica do controle é feita de cifras, que marcam o acesso à informação, ou a rejeição. Os indivíduos tornaram-se 'dividuais', divisíveis, e as massas tornaram-se amostras, dados, mercados ou 'bancos'.[60]

---

[54] DELEUZE, Gilles. **Conversações**, 1972-1990. Tradução de Peter Pál Pelbart. São Paulo: 34, 1992. p. 220-221.
[55] DELEUZE, Gilles. **Conversações**, 1972-1990. Tradução de Peter Pál Pelbart. São Paulo: 34, 1992. p. 221-222.
[56] HAN, Byung-Chul. **Psicopolítica**: O neoliberalismo e as novas técnicas de poder. Tradução de Maurício Liesen. Belo Horizonte: Âyiné, 2018. p. 9.
[57] DELEUZE, Gilles. **Conversações**, 1972-1990. Tradução de Peter Pál Pelbart. São Paulo: 34, 1992. p. 222-223.
[58] HAN, Byung-Chul. **Psicopolítica**: O neoliberalismo e as novas técnicas de poder. Tradução de Maurício Liesen. Belo Horizonte: Âyiné, 2018. p. 29-31.
[59] DELEUZE, Gilles. **Conversações**, 1972-1990. Tradução de Peter Pál Pelbart. São Paulo: 34, 1992. p. 222-224.
[60] DELEUZE, Gilles. **Conversações**, 1972-1990. Tradução de Peter Pál Pelbart. São Paulo: 34, 1992. p. 222.

Apoiando-se na obra de Gabriel Tarde, e dando continuidade as discussões de Deleuze a respeito das sociedades de controle, Maurizio Lazzarato explica que nessa sociedade o poder se expressa pela ação à distância de uma mente sobre outra, pela capacidade dos cérebros de afetar e serem afetados, capacidade essa que é beneficiada pelas tecnologias. Esse controle das mentes, segundo ele, é feito pela modulação dos fluxos de desejos, crenças e forças (memórias e atenção). O homem espírito, que para Foucault é objeto do biopoder apenas em segundo plano, passa a estar no centro da sociedade de controle.[61] Lazzarato define essas novas relações de poder, que possuem como objeto a memória e a atenção, como noopolítica, que consistiria no conjunto das técnicas de controle. Segundo ele, "se as disciplinas moldavam os corpos ao constituir hábitos, principalmente na memória corporal, as sociedades de controle modulam os cérebros, constituindo hábitos sobretudo na memória mental".[62] Nesse sentido, na visão de Lazzarato, há na sociedade contemporânea a moldagem dos corpos pelas disciplinas, a gestão da vida pelo biopoder e a modulação da memória pela noopolítica, sendo que esses dispositivos, com finalidades divergentes, não se substituem, mas se agenciam e se integram.[63]

Esse conceito de noopolítica aproxima-se do conceito de psicopolítica, desenvolvido por Byung Chul-Han[64], que é essencial para a análise da vigilância na sociedade contemporânea, tendo em vista que a vigilância é um instrumento para o exercício do poder, tanto do poder disciplinar e biopoder que garantem a manutenção da sociedade disciplinar quanto do poder exercido por meio da modulação (psicopolítica/noopolítica) que garantem a manutenção da sociedade de controle.

Byung Chul-Han, assim como Gilles Deleuze e Maurizio Lazzarato, parte das obras de Michel Foucault sobre a sociedade disciplinar e a biopolítica para descrever a passagem dessas para a sociedade de controle neoliberal. Para Han, o regime neoliberal explora a psique e, desse modo, a psicopolítica é a sua forma de governo e o poder assume, cada vez mais, uma forma permissiva, promovendo uma falsa sensação de liberdade naqueles que subjuga por ser inacessível aos sujeitos submissos, os quais nunca se tornam conscientes do contexto de

---

[61] LAZZARATO, Maurizio. **As revoluções do capitalismo**. Tradução de Leonora Corsini. Rio de Janeiro: Civilização Brasileira, 2006. p. 76, 84-85

[62] LAZZARATO, Maurizio**. As revoluções do capitalismo**. Tradução de Leonora Corsini. Rio de Janeiro: Civilização Brasileira, 2006. p. 86.

[63] LAZZARATO, Maurizio. **As revoluções do capitalismo.** Tradução de Leonora Corsini. Rio de Janeiro: Civilização Brasileira, 2006. p. 86-87.

[64] HAN, Byung-Chul. **Psicopolítica**: O neoliberalismo e as novas técnicas de poder. Tradução de Maurício Liesen. Belo Horizonte: Âyiné, 2018.

dominação.[65] O poder disciplinar, descrito por Foucault, se baseia na negatividade, e é expresso de forma inibitória. Contrariamente, no regime neoliberal, o poder é expresso de forma mais sutil e flexível, fazendo com que as pessoas se submetam ao contexto de dominação por vontade própria. "Ao invés de tornar as pessoas obedientes, tenta deixá-las dependentes".[66]

Essa técnica de poder é muito mais eficiente do que o poder da sociedade disciplinar, pois não age por meio da proibição e da suspensão, mas sim por meio do agrado e da satisfação. Não impõe silêncio aos seus submissos, mas os convida a compartilhar incessantemente suas opiniões, desejos, preferências, necessidades etc., para então explorá-las, criando o que Han chama de "crise da liberdade", que consiste em "estar diante de uma técnica de poder que não rejeita ou oprime a liberdade, mas a explora".[67] Nesse sentido, Han observa que:

> As sociedades de controle caracterizam-se assim pela multiplicação da oferta de 'mundos' (de consumo, de informação, de trabalho, de lazer). Trata-se, porém, de mundos lisos, banais, formatados, porque são mundos da maioria, vazios de toda singularidade. [...] Diante desses mundos normalizados, nossa 'liberdade' é exercida exclusivamente para escolher dentre possíveis que outros instituíram e conceberam. Ficamos sem o direito de participar da construção dos mundos, de formular problemas e de inventar soluções, a não ser no interior de alternativas já estabelecidas.[68]

A forma de governo psicopolítica, portanto, utiliza o poder (psicopoder) para explorar a psique, modulando-a, ao invés de discipliná-la e submetê-la a coações e proibições. A sociedade caminha de uma vigilância passiva ao controle ativo, sob o qual até a vontade própria dos sujeitos submissos é atingida, tendo em vista que o psicopoder possui a capacidade – com a ajuda da vigilância digital - de intervir nos processos psicológicos, explorando o indivíduo por completo, sua atenção total.[6970] Tudo o que pertence às práticas e formas de expressão da liberdade são explorados na sociedade de controle. Nessa sociedade, a liberdade e a comunicação transformam-se em monitoramento e controle[71]. Nesse ponto, Han faz uso da figura do panóptico para diferenciar como o dispositivo de vigilância é utilizado em uma e em

---

[65] HAN, Byung-Chul. **Psicopolítica**: O neoliberalismo e as novas técnicas de poder. Tradução de Maurício Liesen. Belo Horizonte: Âyiné, 2018. p. 26, 30, 35.
[66] HAN, Byung-Chul. **Psicopolítica**: O neoliberalismo e as novas técnicas de poder. Tradução de Maurício Liesen. Belo Horizonte: Âyiné, 2018. p. 26.
[67] HAN, Byung-Chul. **Psicopolítica**: O neoliberalismo e as novas técnicas de poder. Tradução de Maurício Liesen. Belo Horizonte: Âyiné, 2018. p. 26-27.
[68] LAZZARATO, Maurizio. **As revoluções do capitalismo**. Tradução de Leonora Corsini. Rio de Janeiro: Civilização Brasileira, 2006. p. 101-102.
[69] HAN, Byung-Chul. **Psicopolítica**: O neoliberalismo e as novas técnicas de poder. Tradução de Maurício Liesen. Belo Horizonte: Âyiné, 2018. p. 23,45.
[70] HAN, Byung-Chul. **No enxame**: perspectivas do digital. Tradução de Lucas Machado. Petrópolis: Vozes, 2018. p. 130-131.
[71] HAN, Byung-Chul. **Psicopolítica**: O neoliberalismo e as novas técnicas de poder. Tradução de Maurício Liesen. Belo Horizonte: Âyiné, 2018. p. 11, 19.

outra sociedade. Segundo o filósofo, na sociedade disciplinar "os internos do pan-óptico benthaminiano eram isolados uns dos outros, de modo que não conversassem. Os internos do pan-óptico digital, por sua vez, comunicam-se intensivamente e expõem-se por vontade própria. *Participam* assim, ativamente, da construção do pan-óptico digital."[72]

Não se trata propriamente do fim do panóptico, mas do começo de um novo tipo de panóptico, que Han chama de "panóptico digital". Esse se diferencia substancialmente do dispositivo idealizado por Bentham na medida em que é aperspectivístico, isto é, não se tem mais uma torre central de onde um vigia supervisiona os internos, com seu olhar omnividente. Para Han, é justamente a supervisão aperspectivista que torna esse novo tipo de panóptico tão eficiente, sendo possível tornar tudo transparente, a partir de todos os lugares, por cada um.[73]

O que Han chama de panóptico digital, portanto, é a forma de manutenção do poder por meio da exploração da liberdade e da comunicação com o intuito de adquirir um conhecimento de dominação para modular as mentes dos indivíduos submissos, os quais, por sua vez, não são conscientes dessa vigilância e dominação. A vigilância realizada por meio do panóptico digital, diferentemente do panóptico de Bentham, utilizado na sociedade disciplinar, não tem tanto o caráter de omnivisibilidade (referindo-se ao sentido da visão), mas sim um caráter de omnisciência, tendo em vista que a vigilância é mais ubíqua e pervasiva[74], mais líquida, e o conhecimento de dominação vem, portanto, principalmente por meio dos dados.

Observa-se que aqui Han fala de um controle que não é mais exercido por um poder central, pelo Estado, mas sim um controle de todos sobre todos. A sociedade de controle, para ele, se consuma quando todos os sujeitos dessa sociedade se desnudam por coação interna, por necessidade de exposição e, assim, se passa a exigir uma iluminação completa e recíproca e todos passam a controlar todos. Essa sociedade é caracterizada, portanto, pela autoexploração, que para Han é muito mais eficiente do que a exploração pelo outro, tendo em vista que a autoexploração – e a autoiluminação - é acompanhada pelo sentimento de liberdade.[75]

Han afirma que "o que ocorre hoje é uma vigilância sem vigilância", no sentido de que existe uma vigilância implícita entre os cidadãos em toda forma de comunicação feita nas redes,

---

[72] HAN, Byung-Chul. **Psicopolítica**: O neoliberalismo e as novas técnicas de poder. Tradução de Maurício Liesen. Belo Horizonte: Âyiné, 2018. p. 19.
[73] HAN, Byung-Chul. **Sociedade da transparência**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017. p. 106.
[74] Como já mencionado, esses termos são muito utilizados para descrever a característica de omnipresença e distribuição da computação no cotidiano do ser humano. Tendo em vista que a vigilância contemporânea é em muito instrumentalizada por tecnologias e pelo poder computacional, pode-se dizer, partindo do conceito de computação ubíqua e pervasiva já apresentado, que a vigilância apresenta também essas duas características.
[75] HAN, Byung-Chul. **Sociedade da transparência**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017. p. 109-112.

sendo que um é o panóptico do outro e de si mesmo. Ele considera esse tipo de vigilância mais problemática do que aquela feita pelo Estado e seus serviços de inteligência e afirma que a época em que se precisava confrontar o Estado como "instância de dominação que arrecadava dados dos cidadãos contra a vontade deles" já foi superada, na medida em que atualmente os indivíduos se expõem sem coerção[76], afirmação essa um tanto perigosa, já que, apesar da autoexposição voluntária, ainda existem assimetrias de poder e relações de dominação. O que importa, no entanto, é ressaltar que o sujeito submisso a essa dominação participa de sua exploração.

O dispositivo de transparência da sociedade disciplinar era moral ou biopolítico e tinha o intuito de reformar a moral, preservar a saúde, difundir educação etc. A coação por transparência da sociedade de controle, por sua vez, possui um imperativo majoritariamente econômico, pois, de acordo com Han, a pessoa que torna sua vida transparente maximiza sua eficiência econômica. "O cliente transparente é o novo presidiário, sim, o *homo sacer* do panóptico digital".[77] Na medida em que o enfoque do sistema de produção passa a ser o imaterial, mais informação e mais comunicação traduzem-se em mais produtividade. Os sujeitos assimilam um ideal de sucesso e o perseguem com a meta de se enquadrar.[7879] "Consumidores se entregam voluntariamente a observações panópticas que controlam e satisfazem suas necessidades. Aqui, os meios sociais já não se distinguem das máquinas panópticas; comunicação e comércio, liberdade e controle se identificam."[80]

O controle por meio da exploração da liberdade se faz possível, em grande parte, graças à autoexposição voluntária. A total transparência, característica do panóptico na sociedade disciplinar, torna-se, também, um dispositivo neoliberal. "No final, a abertura serve à comunicação sem limites, que é oposta ao fechamento, à reserva e à interioridade".[81] É essa autoexposição voluntária, fruto da exploração pela liberdade, que possibilita a geração de um "conhecimento de dominação" por parte daqueles que detém o poder e fazem uso desses dados,

---

[76] HAN, Byung-Chul. **Psicopolítica**: O neoliberalismo e as novas técnicas de poder. Tradução de Maurício Liesen. Belo Horizonte: Âyiné, 2018. p. 21-22.
[77] HAN, Byung-Chul. **Sociedade da transparência**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017. p. 113.
[78] HAN, Byung-Chul. **Psicopolítica**: O neoliberalismo e as novas técnicas de poder. Tradução de Maurício Liesen. Belo Horizonte: Âyiné, 2018. p. 19-20
[79] HAN, Byung-Chul. **Sociedade da transparência**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017. p. 113-114.
[80] HAN, Byung-Chul. **Sociedade da transparência**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017. p. 114.
[81] HAN, Byung-Chul. **Psicopolítica**: O neoliberalismo e as novas técnicas de poder. Tradução de Maurício Liesen. Belo Horizonte: Âyiné, 2018. p. 20

permitindo a intervenção na psique. É nesse sentido que o psicopoder se faz tão eficiente[82], pois para Han:

> O poder inteligente lê e avalia nossos pensamentos conscientes e inconscientes. Baseia-se na auto-organização e na otimização pessoal voluntárias. Assim, não precisa superar nenhuma resistência. Essa dominação não necessita de nenhum grande esforço, de nenhuma violência, porque simplesmente acontece. Deseja dominar buscando agradar e gerando dependência.[83]

Dados pessoais e informações são o que dão suporte ao psicopoder. De acordo com boyd e Crawford, "*Big Data*[84] *is fundamentally networked. Its value comes from the patterns that can be derived by making connections between pieces of data, about an individual, about individuals in relation to others, about groups of people, or simply about the structure of information itself*".[85] Desse modo, o *Big Data* torna-se um instrumento essencial para seu exercício, já que é por meio do tratamento de grande quantidade de dados – como, por exemplo, por meio da aplicação de técnicas de Mineração de Dados (*Data Mining*)[86] - que se pode obter informações relevantes desses dados, as quais são transformadas em conhecimento, por exemplo, sobre as dinâmicas e comportamentos sociais, bem como prognósticos sobre o comportamento humano, tornando acessível modelos de comportamento sobre os quais os próprios indivíduos não estavam conscientes (*inconsciente-coletivo*)[87], o que "positiviza" os

---

[82] HAN, Byung-Chul. **Psicopolítica**: O neoliberalismo e as novas técnicas de poder. Tradução de Maurício Liesen. Belo Horizonte: Âyiné, 2018. p. 23.

[83] HAN, Byung-Chul. **Psicopolítica**: O neoliberalismo e as novas técnicas de poder. Tradução de Maurício Liesen. Belo Horizonte: Âyiné, 2018. p. 28.

[84] O termo Big Data é utilizado para se referir à grandes conjuntos de dados, cujo tamanho vai além da capacidade de softwares tradicionais de bancos de dados para capturar, armazenas, gerenciar e analisar esses dados. (MANYIKA, James et al. **Big Data**: the next frontier for innovation, competition, and productivity. McKinsey Global Institute, 2011, p.1). Nesse sentido, o Big Data é assim caracterizado pelos 3 V's: volume, velocidade e variedade de tipos de dados. (KITCHIN, Rob. **The data Revolution**: Big Data, open data, data infrastructures and their consequences. Los Angeles: Sage, 2014)

[85] BOYD, Danah; CRAWFORD, Kate. **Six Provocations for Big Data**. Oxford, 2011. Paper apresentado em A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, Oxford Internet Institute em 21 set. 2011. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1926431. Acesso em: 04 mai. 2021. p. 2.

[86] O termo "Mineração de Dados" alude ao processo de mineração, extração de minerais valiosos de uma mina, tendo em vista que no processo de mineração de dados, faz-se a exploração de uma base de dados, usando algoritmos como ferramentas para se obter conhecimento. Isso porque, de acordo com Castro e Ferrari, "os dados são símbolos ou signos não estruturados, sem significado, como valores em uma tabela, e a informação está contida nas descrições, agregando significado e utilidade aos dados, como o valor da temperatura do ar. Por fim, o conhecimento é algo que permite uma tomada de decisão para a agregação de valor, então, por exemplo, saber, que vai chover no fim de semana pode influenciar sua decisão de viajar ou não para a praia" (CASTRO, Leandro Nunes; FERRARI, Daniel Gomes. **Introdução à Mineração de Dados**: conceitos básicos, algoritmos e aplicações. São Paulo: Saraiva, 2016. p. 7).

[87] HAN, Byung-Chul. **No enxame**: perspectivas do digital. Tradução Lucas de Machado. Petrópolis: Vozes, 2018. p. 133-134.

indivíduos, tornando-os quantificáveis, mensuráveis e controláveis. De forma pessimista, Han afirma que "os big data anunciam o fim da pessoa e do livre-arbítrio".[88]

Essa vigilância realizada por meio do tratamento de dados não é visível aos vigiados. De acordo com Han, no panóptico digital, os indivíduos não se sentem vigiados ou ameaçados de qualquer forma, uma vez que esse dispositivo faz uso precisamente da revelação voluntária dos internos. Desse modo, o termo "Estado de vigilância" não seria apropriado para o contexto, já que os indivíduos participam de sua própria vigilância. Para Han, a vigilância e o controle são partes inerentes da comunicação social por meio das redes. Todos vigiam a todos.[89]

Han ainda observa que as constantes evoluções tecnológicas trazem tecnologias cada vez mais sofisticadas e que possuem a capacidade de vigilância, ainda que não tenham sido criadas especificamente para esse fim, consumando a sociedade de controle. É o caso da Internet das Coisas (*Internet of Things*)[90], que faz dos próprios objetos "agentes ativos de comunicação". "Somos agora observados, desse modo, também pelas coisas que usamos todo dia. [...] Elas participam ativamente do protocolamento total da vida".[91] Em suma, Han utiliza-se, principalmente, de 03 (três) termos para descrever essa sociedade dominada pelo panóptico digital: "sociedade da transparência", "sociedade da vigilância" e "sociedade de controle". Para o filósofo, essas sociedades se aproximam estruturalmente[92]. Pode-se dizer que a lógica da sociedade da transparência facilita o desenvolvimento de uma sociedade da vigilância total, o que, por sua vez, permite a consumação da sociedade de controle por meio do psicopoder – instrumentalizado pelo Big Data. A vigilância ubíqua e pervasiva é característica da sociedade contemporânea, como um instrumento para controle e administração da sociedade.

A psicopolítica, aparelhada pela vigilância digital, lê e controla pensamentos, estando em posição de intervir em processos psicológicos. O psicopoder vigia, controla e influencia o ser humano a partir de dentro. De acordo com Han, esse poder da sociedade de controle,

---

[88] HAN, Byung-Chul. **Psicopolítica**: O neoliberalismo e as novas técnicas de poder. Tradução de Maurício Liesen. Belo Horizonte: Âyiné, 2018. p. 23.
[89] HAN, Byung-Chul. **Psicopolítica**: O neoliberalismo e as novas técnicas de poder. Tradução de Maurício Liesen. Belo Horizonte: Âyiné, 2018. p. 57.
[90] O termo "Internet das Coisas" refere-se ao fenômeno de integração da tecnologia, Internet e capacidade de processamento em objetos do cotidiano. Objetos e eletrodomésticos até então "mundanos" se tornam agora conectados, sensitivos, automatizados e que possuem a capacidade de comunicação por meio da rede de Internet. Assim, a Internet não está mais limitada aos computadores, mas estende-se à objetos que em um primeiro momento não foram pensados para serem conectados. (THIERER, Adam D. **The Internet of Things and Wearable Technology**: Addressing privacy and security concerns without derailing innovation. In: Richmond Journal of Law and Technology, v. 21, n. 2, 2015, p. 5-7).
[91] HAN, Byung-Chul. **No enxame**: perspectivas do digital. Tradução de Lucas Machado. Petrópolis: Vozes, 2018. p. 126-127.
[92] HAN, Byung-Chul. **No enxame**: perspectivas do digital. Tradução de Lucas Machado. Petrópolis: Vozes, 2018. p. 122.

equipada com a vigilância, torna possível o acesso ao inconsciente-coletivo, podendo desenvolver traços totalitários, contrariamente ao que acreditava Foucault em relação ao poder disciplinar equipado com o dispositivo panóptico.[93]

Diante do exposto, observa-se que, apesar de seu exercício e suas finalidades terem sofrido mudanças significativas, a vigilância sempre possuiu um papel importante para a governança estatal e a manutenção de relações de poder. Para a finalidade a que se propõe a presente pesquisa, faz-se necessário delimitar um conceito de vigilância que possa ser aplicado independente da forma como ela venha a ser exercida, às tecnologias utilizadas como um instrumento para seu exercício, ou sua finalidade específica. Assim, no próximo tópico, realiza-se uma análise teórico-conceitual da vigilância.

2.2 CONCEITUAÇÃO DE VIGILÂNCIA

Por meio dessa breve e simplificada cronologia das relações entre Estado, poder e sociedade, o que se observa é que a vigilância é arcaica e foi utilizada como um instrumento de poder em muitas sociedades, em contextos e finalidades diversas e com maior ou menor grau de protagonismo, mas sempre como apoio à manutenção do poder exercido, principalmente – mas não somente –, pelo Estado. Isso porque, conforme explica Foucault, o poder necessita de instrumentos, técnicas e procedimentos que o mantenha, sendo um deles a formação de saber.[94] Todo saber possibilita e garante o exercício de um poder e todo exercício de poder é, ao mesmo tempo, um lugar ou momento de formação de saber. Essa é a relação poder/saber diretamente ligada aos sistemas de controle da sociedade moderna – mas que subsiste durante a passagem para a sociedade pós-moderna. O saber e o poder estão, portanto, intimamente relacionados, de modo que o agente do poder passa a ser um agente de constituição do saber.[95]

Para exemplificar essa relação, Foucault utiliza o exemplo da vigilância administrativa das populações, que é uma das necessidades de todo poder, segundo o filósofo. A vigilância administrativa, exercida para a manutenção do poder, dava ensejo a certos saberes sobre a população, os sujeitos vigiados, entre eles: um saber ligado à gestão da população, com o intuito de discriminar, por exemplo, quem deveria pagar os imposto, sobre quais produtos era

---

[93] HAN, Byung-Chul. **No enxame**: perspectivas do digital. Tradução de Lucas Machado. Petrópolis: Vozes, 2018. p. 134.
[94] FOUCAULT, Michel. **Em defesa da sociedade**: curso no Collège de France (1975-1976). Tradução de Maria Ermantina Galvão. 2. ed. São Paulo: WMF Martins Fontes, 2010. p. 26-30.
[95] FOUCAULT, Michel**. A sociedade punitiva**: curso no Collège de France (1972-1973). Tradução de Ivone C. Benedetti. São Paulo: WMF Martins Fontes, 2015. p. 212-213.

necessário impor taxas alfandegárias, quem precisava ser melhor vigiado para garantir que se pagasse os impostos devidos; um saber ligado à pesquisa da sociedade, que se relaciona diretamente com o exercício do biopoder e a elaboração de censos; e, um saber ligado à investigação policial.[96] O poder é gerado e exercido por meio da vigilância.[97]

Quando se fala em vigilância como um instrumento de poder não se está referindo à um ato ou elemento estático e imutável. A vigilância não consiste apenas no ato de observação ou monitoramento de um indivíduo ou população. Fernanda Bruno destaca 03 (três) aspectos recorrentes na história das práticas de vigilância, sendo eles: a observação, o conhecimento e a intervenção.[98] Importa destacar que a fase de observação se refere a qualquer modo de atenção ou monitoramento focalizado e sistemático, não necessariamente consistindo no ato visual da observação. Nesse sentido, talvez "atenção" ou "monitoramento" sejam termos mais apropriados para descrever a primeira fase ou elemento formador da prática de vigilância.

De modo geral, portanto, esses elementos – o monitoramento, o conhecimento e a intervenção – devem estar presentes para que a prática seja considerada vigilância. O monitoramento, como já mencionado, consiste na inspeção ou atenção regular, sistemática e focalizada sobre indivíduos ou populações, informações ou processos comportamentais, sejam corporais, psíquicos, sociais ou outros. Essa inspeção pode ser realizada de diferentes modos, seja de modo visual, mecânico, auditivo, eletrônico ou digital. Essa informação coletada deve permitir a produção de conhecimento, produção de um saber, sobre os sujeitos vigiados, podendo ser obtido de diversas formas, como a revelação de padrões, regularidades ou cadeias causais. Esse conhecimento é instrumental para que aquele em seu poder possa agir sobre escolhas, subjetividades e comportamentos daqueles sob vigilância, o que consiste no terceiro elemento desse processo: a intervenção. Para que um processo possa ser considerado vigilância, o monitoramento e a obtenção de conhecimento que dele derivam são insuficientes se não houver a intenção de agir sobre os indivíduos ou população.[99]

Seguindo os passos metodológicos de Fernanda Bruno[100], cabe aqui recuperar o conceito de dispositivo de Michel Foucault para melhor explicar e conceituar a vigilância. Foucault descreve o dispositivo elencando (03) três componentes que o constituem, seus traços

---

[96] FOUCAULT, Michel**. A sociedade punitiva**: curso no Collège de France (1972-1973). Tradução de Ivone C. Benedetti. São Paulo: WMF Martins Fontes, 2015. p. 212-213.
[97] LYON, David. **Surveillance Studies**: An Overview. Cambridge: Polity Press, 2007. P. 23.
[98] BRUNO, Fernanda. **Máquinas de ver, modos de ser**: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013. p. 18.
[99] BRUNO, Fernanda. **Máquinas de ver, modos de ser**: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013. p. 18.
[100] BRUNO, Fernanda. **Máquinas de ver, modos de ser**: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013. p. 19-21.

característicos: (i) um conjunto de elementos heterogêneos; (ii) uma função estratégica; (iii) jogos de poder e configurações de saber. Em primeiro lugar, portanto, o dispositivo é constituído de uma rede de elementos heterogêneos, que engloba "discursos, instituições, organizações arquitetônicas, decisões regulamentares, leis, medidas administrativas, enunciados científicos, proposições filosóficas, morais, filantrópicas". O que importa não é tanto os elementos em si, mas a rede que se estabelece por suas relações e as mudanças de posição e modificações de função pelas quais esses elementos passam. Em segundo lugar, o dispositivo tem sempre uma função estratégica, função essa que envolve responder a uma urgência em determinado momento histórico. Para explicar esse traço, Foucault usa o exemplo do dispositivo de controle-dominação da loucura, empregue em um momento histórico em que a economia mercantilista predominava, para controlar uma massa de população que se tornou incômoda: o doente mental. Como terceiro traço tem-se o distintivo do dispositivo: sua inserção em jogos de poder e ligado a configurações de saber que nascem do poder e o condiciona a um só tempo.[101]

Pode-se observar, a partir da noção de Foucault, que a vigilância se constitui como um dispositivo. Primeiramente porque a vigilância sempre se constituiu de uma série de práticas, discursos, instituições, empreendimentos científicos, projetos arquitetônicos, medidas legais e administrativas etc., e em sua forma contemporânea, torna-se ainda mais distribuída. Segundo porque a vigilância sempre teve uma função estratégica, que consistia no controle dos corpos e gestão da vida na sociedade moderna, e que consiste na segurança, controle e aumento de eficácia na sociedade contemporânea. E, por fim, porque a vigilância, seja em sua forma moderna ou contemporânea, é constituída por relações de poder e formações de saber.[102]

Nesse sentido, a vigilância pode ser conceituada, de forma abrangente, como um processo de atenção focalizada e sistemática de indivíduos, grupos de indivíduos, populações ou grupos de populações ou informações sobre eles, com o intuito de obter conhecimento que permita, finalmente, que se possa agir sobre os sujeitos vigiados, intervindo em comportamentos, escolhas e processos sociais e conduzindo suas condutas.[103] Essa atenção deve, necessariamente, ser sistemática e rotineira, no sentido de que não é ocasional, mas sim metódica e ordenada, ocorrendo constantemente, como parte do dia-a-dia.[104] Pode-se dizer,

---

[101] FOUCAULT, Michel. **Microfísica do poder**. Organização, introdução e revisão técnica de Roberto Machado. 11ª ed. São Paulo: Paz e Terra, 2021. p. 364-365.
[102] BRUNO, Fernanda. **Máquinas de ver, modos de ser**: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013. p. 19-21.
[103] BRUNO, Fernanda. **Máquinas de ver, modos de ser**: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013. p. 18.
[104] LYON, David. **Surveillance Studies**: An Overview. Cambridge: Polity Press, 2007. p.14.

portanto, que a vigilância é uma série de práticas que necessariamente se conectam com propósitos e, por isso, está diretamente relacionada ao exercício e manutenção do poder. Ainda, tendo em vista que o poder é exercido dentro de relações, a vigilância também envolve visibilidade, isto é, a autoexposição dos indivíduos de uma sociedade interfere na forma como a vigilância é percebida e entendida por aqueles que estão sendo vigiados, o que, por sua vez, impacta a forma como a vigilância é exercida, bem como seus efeitos.[105]

Apesar de haver muita divergência no que diz respeito à conceituação da vigilância dentro dos campos de estudo sobre essa temática, especialmente daquela que ocorre nas sociedades contemporâneas – como demonstram as obras "*Surveillance Studies: A reader*" editado por Torin Monahan e David Murakami Wood[106], e "*Routledge Handbook of Surveillance Studies*" editado por Kirstie Ball, Kevin Haggerty e David Lyon[107], as quais reúnem trabalhos de grandes estudiosos do tema –, em linhas gerais, muitos conceitos se aproximam desse aqui elaborado – com base na análise da Professora Fernanda Bruno –, em especial no que diz respeito ao primeiro e último elemento componentes da vigilância, anteriormente descritos.

A finalidade de intervenção ou controle sobre os sujeitos vigiados aparecem com frequência, portanto, em conceituações de vigilância. Para David Lyon, a vigilância pode ser considerada, de forma geral, como "a atenção focada, sistemática e rotineira aos detalhes pessoais para fins de influência, gestão, proteção ou direção" (tradução livre).[108] [109] James B. Rule et al. definem vigilância como "qualquer atenção sistemática à vida de uma pessoa com o objetivo de exercer influência sobre ela" (tradução livre).[110] [111] Para Gilliom e Monahan, a vigilância pode ser definida como "o monitoramento de pessoas para regular ou governar seu comportamento" (tradução livre)[112] [113]. Nas palavras de Gilliom, "a vigilância do comportamento humano existe para controlar o comportamento humano, seja limitando o acesso a programas ou instituições, monitorando e afetando o comportamento dentro dessas

---

[105] LYON, David. **Surveillance Studies**: An Overview. Cambridge: Polity Press, 2007. p.15-16.
[106] MONAHAN, Torin; WOOD, David Murakami (Ed.). **Surveillance Studies**: a reader. New York: Oxford University, 2018.
[107] BALL, Kirstie; HAGGERTY, Kevin D.; LYON, David (Ed.). **Routledge Handbook of Surveillance Studies**. London/New York: Routledge, 2012.
[108] LYON, David. **Surveillance Studies**: An Overview. Cambridge: Polity, 2007. p.14
[109] "*The focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction*"
[110] RULE, James B.; MCADAM, Douglas; STEARNS, Linda; UGLOW, David. Documentary Identification and Mass Surveillance in the United States. In: **Social Problems**, v. 31, n. 2, 1983. p. 222-234.
[111] "*Any systematic attention to a person's life aimed at exerting influence over it*".
[112] GILLIOM, John; MONAHAN, Torin. **SuperVision**: An introduction to the Surveillance Society. Chicago: The University of Chicago Press, 2013. p. 2
[113] "*Monitoring people in order to regulate or govern their behavior*".

arenas, ou aplicando regras e normas por meio da observação e registro de atos de conformidade e desvio" (tradução livre).[114] [115]

No entanto, existem aqueles, como Gary T. Marx, que entendem a vigilância apenas como o monitoramento ou coleta de dados, descartando a possibilidade de que a vigilância, de forma geral, apresente a finalidade de controle, para apreciar "novas" formas de vigilância que apresentam caráter bidirecional e horizontal, além do caráter vertical apresentado pelas demais posições.[116] Desse modo, para Marx, a vigilância de humanos (que pode ou não ser sinônimo de vigilância humana), pode ser considerada, em seu nível mais geral, como "observação ou atenção a outros (seja uma pessoa, um grupo ou um agregado como em um censo nacional) ou a fatores presumivelmente associados a estes. Uma característica central é a coleta de alguma forma de dado contestável a indivíduos (seja como indivíduos identificados ou como membros de uma categoria)" (tradução livre).[117] [118]

Gary T. Marx afirma que o conceito de vigilância deve ser dissociado da finalidade de controle na medida em que essa não é a única finalidade apresentada pelas práticas de vigilância existentes na sociedade, as quais podem ter por intuito a proteção ou o entretenimento, por exemplo, e que podem ser exercidas reciprocamente, bilateralmente, ainda que em uma relação em que existe hierarquia, já que em sociedades democráticas, com liberdades civis e políticas, há a coleta de dados e informações tanto "de baixo" quanto "de cima".[119]

Partindo dessa análise feita por Marx, há (03) três considerações a serem feitas. Inicialmente, quando se fala na finalidade de controle, deve-se considerar o termo controle não só como referência à dominação ou exploração, mas também como referência à administração e gestão, o que irá divergir dependendo do contexto em que a vigilância ocorre. Assim, quando se afirma que a vigilância tem como finalidade a intervenção ou o controle de comportamentos, escolhas e processos sociais envolvendo os sujeitos vigiados, estão aí inclusas as finalidades de

---

[114] GILLIOM, John. Overseers of the poor: Surveillance, resistance, and the limits of privacy. In: MONAHAN, Torin; WOOD, David Murakami (Ed.). **Surveillance Studies**: a reader. New York: Oxford University, 2018. p. 230-233. p. 230-231.

[115] *"Surveillance of human behavior is in place to control human behavior, whether by limiting access to programs or institutions, monitoring and affecting behavior within those arenas, or otherwise enforcing rules and norms by observing and recording acts of compliance and deviance".*

[116] MARX, Gary T. Surveillance Studies. In: **International Encyclopedia of the Social & Behavioral Sciences**, 2nd Ed., v. 23. Oxford: Elsevier, 2015. p. 733-741. p. 734-735.

[117] MARX, Gary T. Surveillance Studies. In: **International Encyclopedia of the Social & Behavioral Sciences**, 2nd Ed., v. 23. Oxford: Elsevier, 2015. p. 733-741. p. 734.

[118] *"Regard or attendance to others (whether a person, a group, or an aggregate as with a national census) or to factors presumed to be associated with these. A central feature is gathering some form of data connectable to individuals (whether as uniquely identified or as a member of a category)"*

[119] MARX, Gary T. Surveillance Studies. In: **International Encyclopedia of the Social & Behavioral Sciences**, 2nd Ed., v. 23. Oxford: Elsevier, 2015. p. 733-741. p. 735.

melhoria na prestação e gestão dos serviços públicos; dominação ou exploração de populações; controle de criminalidade; aumento de segurança pública, nacional ou privada; aumento de eficiência na prestação de serviços ou na produção de bens; direcionamento de marketing e aumento de lucros; proteção, entre outros. A especificidade da finalidade dependerá de diversos fatores como o contexto e os sujeitos envolvidos na atividade de vigilância.

Em segundo lugar, quando Marx fala em vigilância com a finalidade de entretenimento ele está se referindo aos regimes de visibilidade, referentes ao espetáculo e suas produções de subjetividades e regimes atencionais, presentes nos reality shows, setores do jornalismo e sites e aplicativos de compartilhamento de vídeo e imagem (redes sociais). Muitos estudiosos consideram esse um eixo dos processos de vigilância, no entanto, para o presente estudo e frente o conceito inicial anteriormente proposto, esses processos de atenção voltados ao entretenimento, tendo como agente ativo de "vigilância" o indivíduo em suas relações pessoais e no uso de redes sociais, não será considerado aqui como vigilância, já que essa atenção focalizada à vida e detalhes pessoais de conhecidos ou desconhecidos (figuras públicas), por meio das redes sociais ou programas de reality shows, não vem acompanhada de qualquer finalidade de intervenção na vida daqueles a quem ela está voltada, sendo uma atenção que tem por objetivo, como o próprio Marx diz, o entretenimento. Não se desconsidera aqui, no entanto, o papel que esse entretenimento tem na criação de subjetividades, de normalização e transformação da vigilância em "diversão, prazer, sociabilidade", e, finalmente, de legitimação da vigilância.[120] O espetáculo se torna um elemento da vigilância na medida em que incorpora "o olhar e a atenção vigilantes ao repertório cultural moderno e contemporâneo"[121], formando o que David Lyon chama de "cultura da vigilância"[122], mas sem que se possa caracterizar o espetáculo ou essa cultura vigilante como vigilância – no sentido da conceituação aqui colocada, qual seja, vigilância como um processo de atenção focalizada e sistemática com o intuito de obter conhecimento que permita agir sobre os sujeitos vigiados.

E, por fim, como terceira consideração, a questão da bilateralidade e reciprocidade da vigilância em determinados contextos de sociedades democráticas deve ser analisada cuidadosamente. Marx afirma que em sociedades democráticas, as quais possuem liberdades civis, a vigilância pode ocorrer de forma bilateral ou recíproca, já que os cidadãos (em relação ao Estado), consumidores (em relação aos fornecedores) ou trabalhadores (em relação a seus

---

[120] BRUNO, Fernanda. **Máquinas de ver, modos de ser**: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013. p. 34, 45-48.
[121] BRUNO, Fernanda. **Máquinas de ver, modos de ser**: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013. p. 22.
[122] LYON, David. **The culture of surveillance**: watching as a way of life. Cambridge/Medford: Polity, 2018.

superiores) têm acesso a dados mesmo estando em uma posição baixa em uma hierarquia.[123] No entanto, a capacidade de coleta, armazenamento e tratamento de dados de um indivíduo não pode ser comparada à capacidade de governos, corporações e empresas, que possuem maior poderio econômico e capacidade técnica. Há, necessariamente, uma assimetria de poder nas relações entre vigia e vigiado, entre quem coleta e trata dados pessoais e o titular de dados.[124] Feitas essas considerações, tem-se que o conceito de vigilância adotado na presente pesquisa envolve, necessariamente, relações hierárquicas e de poder. Ainda, para a correta compreensão da vigilância, especialmente a vigilância contemporânea, é necessário que se parta do pressuposto de que a vigilância é um processo e envolve uma série de mecanismos que se interrelacionam – sendo, portanto, um dispositivo.

Vale ressaltar que a vigilância possui um conceito único, seja ela inserida na sociedade moderna ou na sociedade contemporânea. No entanto, a vigilância moderna, das sociedades disciplinar e biopolítica, e a vigilância contemporânea, da sociedade de controle, devem ser diferenciadas, por mais que a última tenha suas linhagens na primeira e deva ser entendida dentro desse contexto histórico de mudança de uma sociedade para outra, pois elas possuem elementos diversos, funções diversas e relações de poder – e, portanto, formações de saber – diversas.[125] A sociedade de controle, portanto, faz uso do dispositivo da vigilância em suas relações de poder – onde o psicopoder toma protagonismo -, para criar um saber que possa ser utilizado para controlar e influenciar o ser humano – sua vida, vontades, decisões e comportamento - a partir de dentro.[126] Para que se possa compreender em sua totalidade a vigilância contemporânea, se faz necessário buscar os elementos heterogêneos que a compõem, bem como suas funções estratégicas e as relações de poder e formação de saber em que ela se insere.

2.3 TECNOPOLÍTICAS DE VIGILÂNCIA NA SOCIEDADE DE CONTROLE

Durante séculos a vigilância foi limitada à observação humana. Aos poucos, com o desenvolvimento de tecnologias, o escopo da vigilância foi se expandindo. Uma das diferenças

---

[123] MARX, Gary T. Surveillance Studies. In: **International Encyclopedia of the Social & Behavioral Sciences**, 2nd Ed., v. 23. Oxford: Elsevier, 2015. p. 733-741. p. 735.
[124] RICHARDS, Neil M. The danger of surveillance. In: **Harvard Law Review**, v. 126, pp. 1934-1965, 2013. p. 1952-1953.
[125] BRUNO, Fernanda. **Máquinas de ver, modos de ser**: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013. p. 21-22.
[126] HAN, Byung-Chul. **No enxame**: perspectivas do digital. Tradução de Lucas Machado. Petrópolis: Vozes, 2018. p. 134.

mais notáveis entre a vigilância moderna e a vigilância contemporânea é a pervasividade. O poder computacional transformou as técnicas de vigilância, difundindo esse dispositivo por variados contextos e relações de poder e criando novas subjetividades que a legitimam. De acordo com Roger Clarke, no final do século XX surgem novas formas de exercício de vigilância para além da vigilância física[127], da vigilância de localização e rastreamento[128], da vigilância de comunicações[129] e da vigilância corporal[130] já utilizadas durante a modernidade, entre elas: a vigilância de dados[131] (vigilância realizada por meio da coleta e tratamento de dados) e a vigilância omnipresente ou omnisciente[132]. Assim, a vigilância é exercida de forma massiva por meio de tecnologias com poder computacional, em diversos contextos e relações de poder e com diversas funções. Com a evolução computacional, a dissociação entre vigilância

[127] A vigilância física seria aquela exercida por meios visuais e auditivos para o monitoramento de indivíduos ou grupos de indivíduos por meio da observação de imagens e sons, a qual pode ser dividida em: observação por meio dos sentidos humanos, sem auxílios técnicos; a observação aprimorada pelo uso de tecnologias que auxiliem no monitoramento visual e auditivo; e a gravação – limitada no espaço e no tempo – de imagens e sons. (CLARKE, Roger. Information technology and dataveillance. In: **Communications of the ACM**, v. 31, n. 5, 1988. p. 498-512. p. 499).

[128] A vigilância de localização e rastreamento é a vigilância de pessoas ou grupos de pessoas realizada por meio do monitoramento de sua localização em algum espaço físico. Exercícios mais antigos dessa forma de vigilância envolviam a observação humana e a realização de perseguição e demarcação de localização. Com a democratização do computador pessoal e dispositivos móveis e o desenvolvimento de tecnologias como o GPS, essa forma de vigilância tornou-se mais sofisticada, uma vez que o monitoramento da localização de um ou mais indivíduos pode ser realizada de forma automatizada. (CLARKE, Roger. **A framework for surveillance analysis**. 16 feb. 2012. Disponível em: http://www.rogerclarke.com/DV/FSA.html. Acesso em: 07 out. 2021).

[129] A vigilância de comunicações refere-se ao monitoramento de indivíduos ou grupos de indivíduos por meio do monitoramento de mensagens ou outras formas de comunicação, como ligações ou mensagens gravadas. (CLARKE, Roger. Information technology and dataveillance. In: **Communications of the ACM**, v. 31, n. 5, 1988. p. 498-512. p. 499)

[130] O termo "vigilância corporal" refere-se à vigilância de pessoas focalizada em dados que revelem características corporais e/ou na medição direta de algum aspecto corporal desse indivíduo. Esse monitoramento pode incluir: a detecção e/ou o registro de dados referentes a características naturais de uma pessoa, como amostras de urina ou sangue para testes ou biometria facial, de íris e impressão digital; a detecção e/ou registro de dados pessoais sensíveis advindos de dispositivos móveis, objetos pessoais ou veículos; e a detecção e/ou registro de dados pessoais sensíveis advindos de recursos incorporados em um indivíduo, como bio-sensores implantados para coleta de sinais vitais, por exemplo. (CLARKE, Roger. **A framework for surveillance analysis**. 16 feb. 2012. Disponível em: http://www.rogerclarke.com/DV/FSA.html. Acesso em: 07 out. 2021).

[131] O termo "vigilância de dados" – ou *dataveillance*, em inglês – refere-se à vigilância de pessoas ou grupos de pessoas exercida por meio do uso sistemático de sistemas de dados pessoais. Segundo Roger Clarke, essa forma de vigilância pode se dar por meio do monitoramento de transações e por meio de técnicas como o *profiling, front-end verification* e *data matching*. Essa forma de vigilância e suas técnicas serão retomadas mais adiante nesse mesmo subtópico (CLARKE, Roger. Information technology and dataveillance. In: **Communications of the ACM**, v. 31, n. 5, 1988. p. 498-512. p. 499).

[132] Os termos "vigilância omnipresente" e "vigilância omnisciente" referem-se à aplicação integrada de múltiplas formas de vigilância, o que permite à vigilância exercida pela totalidade de um espaço, a todo tempo e que permite o saber completo sobre a pessoa ou grupo de pessoas vigiadas. (CLARKE, Roger. **A framework for surveillance analysis**. 16 feb. 2012. Disponível em: http://www.rogerclarke.com/DV/FSA.html. Acesso em: 07 out. 2021).

e tecnologia vai se tornando cada vez mais difícil. A tecnologia, como um instrumento, um meio, molda as técnicas de vigilância e é moldada por ela.[133]

O poder computacional transforma diversos aspectos do exercício da vigilância, os quais são a chave para compreender a extensão da vigilância contemporânea. Gary T. Marx elenca dez características compartilhadas pelas novas formas de vigilância que fazem possível diferenciar a vigilância contemporânea de formas mais antigas. Segundo o sociólogo, as dez características são:

> a) A primeira característica da "nova vigilância" consiste no fato de que ela transcende distância, escuridão e barreiras físicas. Diferentemente do que acontecia nas sociedades de soberania e nas sociedades disciplinares, barreiras físicas e psicológicas que se colocavam contra o exercício do poder e controle são agora penetráveis e os dados coletáveis podem ser transmitidos por longas distâncias. Ainda, a escuridão não é mais um impeditivo à "observação", tecnologias como a visão infravermelho ou visão noturna ou, ainda, o monitoramento por meio da coleta e tratamento de dados nas redes, retiram a preocupação com a visibilidade do alvo.[134]
>
> b) A segunda diz respeito ao tempo: a vigilância contemporânea transcende o tempo, na medida em que seus registros podem ser armazenados, combinados, analisados, comunicados, transferidos e recuperados, se fazendo disponível durante anos após a coleta.[135]
>
> c) A terceira característica diz respeito ao caráter preventivo da vigilância, que busca reduzir o risco e a incerteza, fazendo com que os fenômenos e comportamentos sociais sejam cada vez mais previsíveis, confiáveis e efetivos.[136]
>
> d) A sua baixa visibilidade ou invisibilidade, isto é, a falta de transparência da vigilância é sua quarta característica. Com a sofisticação das técnicas de vigilância, fica cada vez

---

[133] Isso não significa que todas as tecnologias utilizadas como instrumento para o exercício da vigilância são criadas para esse fim em específico, muitas vezes esse é um efeito potencial de uma tecnologia cuja função original é outra. De acordo com David Lyon, algumas capacidades dos sistemas tecnológicos fazem deles instrumentos atrativos para o exercício da vigilância em determinados contextos sociais, políticos e econômicos, uso que não havia sido planejado quando da criação da tecnologia. (LYON, David. **The Electronic Eye**: The rise of surveillance society. Cambridge: Polity, 1994. Kindle Edition. p. 9).

[134] MARX, Gary T. **Undercover**: Police surveillance in America. Berkeley/Los Angeles/London: University of California Press, 1988. p. 217.

[135] MARX, Gary T. **Undercover**: Police surveillance in America. Berkeley/Los Angeles/London: University of California Press, 1988. p. 217.

[136] MARX, Gary T. **Undercover**: Police surveillance in America. Berkeley/Los Angeles/London: University of California Press, 1988. p. 218.

mais difícil para um indivíduo ou grupo de indivíduos saber se está sendo vigiado, quando e por quem.[137]

e) A quinta característica refere-se ao caráter frequentemente involuntário assumido pela vigilância, ou seja, refere-se à capacidade de acesso à dados pessoais sem a participação e a consciência do vigiado. O que, por sua vez, se faz possível em razão da sexta característica.[138]

f) A sexta característica diz respeito ao autopoliciamento descentralizado, a participação do vigiado em seu próprio monitoramento, o qual é levado a fornecer vastas quantidades de dados pessoais "voluntariamente", bem como que fornece dados ao andar na rua, usar o telefone ou redes sociais, realizar compras na Internet e frequentar locais com controle de entrada e saída.[139]

g) Em razão dessa facilidade em vigiar, a sétima característica diz respeito a um caráter econômico, qual seja: a vigilância torna-se cada vez mais barata por unidade vigiada. Assim, tornou-se mais econômico para aquele que exerce a vigilância monitorar pessoas e situações que antes eram ignoradas.[140]

h) A oitava característica é a massificação da vigilância. Atualmente a vigilância é massificada, alcançando não só uma área maior, mas também áreas antes inalcançáveis, coletando uma quantidade de dados cada vez maior sobre um número cada vez maior de pessoas e tornando a vigilância parte do dia a dia das sociedades. O que antes era direcionado a indivíduos específicos, por razões específicas, agora é direcionado à toda uma população, envolvendo a suspeita categórica e generalizada, com a finalidade de identificar sujeitos que podem vir a ser considerados suspeitos, bem como restringir, influenciar e controlar o comportamento de todo o grupo.[141][142]

i) A nona característica é a continuidade da vigilância, o que faz, novamente, com que seu objeto passe de suspeitos específicos para a suspeita categórica de todos, ou todos

---

[137] MARX, Gary T. **Undercover**: Police surveillance in America. Berkeley/Los Angeles/London: University of California Press, 1988. p. 217-218.
[138] MARX, Gary T. **Undercover**: Police surveillance in America. Berkeley/Los Angeles/London: University of California Press, 1988. p. 218.
[139] MARX, Gary T. **Undercover**: Police surveillance in America. Berkeley/Los Angeles/London: University of California Press, 1988. p. 218.
[140] MARX, Gary T. **Undercover**: Police surveillance in America. Berkeley/Los Angeles/London: University of California Press, 1988. p. 218.
[141] MARX, Gary T. **Undercover**: Police surveillance in America. Berkeley/Los Angeles/London: University of California Press, 1988. p. 219.
[142] CLARKE, Roger. Information technology and dataveillance. In: **Communications of the ACM**, v. 31, n. 5, 1988. p. 498-512. p. 503.

> dentro de uma categoria específica. Todos se tornam alvos razoáveis, o que ajuda a consolidar uma sociedade onde todos são culpados até que se prove o contrário.[143]
>
> j) Por fim, a décima característica diz respeito ao caráter cada vez mais intenso e profundo da vigilância. Suas novas formas permitem que se tenha acesso a saberes mais abrangentes, penetrando não só no corpo, como também na psique.[144]

Por ser massificada e contínua, tem-se, também, que a vigilância direcionada para um sujeito, objeto ou processo específico e, portanto, com uma finalidade específica pode gerar, como subproduto, o monitoramento de outros sujeitos, objetos ou processos, do qual pode advir uma outra finalidade. Assim, seus efeitos não se limitam às intenções de quem monitora, as quais podem ser ultrapassados, produzindo efeitos imprevistos.[145]

A vigilância, portanto, torna-se universal na sociedade contemporânea, na medida em que se faz cada vez mais necessária como um meio de organização frente às crescentes complexidades do mundo pós-moderno. As transformações políticas, sociais e econômicas ocorridas durante o século XX impulsionaram o exercício da vigilância, bem como modificaram o imaginário da população sobre seus efeitos. Ainda na modernidade, o exercício da vigilância podia ser encontrado em variados contextos, como no setor comercial e industrial capitalistas, em setores dependentes de organização burocrática e na passagem da punição da população (sociedade de soberania) para a disciplina dos corpos e controle da alma (sociedade disciplinar).[146] Na pós-modernidade - ou na modernidade líquida de Bauman -, essa distribuição da vigilância se intensifica, instrumentalizada pelo poder computacional, tornando-se mais "móvel" e "flexível" e se espalhando por áreas em que antes exercia influência apenas periférica. No mesmo sentido do entendimento de Han, Bauman e Lyon afirmam a superação do dispositivo panóptico, uma vez que a arquitetura das tecnologias móveis por meio das quais o poder se afirma atualmente torna a arquitetura do panóptico redundante. Na sociedade contemporânea, a mobilidade e o nomadismo são valorizados e, dessa forma, as formas de controle exercidas pelo poder não tem conexão óbvia e direta com o aprisionamento como tinha

---

[143] MARX, Gary T. **Undercover**: Police surveillance in America. Berkeley/Los Angeles/London: University of California Press, 1988. p. 219.
[144] MARX, Gary T. **Undercover**: Police surveillance in America. Berkeley/Los Angeles/London: University of California Press, 1988. p. 219.
[145] BRUNO, Fernanda. **Máquinas de ver, modos de ser**: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013. p. 20.
[146] LYON, David. **Surveillance Studies**: An Overview. Cambridge: Polity, 2007. p. 4.

na sociedade moderna disciplinar.[147] A vigilância na sociedade pós-moderna caracteriza-se por sua liquidez, conforme explicam Bauman e Lyon:

> Velhas amarras se afrouxam à medida que fragmentos de dados pessoais obtidos para um objetivo são facilmente usados com outro fim. A vigilância se espalha de formas até então inimagináveis, reagindo à liquidez e reproduzindo-a. Sem um contêiner fixo, mas sacudida pelas demandas de "segurança" e aconselhada pelo marketing insistente das empresas de tecnologia, a segurança se esparrama por toda parte.[148]

No setor estatal, a vigilância é dividida em duas principais finalidades: controle e administração da população e policiamento e segurança. De forma geral, a vigilância sempre foi empregada para monitorar quem está e quem não está cumprindo regras, bem como para identificar e localizar os últimos.[149] A partir da crescente complexidade presente nas sociedades pós-modernas, bem como da introdução da noção de risco, a vigilância, instrumentalizada por novas tecnologias, é intensificada e distribuída, tornando-se massificada e contínua, dirigindo-se não mais a espaços ou grupos considerados suspeitos, mas para a totalidade da população. Assim, por ser utilizada como resposta a riscos sociais, a vigilância preditiva, com finalidade preventiva, assume protagonismo.[150][151]

Especialmente após os atentados ocorridos em 11 de setembro de 2001 em Nova Iorque, nos Estados Unidos, as preocupações ligadas à segurança nacional cresceram não só nesse país, mas também em todo o mundo, impulsionando a vigilância interna e internacional exercida por departamentos governamentais, como os serviços de inteligência, com a finalidade de segurança nacional, o que se tornou mais aparente com as revelações de Snowden.[152] Daí surgem duas grandes vias de legitimação do exercício da vigilância, ou seja, justificativas para seu exercício, que o tornam toleráveis ou desejáveis, sendo elas: a eficácia e a segurança. Eficácia porque, cada vez mais, a vigilância por meio de dados é realizada em busca de maior efetividade e rapidez na administração, gestão de políticas públicas e serviços públicos etc. E no campo da segurança, a lógica do risco – seja interno ou externo - legitima, e por vezes requer,

---

[147] BAUMAN, Zygmunt; LYON, David. **Vigilância líquida**. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2014. p. 6-7

[148] BAUMAN, Zygmunt; LYON, David. **Vigilância líquida**. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2014. p. 6.

[149] LYON, David. **The Electronic Eye**: The rise of surveillance society. Cambridge: Polity, 1994 (Kindle Edition). p. 91.

[150] MARX, Gary T. **Undercover**: Police surveillance in America. Berkeley/Los Angeles/London: University of California Press, 1988. p. 217-219.

[151] BRUNO, Fernanda. **Máquinas de ver, modos de ser**: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013. p. 8, 37-45.

[152] LYON, David. **The culture of surveillance**: Watching as a way of life. Cambridge/Medford: Polity, 2018. p. 20.

a instalação de uma série de dispositivos de vigilância com caráter preditivo e/ou preventivo, que monitoram e classificam sistematicamente as informações pessoais de populações inteiras no intuito de prever e prevenir atos criminosos e terroristas.[153]

Uma terceira via de legitimação advém das práticas de visibilidade, herança da cultura do espetáculo nascente na modernidade. Ao mesmo tempo em que os indivíduos da sociedade moderna eram um foco de monitoramento dos dispositivos disciplinares, eles eram também incitados por uma crescente cultura visual advinda das novas tecnologias de produção e reprodução da imagem (fotografia, cinema, estereoscópio etc.). Com o desenvolvimento das TIC esse regime de visibilidade foi enriquecido, conferindo novas significações sociais às práticas do ver e do ser visto, que ganham sentidos atrelados à reputação, admiração, desejo, pertencimento, conferindo uma significação prioritariamente positiva e desejável a práticas de visibilidade, o que incentiva a autoexposição e revelação voluntárias dos indivíduos nas redes, característica central do que Han chama de panóptico digital[154], isto é, a vigilância como dispositivo da sociedade digital de controle. Embora haja a presença de resistências nas três vias de legitimação, elas se alimentam e se apoiam, fazendo com que a vigilância seja normalizada, tolerada e, por vezes, até requerida.[155]

Nesse sentido, apesar da vigilância originalmente estar presente em instituições específicas como o exército, as corporações e departamentos governamentais, essas mudanças sociais, econômicas e políticas que causaram transformações tanto no exercício da vigilância, quanto em seus efeitos, fizeram com que a vigilância fosse distribuída e passasse a ser exercida em todas as áreas da vida.[156]

De acordo com David Lyon:

> Tudo isso ocorre dentro de um contexto cultural mais amplo no qual a aferição de riscos e oportunidades é central, a antecipação do futuro é um objetivo chave e, é claro, onde a prosperidade econômica e a segurança do Estado estão fechadas em um abraço mútuo. O resultado? A vigilância inteligente e a classificação social andam de mãos dadas. Cada clique do mouse, busca na web ou mensagem de texto emite uma exaustão de dados que é usado para criar perfis que, por sua vez, pontuam e classificam os usuários, colocando-os em categorias. Sutilmente, a vigilância inteligente e a classificação social informam e inspiram imaginários e práticas de vigilância, que por sua vez ajudam a permitir ou restringir o desenvolvimento futuro da vigilância inteligente. [...] Como as atitudes e ações se desenvolvem em relação a

[153] BRUNO, Fernanda. **Máquinas de ver, modos de ser**: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013. p. 37-45, 49.
[154] HAN, Byung-Chul. **Psicopolítica**: O neoliberalismo e as novas técnicas de poder. Tradução de Maurício Liesen. Belo Horizonte: Âyiné, 2018. p. 19, 57,
[155] BRUNO, Fernanda. **Máquinas de ver, modos de ser**: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013. p. 45-47.
[156] LYON, David. **The culture of surveillance**: Watching as a way of life. Cambridge/Medford: Polity, 2018. p. 5.

> isso faz a diferença entre simplesmente ver os ambientes de vigilância como convenientes e confortáveis - ou como desafiadores e contestáveis" (tradução livre).[157][158]

O desenvolvimento das TICs e do poder computacional assumem um papel essencial nesse processo de transformação da vigilância, influenciando e sendo influenciado pela própria vigilância. As TICs deram origem à forma de vigilância conhecida como *dataveillance*, abreviação de *data surveillance* – vigilância de dados em português –, termo cunhado por Roger Clarke e que, em suas palavras, refere-se ao processo de "uso sistemático de sistemas de dados pessoais na investigação ou no monitoramento das ações ou comunicações de uma ou mais pessoas" (tradução livre).[159] [160] Segundo o autor, essa forma de vigilância é essencialmente realizada por meio de computadores, "com a responsabilidade de 'vigiar e informar' delegada a um servo confiável e sempre vigilante" (tradução livre)[161], o que tornou a vigilância em massa automatizada e que foi substituindo, com o tempo, formas mais tradicionais de exercício de vigilância, por ser mais barata e eficaz.[162] [163] Essa nova forma de vigilância faz uso de uma variedade de técnicas e métodos de tratamento de dados para que se possa atingir os objetivos do exercício da vigilância em cada contexto, entre elas a técnica de *front-end verification*, que segundo ele diz respeito ao processo de "verificação cruzada de dados em um formulário de requerimento, contra dados de outros sistemas de dados pessoais, a fim de facilitar o processamento de uma transação" (tradução livre)[164]; a técnica de *computer matching* ou *data matching*, que consiste na "expropriação de dados mantidos por dois ou mais sistemas de dados pessoais, a fim de fundir dados previamente separados sobre um grande número de indivíduos"

---

[157] LYON, David. **The culture of surveillance**: Watching as a way of life. Cambridge/Medford: Polity, 2018. p. 21.

[158] "*All this occurs within a wider cultural context in which gauging risk and opportunity is central, anticipating the future is a key goal, and of course where economic prosperity and state security are locked in a mutual embrace. The result? Smart surveillance and social sorting go hand in glove. Every mouse click, web search or text message gives off data exhaust that is used to create profiles which in turn score and rank users, placing them in consequential categories. Subtly, smart surveillance and social sorting inform and inspire surveillance imaginaries and practices, which in turn help to enable or constrain the further development of smart surveillance. […] How attitudes and actions develop in relation to this makes the difference between simply seeing surveillant environments as convenient and comfortable – or as challenging and contestable."*

[159] CLARKE, Roger. Information technology and dataveillance. In: **Communications of the ACM**, v. 31, n. 5, 1988. p. 498-512. p. 499.

[160] *"Systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons".*

[161] *"With the 'watch and report' responsibility delegated to a reliable, ever-wakeful servant"*

[162] CLARKE, Roger. Information technology and dataveillance. In: **Communications of the ACM**, v. 31, n. 5, 1988. p. 498-512. p. 501.

[163] CLARKE, Roger. Profiling: a hidden challenge to the regulation of data surveillance. In: **Journal of Law and Information Science**, v. 4, n.2, Dec. 1993. Disponível em: http://www.rogerclarke.com/DV/PaperProfiling.html. Acesso em: 10 set. 2021.

[164] "*Cross-checking of data in an application form, against data from other personal data systems, in order to facilitate the processing of a transaction*".

(tradução livre)[165]; e a técnica de *profiling*, que diz respeito ao processo "no qual um conjunto de características de uma determinada classe de pessoas é inferido a partir da experiência passada, e, posteriormente, indivíduos que possuem uma proximidade com esse conjunto de características determinado são procurados em uma base de dados, com o intuito de classificá-lo" (tradução livre)[166] [167] [168] [169]

À medida que fontes de dados se tornaram mais acessíveis e móveis e seu processamento mais rápido e barato, a vigilância de dados foi alcançando mais espaço. O crescente uso de dispositivos móveis pela população criou um grande potencial para o exercício da vigilância por meio da coleta e tratamento de dados, uma vez que facilitou a coleta em massa de dados, aumentando a capacidade de vigilância. Um dos traços distintivos dessa vigilância é a capacidade de transformar dados brutos em informação e conhecimento, a partir dos quais se pode agir.[170] Na sociedade de controle todo tipo de dado sobre as vidas dos indivíduos é coletado, tratado e armazenado em grandes bases de dados pertencentes à governos e corporações, fenômeno que dá origem à sociedade da vigilância e, posteriormente, à cultura da vigilância, onde a vigilância é fluida, líquida. Essa forma de vigilância se beneficia dos rastros digitais deixados pelos indivíduos ao utilizar redes sociais ou realizar transações por meio da Internet.[171] Os vigiados, muito comumente, não sabem quem os está vigiando, para quais finalidades, que tipo de dados eles possuem e com quem esses dados são compartilhados.[172] Na sociedade de controle contemporânea, onde a vigilância é massivamente distribuída e está presente em diferentes contextos e relações de poder, há a criação de uma lógica de registro total da vida. Viver em sociedade na contemporaneidade significa estar sob vigilância.[173] Nas palavras de Byung-Chul Han:

---

[165] "*expropriation of data maintained by two or more personal data systems, in order to merge previously separate data about large numbers of individuals*".
[166] "*whereby a set of characteristics of a particular class of person is inferred from past experience, and data-holdings are then searched for individuals with a close fit to that set of characteristics*".
[167] CLARKE, Roger. **Introduction to dataveillance and information privacy, and definitions of terms**. July 2016. Disponível em: http://www.rogerclarke.com/DV/Intro.html#DV. Acesso em: 10 set. 2021.
[168] CLARKE, Roger. Information technology and dataveillance. In: **Communications of the ACM**, v. 31, n. 5, 1988. p. 498-512. p. 501.
[169] CLARKE, Roger. Profiling: a hidden challenge to the regulation of data surveillance. In: **Journal of Law and Information Science**, v. 4, n.2, Dec. 1993. Disponível em: http://www.rogerclarke.com/DV/PaperProfiling.html. Acesso em: 10 set. 2021.
[170] CLAVELL, Gemma Galdon. Dataveillance. In: ARRIGO, Bruce A. (Ed.). **The SAGE encyclopedia of surveillance, security, and privacy**. V.1. Thousand Oaks: SAGE, 2018. pp. 284-285. P. 285.
[171] CLARKE, Roger. **Dataveillance**: 15 years on. March 2003. Disponível em: http://www.rogerclarke.com/DV/DVNZ03.html. Acesso em: 10 set. 2021.
[172] LYON, David. **The culture of surveillance**: Watching as a way of life. Cambridge/Medford: Polity, 2018. p. 3.
[173] LYON, David. **The culture of surveillance**: Watching as a way of life. Cambridge/Medford: Polity, 2018. p. 4.

> Todo clique que eu faço é salvo. Todo passo que eu faço é rastreável. Deixamos os rastros digitais em todo lugar. Nossa vida digital se forma de modo exato na rede. A possibilidade de um protocolamento total da vida substitui a confiança inteiramente pelo controle. No lugar do Big Brother, entra o Big Data.[174]

À medida que a vigilância exercida por governos e corporações se torna mais intensa e distribuída, bem como que uma cultura vigilantista se desenvolve no meio digital, a vigilância se torna parte do dia a dia da vida em sociedade e novas subjetividades e maneiras de percepção dessa vigilância pelos próprios vigiados são criadas. A vigilância na sociedade de controle contemporânea, portanto, depende dessa participação dos vigiados, os quais vivem na ilusão da liberdade e são incentivados a manter uma hipercomunicação que municia o panóptico digital com dados pessoais expostos voluntariamente e intencionalmente - ou não -, tornando o controle total da vida possível. Essa é a consumação da sociedade de controle, segundo Han, pois os habitantes do panóptico digital "se comunicam não por coação exterior, mas sim por carência interna, onde, então, o medo de ter de abdicar de sua esfera privada e íntima dá lugar à carência de se colocar desavergonhadamente à vista [...]"[175], participando, dessa forma, de seu próprio monitoramento, uma das características da nova vigilância citada por Marx (o autopoliciamento descentralizado).[176] Nas palavras de David Lyon, "a vigilância de hoje é possível através de nossos próprios cliques em websites, nossas mensagens de texto e troca de fotos. As pessoas comuns contribuem para a vigilância como nunca antes. O conteúdo gerado pelo usuário gera os dados através dos quais as ações diárias são monitoradas". (tradução livre).[177] [178]

Essa conjunção de fatores forma o que Lyon denomina cultura de vigilância, que consiste na forma como a vigilância é possibilitada não só por meio de tecnologias e tecnopolíticas, mas também pelo entusiasmo, ignorância e, por vezes, cooperação – relutante ou não – e iniciativa dos vigiados.[179] A noção do desenvolvimento de uma cultura da vigilância é essencial para se entendê-la no contexto da sociedade digital de controle, pois desempenha

---

[174] HAN, Byung-Chul. **No enxame**: perspectivas do digital. Tradução de Lucas Machado. Petrópolis: Vozes, 2018. p. 122.
[175] HAN, Byung-Chul. **No enxame**: perspectivas do digital. Tradução de Lucas Machado. Petrópolis: Vozes, 2018. p. 77.
[176] MARX, Gary T. **Undercover**: Police surveillance in America. Berkeley/Los Angeles/London: University of California Press, 1988. p. 217-218.
[177] LYON, David. **The culture of surveillance**: Watching as a way of life. Cambridge/Medford: Polity, 2018. p. 2.
[178] "*today's surveillance is made possible by our own clicks on websites, our texting messages and exchanging photos. Ordinary people contribute to surveillance as never before. User-generated content engenders the data by which daily doings are monitored*".
[179] LYON, David. **The culture of surveillance**: Watching as a way of life. Cambridge/Medford: Polity, 2018. p. 30.

um papel importante em instruir os imaginários sociais sobre essas práticas, bem como em facilitar a aceitação, a tolerância e a normalização dessas práticas exercidas em contextos políticos e econômicos.[180] Trazendo como um exemplo marcante da cultura da vigilância, Lyon cita o aplicativo de jogo para celular, *Angry Birds*:

> Jogar Angry Birds, por exemplo, é visto como um aliviador do estresse e se tornou extremamente popular devido à sua simplicidade, recompensas, humor e previsibilidade. Interagir com um jogo como esse em um dispositivo móvel enquanto, digamos, desloca-se pela cidade em um ônibus ou carro pode ser culturalmente representado como diversão inocente. No entanto, o jogo é orientado por seus projetistas para identificar e influenciar os jogadores mais propensos a aderir aos aspectos pagos do jogo, em vez de jogar de graça. E isso é apenas o lado da vigilância do consumidor. Entre os primeiros vazamentos de Snowden estava um documento mostrando como a agência de segurança das comunicações do Reino Unido, a GCHQ (Government Communications Headquarters), utiliza 'aplicativos com vazamento', como o Angry Birds, para obter dados sensíveis sobre a idade, sexo, localização e até mesmo orientação sexual dos jogadores. (tradução livre).[181] [182]

Conforme o exercício da vigilância torna-se cada vez mais ubíquo e pervasivo, não só os imaginários sociais apresentam divergências, como também os efeitos da vigilância na sociedade são variados, o que significa que essa massificação e alta penetração no dia a dia da vida em sociedade não se traduz, necessariamente, em efeitos totalmente negativos ou positivos. Como já citado, a vigilância não é inerentemente boa ou ruim, apesar de também não ser neutra, sendo sempre ambígua, isto é, sistemas de vigilância podem ser implementados para garantir o pagamento correto de benefícios sociais aos cidadãos, para prevenir ataques terroristas, garantir a segurança pública, gestar políticas públicas etc., mas também podem apresentar danos aos cidadãos. Esses mesmos sistemas também são utilizados como meio para controle social, na medida em que criam assimetrias de poder entre os vigilantes e os vigiados[183], especialmente a vigilância exercida por corporações e organizações governamentais, as quais estão intimamente interligadas, uma vez que as corporações não só realizam a vigilância em larga-escala de seus

---

[180] LYON, David. **The culture of surveillance**: Watching as a way of life. Cambridge/Medford: Polity, 2018. p. 17.

[181] LYON, David. **The culture of surveillance**: Watching as a way of life. Cambridge/Medford: Polity, 2018. p. 17.

[182] *"Playing Angry Birds, for example, is seen as a stress reliever and became wildly popular due to its simplicity, rewards, humour and predictability. Interacting with such a game on a mobile device while, say, commuting by bus or streetcar may be culturally represented as innocent fun. However, the game is geared by its designers to identifying and grooming those players most likely to buy-in, rather than to play for free. And that is only the consumer surveillance side. Early among the Snowden releases was a document showing how the United Kingdom's communications security agency, GCHQ (Government Communications Headquarters), taps into 'leaky apps' such as Angry Birds for sensitive data on the age, gender, location and even sexual orientation of players"*

[183] LYON, David. **The Electronic Eye**: The rise of surveillance society. Cambridge: Polity, 1994 (Kindle Edition). p. 4-5, 92.

consumidores, mas também compartilham dados e tecnologias com capacidade de vigilância para instruir tecnopolíticas implementadas por agências governamentais, fazendo com que o exercício da vigilância adquira o caráter de uma grande indústria.[184] Segundo Han, "atualmente, os *big data* não se manifestam apenas na forma do Grande Irmão, mas também de um *big deal*", ou seja, o Estado de vigilância e o mercado se tornem um só. [185]

Essa vigilância de dados, embora seja feita remotamente, de forma generalizada e de difícil percepção por parte dos vigiados, e embora, por vezes, produza efeitos considerados positivos, pode produzir consequências reais para as experiências e as chances de vida das pessoas vigiadas, tendo em vista que conclusões, decisões e julgamentos são feitos com base no perfil pessoal criado por meio da análise dos dados pessoais coletados, causando um impacto desproporcional sobre as vidas das minorias. Nesse sentido, para Han, o Big Data introduz uma nova sociedade de classes digital, pois, segundo ele:

> Quem está na categoria lixo pertencem à classe mais baixa. Aos indivíduos com pontuação ruim são negados empréstimos. Logo, junto ao pan-óptico surge um «ban-óptico». O pan-óptico monitora os internos incluídos no sistema. O ban-óptico é um dispositivo que identifica como indesejadas as pessoas estranhas ou hostis ao sistema e as exclui (em inglês: *to ban*). O pan-óptico clássico serve para disciplinar; os ban-ópticos garantem a segurança e a eficiência do sistema.[186]

Assim, surge a preocupação com as tendências totalitários que essas tecnopolíticas de vigilância podem apresentar, já que, segundo Han, "a sociedade digital de vigilância, que tem acesso ao inconsciente-coletivo, ao comportamento social futuro das massas, [...] nos entrega à programação e ao controle psicopolíticos". Ressalta-se que esses sistemas podem, dependendo do contexto e da finalidade em que são utilizados, bem como das relações de poder em que estão envolvidos e dos efeitos previstos e não previstos a que dão origem, ultrapassar limites legais estabelecidos para a proteção dos direitos à privacidade e à proteção de dados pessoais. Desse modo, faz-se necessário a análise dos riscos que essas tecnopolíticas apresentam para esses direitos e para as liberdades que deles derivam, pilares de uma sociedade livre e democrática.

---

[184] LYON, David. **The culture of surveillance**: Watching as a way of life. Cambridge/Medford: Polity, 2018. p. 13-14.
[185] HAN, Byung-Chul. **Psicopolítica**: O neoliberalismo e as novas técnicas de poder. Tradução de Maurício Liesen. Belo Horizonte: Âyiné, 2018. p. 90.
[186] HAN, Byung-Chul. **Psicopolítica**: O neoliberalismo e as novas técnicas de poder. Tradução de Maurício Liesen. Belo Horizonte: Âyiné, 2018. p. 91.

2.4 OS EFEITOS NEGATIVOS DAS TECNOPOLÍTICAS DE VIGILÂNCIA NA SOCIEDADE

Como já mencionado no início desse capítulo, a vigilância e o controle social estão presentes – e são necessários – em todos os Estados democráticos. Nas sociedades contemporâneas, nas quais há intensa dispersão geográfica, diversidade cultural e segmentação social, o controle social, especialmente esse exercido por meio de tecnologias, é desejável para que se possa reproduzir os valores da sociedade por toda sua extensão, bem como manter a coesão social e garantir os direitos e garantias fundamentais aos seus titulares.[187] Os Estados necessitam de informações sobre os cidadãos para fins de discriminação entre quem pode ou não votar, quem possui determinados direitos e obrigações, quem tem direito a benefícios sociais, quem pagará determinados impostos, quais políticas públicas são necessárias e para quais fins, e assim por diante. Essa necessidade de identificação e discriminação de cidadãos entre populações é um dos fatores que contribui para a instalação de sistemas informacionais e tecnopolíticas de vigilância em sociedades diversas – além da instalação de sistemas de tecnopolíticas de vigilância para fins de segurança nacional e pública, como um meio de fazer com que problemas e atos criminosos sejam "legíveis" para as autoridades antes mesmo de acontecerem, visando a prevenção dos crescentes riscos nas sociedades. Nesse sentido, a vigilância é um componente essencial da democracia e das formas liberais de governança.[188]

Um dos aspectos fundamentais da vigilância contemporânea, como anteriormente mencionado, é sua íntima relação com as novas tecnologias. O *Big Data* mudou o foco da vigilância de fixa para líquida.[189] Assim, o exercício da vigilância na contemporaneidade é em muito instrumentalizado pelo *Big Data*, na medida em que o monitoramento de pessoas por meio da coleta e tratamento de dados pessoais se torna a forma dominante de exercício da vigilância, fenômeno a que Roger Clarke denomina *dataveillance*[190], conforme já mencionado no item 1.3. Para Han, a vigilância digital é mais eficiente que aquela analógica, tendo em vista que o *Big Data* liberta o monitoramento de ópticas perspectivistas, na medida em que:

---

[187] MONAHAN, Torin. Social inequality and the pursuit of democratic surveillance. In: HAGGERTY, Kevin D.; SAMATAS, Minas. (Ed.). **Surveillance and Democracy**. Abingdon/New York: Routledge, 2010. p. 91-110. p. 105-106.

[188] HAGGERTY, Kevin D.; SAMATAS, Minas. Surveillance and democracy: an unsettled relationship. In: HAGGERTY, Kevin D.; SAMATAS, Minas. (Ed.). **Surveillance and Democracy**. Abingdon/New York: Routledge, 2010. p. 1-16. P. 7.

[189] LYON, David. **The culture of surveillance**: Watching as a way of life. Cambridge/Medford: Polity Press, 2018. p. 5, 21.

[190] CLARKE, Roger. Information technology and dataveillance. In: **Communications of the ACM**, v. 31, n. 5, 1988. p. 498-512. p. 499.

> Os big data sugerem um conhecimento absoluto. Tudo é mensurável e quantificável. As coisas revelam suas correlações secretas, que até então estavam ocultas. Do mesmo modo, o comportamento humano também deve ser previsível. Uma nova era de conhecimento é anunciada. As correlações substituem a causalidade. O é assim mesmo substitui o por quê. A quantificação da realidade movida a dados afasta completamente o espírito do conhecimento.[191]

A vigilância contemporânea é fortemente dependente de bases de dados digitais, tendo em vista que essas são utilizadas para armazenar e permitir o tratamento de dados coletados durante o monitoramento realizado no exercício da vigilância, seja governamental ou privada.[192] Essas bases de dados, sejam elas centralizadas ou não, são o que permitem que diferentes algoritmos possam ser aplicados, seja para descobrir padrões ou determinar correlações entre conjuntos de dados, estabelecendo perfis, que representam pessoas ou grupos de pessoas e identificando padrões de comportamento que podem ser utilizados para predição de comportamentos – para fins de influência –, bem como para a tomada de decisão que influenciará as oportunidades (*life chances)* de indivíduos ou grupos de indivíduos.[193] [194] Nesse sentido, os dados abstratos coletados nos processos de *dataveillance* são tratados por meio de uma variedade de métodos e técnicas - como a Mineração de Dados*, data matching, profiling* etc.*[195]* -, para que sejam ordenados e classificados e para que padrões e correlações sejam determinados, produzindo classificações, perfis ou predições, que auxiliam nos processos de influenciar e administrar populações e indivíduos, gerando conhecimento sobre os sujeitos ou objetos da vigilância e determinando, por exemplo, quem tem direito a tratamento especial, quem será considerado um suspeito, quem é elegível, quem será incluído e terá acesso a bens e serviços e quem será excluído dessas oportunidades, quais áreas serão mais intensamente policiadas e etc., prevendo padrões comportamentais e prevenindo riscos, sejam eles quais forem, e, consequentemente, afetando, direta e indiretamente, as escolhas e oportunidades (*life chances*) desses sujeitos.[196]

---

[191] HAN, Byung-Chul. **Psicopolítica**: O neoliberalismo e as novas técnicas de poder. Tradução de Maurício Liesen. Belo Horizonte: Âyiné, 2018. p. 93.
[192] LYON, David. **The Electronic Eye**: The rise of surveillance society. Cambridge: Polity Press, 1994 (Kindle Edition). p.8
[193] CLARKE, Roger. Information technology and dataveillance. In: **Communications of the ACM**, v. 31, n. 5, 1988. p. 498-512. p. 501.
[194] CLARKE, Roger. Profiling: a hidden challenge to the regulation of data surveillance. In: **Journal of Law and Information Science**, v. 4, n.2, Dec. 1993. Disponível em: http://www.rogerclarke.com/DV/PaperProfiling.html. Acesso em: 10 set. 2021.
[195] CLARKE, Roger. Information technology and dataveillance. In: **Communications of the ACM**, v. 31, n. 5, 1988. p. 498-512. p. 502-505.
[196] LYON, David. Surveillance as social sorting: computer codes and mobile bodies. In: LYON, David (Ed.). **Surveillance as social sorting**: privacy, risk, and digital discrimination. London/New York: Routledge, 2003. p. 13-30. p. 13-14, 20.

O *profiling*[197] é uma das técnicas muito utilizadas na vigilância de pessoas por meio da coleta de dados, a qual é definida por Roger Clarke como "uma técnica na qual um conjunto de características de uma determinada classe de pessoas é inferido a partir da experiência passada, e, posteriormente, indivíduos que possuem uma proximidade com esse conjunto de características determinado são procurados em uma base de dados, com o intuito de classificá-lo" (tradução livre).[198] [199] Hildebrandt, por sua vez, define *profiling* como sendo "o processo de 'descoberta' de correlações entre dados em bancos de dados que podem ser usados para identificar e representar um sujeito humano ou não (indivíduo ou grupo) e/ou a aplicação de perfis (conjuntos de dados correlatos) para individuar e representar um sujeito ou para identificar um sujeito como membro de um grupo ou categoria" (tradução livre).[200] [201] Ainda, segundo a autora, o objetivo da técnica consiste na "avaliação dos riscos e/ou oportunidades para o controlador de dados (em relação aos riscos e oportunidades referentes ao indivíduo em questão)" (tradução livre).[202] [203] Assim, essa técnica é utilizada com o intuito de determinar atributos relevantes dentro de determinado contexto, auxiliando, dessa forma, na representatividade estatística, isto é, "na determinação da qualidade de uma amostra constituída de modo a corresponder à população no seio da qual ela é escolhida".[204]

A vigilância, como já mencionado, pode ser necessária – e ter efeitos positivos –, tanto no setor governamental, quanto no setor privado, para fins de administração e controle. Ainda, as técnicas de tratamento de dados utilizadas na vigilância são também empregadas nos mais

---

[197] Ressalta-se que o termo aqui utilizado se refere ao *profiling* automatizado, ou seja, o *profiling* que é resultante de um processo de mineração de dados, que, segundo Hildebrandt, consiste no processo "*by which large databases are mined by means of algorithms for patterns of correlations between data*". (HILDEBRANDT, Mireille. Defining profiling: a new type of knowledge? In: HILDEBRANDT, Mireille; GUTWIRTH, Serge (Ed). **Profiling the European Citizen**: cross-disciplinary perspectives. Berlin: Springer, 2008. p. 17-45. p. 18).

[198] CLARKE, Roger. Profiling: a hidden challenge to the regulation of data surveillance. In: **Journal of Law and Information Science**, v. 4, n.2, Dec. 1993. Disponível em: http://www.rogerclarke.com/DV/PaperProfiling.html. Acesso em: 10 set. 2021.

[199] "*A technique whereby a set of characteristics of a particular class of persons is inferred from past experience, and data-holding are then searched for individual with a close fit to the set of characteristics*".

[200] HILDEBRANDT, Mireille. Defining profiling: a new type of knowledge? In: HILDEBRANDT, Mireille; GUTWIRTH, Serge (Ed). **Profiling the European Citizen**: cross-disciplinary perspectives. Berlin: Springer, 2008. p. 17-45. p. 19.

[201] *"The process of 'discovering' correlations between data in databases that can be used to identify and represent a human or nonhuman subject (individual or group) and/or the application of profiles (sets of correlated data) to individuate and represent a subject or to identify a subject as a member of a group or category"*

[202] HILDEBRANDT, Mireille. Defining profiling: a new type of knowledge? In: HILDEBRANDT, Mireille; GUTWIRTH, Serge (Ed). **Profiling the European Citizen**: cross-disciplinary perspectives. Berlin: Springer, 2008. p. 17-45. p. 20.

[203] "The *assessment of risks and/or opportunities for the data controller (in relation to risks and opportunities concerning the individual subject*)".

[204] FREITAS, Cinthia Obladen de Almendra. Tratamento de dados pessoais e a legislação brasileira frente ao *profiling* e à discriminação a partir das novas tecnologias. In: **Revista de Direito, Governança e Novas Tecnologias**, v.3, n.2, 2017. p. 18-38. p. 27-28.

variados sistemas, serviços e empresas para dar conta da crescente complexidade derivada da torrente de informações disponíveis atualmente, em contextos que exigem que contínuas escolhas de ação sejam feitas e que demandam uma certa previsibilidade para enfrentamento dos crescentes riscos da sociedade pós-moderna.[205] [206] No entanto, a vigilância por meio da coleta massiva de dados, por sua própria natureza, é invasiva e pode vir a ameaçar direitos.[207]

A preocupação com a privacidade, que pode ser considerada como a violação mais imediata causada por qualquer tipo de vigilância, deve ser estendida para à sua relação direta com o exercício e garantia de outros direitos fundamentais. A vigilância massiva produz desequilíbrios de poder significativos em relação ao vigia e os vigiados, dando poder de influência e controle ao vigia sobre o vigiado e causando violações de diversos direitos e garantias fundamentais dos cidadãos, como, por exemplo, a violação de liberdades civis e do direito à não discriminação.[208] Esse desequilíbrio de poder vem de uma assimetria existente na relação entre aqueles que coletam e tratam grandes quantidades de dados e aqueles que são alvos dessa coleta (os titulares de dados), tanto em relação ao acesso à grandes quantidades de dados, quanto em relação ao seu processamento e uso. Essa assimetria é o que Mark Andrejevic chama de "*big data divide*", que se relaciona não só com o poder de quem tem acesso à bancos de dados e ao poder de processamento, mas também com os processos de classificação assimétricos e as diferentes formas de se pensar sobre como os dados se relacionam com o conhecimento e sua aplicação.[209] Nesse sentido, Andrejevic observa que:

> A sensação de impotência que os indivíduos expressam sobre as formas emergentes de coleta e mineração de dados reflete tanto as relações de propriedade e controle que moldam o acesso aos recursos de comunicação e informação, quanto a crescente consciência de quão pouco as pessoas sabem sobre as maneiras pelas quais seus dados podem ser usados contra elas (tradução livre).[210] [211]

---

[205] FREITAS, Cinthia Obladen de Almendra. Tratamento de dados pessoais e a legislação brasileira frente ao *profiling* e à discriminação a partir das novas tecnologias. In: **Revista de Direito, Governança e Novas Tecnologias**, v.3, n.2, 2017. p. 18-38. p. 28.

[206] HILDEBRANDT, Mireille. Defining profiling: a new type of knowledge? In: HILDEBRANDT, Mireille; GUTWIRTH, Serge (Ed). **Profiling the European Citizen**: cross-disciplinary perspectives. Berlin: Springer, 2008. p. 17-45. p. 24.

[207] CLARKE, Roger. Information technology and dataveillance. In: **Communications of the ACM**, v. 31, n. 5, 1988. p. 498-512. p. 506.

[208] RICHARDS, Neil M. The danger of surveillance. In: **Harvard Law Review**, v. 126, 2013. p. 1934-1965. p. 1952-1953.

[209] ANDREJEVIC, Mark. The big data divide. In: **International Journal of Communication**, v. 8, 2014, p. 1673-1689. p. 1675.

[210] ANDREJEVIC, Mark. The big data divide. In: **International Journal of Communication**, v. 8, 2014, p. 1673-1689. p. 1675.

[211] "*The sense of powerlessness that individuals express about emerging forms of data collection and data mining reflects both the relations of ownership and control that shape access to communication and information resources, and growing awareness of just how little people know about the ways in which their data might be turned back upon them*".

À medida que a vigilância aumenta em quantidade e sofisticação, seu potencial de discriminação também cresce, o que levanta preocupações a respeito do que David Lyon chama de "*social sorting*".[212] O termo "*social sorting"*, cunhado por David Lyon, evidencia os efeitos discriminatórios facilitados pelo ímpeto classificatório que a vigilância contemporânea apresenta, referindo-se, particularmente, às formas como a vigilância em massa facilitam o desenvolvimento e o uso de técnicas de classificação ou categorização social (*profiling*) e os impactos que essas técnicas exercem na sociedade.[213][214] Segundo o autor, "*social sorting*" refere-se ao "meio de verificar identidades, mas também de avaliar riscos e atribuir valor" (tradução livre).[215] [216] De acordo com Monahan, a vigilância opera como um mecanismo de diferenciação social, discernindo grupos ou indivíduos de uma população por meio de atributos específicos e os governando de acordo com essa classificação.[217] A vigilância é exercida de maneira desproporcional entre grupos sociais diferentes, exercendo um poder de controle diferencial (*differential control,* nas palavras de Monahan[218]) de acordo com os atributos de cada segmento da população, produzindo efeitos desproporcionais em grupos específicos, de acordo com seu perfil informacional ou *data double*[219].[220]

Nesse sentido, segundo Haggerty e Ericson:

---

[212] CLAVELL, Gemma Galdon. Dataveillance. In: ARRIGO, Bruce A. (Ed.). **The SAGE encyclopedia of surveillance, security, and privacy**. V.1. Thousand Oaks: SAGE, 2018. p. 284-285. p. 285.

[213] LYON, David. Surveillance as social sorting: computer codes and mobile bodies. In: LYON, David (Ed.). **Surveillance as social sorting**: privacy, risk, and digital discrimination. London/New York: Routledge, 2003. p. 13-30. p. 13

[214] MOLINER, Liliana Arroyo; FROWD, Philippe M. Social sorting. In: ARRIGO, Bruce A. (Ed.). **The SAGE encyclopedia of surveillance, security, and privacy**. Vol. 3. Thousand Oaks: SAGE, 2018. p. 936-937.

[215] LYON, David (Ed.). **Surveillance as social sorting**: privacy, risk, and digital discrimination. London/New York: Routledge, 2003. p. i.

[216] "*A means of verifying identities but also of assessing risks and assigning wort*"

[217] MONAHAN, Torin. Social inequality and the pursuit of democratic surveillance. In: HAGGERTY, Kevin D.; SAMATAS, Minas. (Ed.). **Surveillance and Democracy**. Abingdon/New York: Routledge, 2010. p. 91-110. p. 97.

[218] MONAHAN, Torin. Social inequality and the pursuit of democratic surveillance. In: HAGGERTY, Kevin D.; SAMATAS, Minas. (Ed.). **Surveillance and Democracy**. Abingdon/New York: Routledge, 2010. p. 91-110. p. 97.

[219] De acordo com David Lyon, o termo "*data-double*" refere-se ao "*electronic profile, compiled from personal data fragments, of an individual person and it takes on increasing social significance as assessments and judgments are made in various contexts based upon it. Also referred to variously as the software self or digital persona, the data-double becomes part of the makeup of the individual, a component of his or her identification, even though the data-subject may question its accuracy"* (LYON, David. Surveillance studies: an overview. Cambridge/Malden: Polity, 2007. p. 199-200). "perfil eletrônico, compilado a partir de fragmentos de dados pessoais de uma pessoa individual e assume crescente importância social à medida em que avaliações e julgamentos são feitos com base nele em variados contextos. Também é conhecido como *software self* ou *digital persona*, o *data-double* torna-se parte da composição do indivíduo, um componente de sua identificação, mesmo que o sujeito titular dos dados possa questionar sua exatidão" (tradução livre).

[220]ABU-LABAN, Yasmeen. The politics of surveillance: civil liberties, human rights and ethics. In: BALL, Kirstie; HAGGERTY, Kevin D.; LYON, David (Ed.). **Routledge Handbook of Surveillance Studies**. London/New York: Routledge, 2012. p. 420-427. p. 423

> As tecnologias de vigilância não monitoram as pessoas *qua* indivíduos, mas operam através de processos de desmontagem e remontagem. As pessoas são divididas em uma série de fluxos informativos discretos que são estabilizados e capturados de acordo com critérios classificatórios pré-estabelecidos. Elas são então transportadas para locais centralizados para serem remontadas e combinadas de forma a servir às agendas institucionais. Cumulativamente, tais informações constituem nossos "perfis virtuais/informacionais" que circulam em vários computadores e contextos de aplicação prática (tradução livre).[221] [222]

Essa vigilância exercida por meio da coleta e tratamento de dados, na maioria dos casos, possui como dano colateral a tendência de criar e/ou sustentar condições de desigualdade social e identidades de marginalidade já existentes, tendo em vista que esses sistemas de vigilância, assim como outras tecnologias empregadas em contextos sociais, absorvem e reproduzem valores culturais dominantes na economia política em que são criados e aplicados, sendo a racionalidade neoliberal a lógica que domina a maioria das instituições de poder e esferas da vida pública na sociedade de controle e que, portanto, influencia a criação, aplicação e os efeitos das tecnologias aplicadas em contextos sociais, como, por exemplo, os sistemas que instrumentalizam as tecnopolíticas de vigilância. A lógica de mercado neoliberal, que veio a colonizar outras esferas da vida pública, prioriza o ganho econômico sobre qualquer outro fim e prega a individualização dos sujeitos e a despolitização de problemas sociais, normalizando as desigualdades. Aqueles que falham em seguir essa lógica de mercado são excluídos, marginalizados ou criminalizados. Assim, práticas de vigilância, que são elemento essencial de toda sociedade democrática, e tem por intuito identificar aqueles que devem receber benefícios, são também utilizadas para identificar aqueles que devem ser excluídos e/ou punidos.[223] Os mesmos instrumentos utilizados para garantir que os indivíduos recebam os benefícios sociais devidos e garantir tratamento justo e equalitário para toda a população, podem criar oportunidade para a implantação de políticas autoritárias ou arbitrárias.[224]

---

[221] HAGGERTY, Kevin D.; ERICSON, Richard V. The new politics of surveillance and visibility. In: HAGGERTY, Kevin D.; ERICSON, Richard V. (Ed.). **The new politics of surveillance and visibility**. Toronto/Buffalo/London: University of Toronto Press, 2006. p. 3-25. p. 4.

[222] "*Surveillance technologies do not monitor people qua individuals, but instead operate through processes of disassembling and reassembling. People are broken down into a series of discrete informational flows which are stabilized and captured according to pre-established classificatory criteria. They are then transported to centralized locations to be reassembled and combined in ways that serve institutional agendas. Cumulatively, such information constitutes our 'data double/ our virtual/informational profiles that circulate in various computers and contexts of practical application*".

[223] MONAHAN, Torin. Social inequality and the pursuit of democratic surveillance. In: HAGGERTY, Kevin D.; SAMATAS, Minas. (Ed.). **Surveillance and Democracy**. Abingdon/New York: Routledge, 2010. p. 91-110. p. 99, 105-106.

[224] LYON, David. Identification, surveillance and democracy. In: HAGGERTY, Kevin D.; SAMATAS, Minas. (editors). **Surveillance and Democracy**. Abingdon/New York: Routledge, 2010. p. 34-50. p. 34.

Essas práticas discriminatórias e de diferenciação para fins de controle sustentam desigualdades já existentes - e criam novas -, na medida em que elas não só identificam e agem sobre as diferenças sociais, mas também fabricam essas diferenças com base em indicadores particulares – raça, condição econômica, localização geográfica da residência etc. - que produzem efeitos significativos nas experiências desses indivíduos e nas oportunidades que lhe são apresentadas, já que essas questões passam a depender da categoria em que eles foram colocados.[225] De acordo com Monahan, existem dois processos que produzem essas diferenciações para fins de controle:

> Enquanto o social sorting normalmente funciona através da aplicação diferencial dos mesmos sistemas tecnológicos à governança de diferentes populações, existem outras formas de vigilância que podem produzir resultados desiguais. O que eu chamo de 'vigilância marginalizadora' implica uma exposição desigual à diferentes sistemas de vigilância com base no endereço social de cada um. Na maioria das vezes, isto significa que alguns dos sistemas mais invasivos de exame e controle são desproporcionalmente aplicados aos pobres, às minorias étnicas, ou às mulheres. [...] Tal vigilância não só simplesmente regula os grupos marginalizados – ela produz ativamente tanto identidades quanto condições de marginalidade. (tradução livre)[226] [227]

> Se o *social sorting* dá a aparência de oferecer incentivos para tratamento diferencial baseado em status econômico ou outros indicadores de risco, a 'vigilância marginalizadora' ameaça com desincentivos disciplinares para aqueles incapazes ou não dispostos a competir no mundo neoliberal. Isto ajuda a explicar por que as formas mais invasivas e discriminatórias da 'vigilância marginalizadora' se concentram quase exclusivamente nos desqualificados econômica ou politicamente, incluindo aqueles que dependem de assistência médica, assistência social, educação pública, transporte público e até mesmo aqueles que tentam acessar locais de votação em comunidades com preponderância de minorias étnicas. (tradução livre)[228] [229]

---

[225] MONAHAN, Torin. Social inequality and the pursuit of democratic surveillance. In: HAGGERTY, Kevin D.; SAMATAS, Minas. (Ed.). **Surveillance and Democracy**. Abingdon/New York: Routledge, 2010. p. 91-110. p. 105-106.

[226] MONAHAN, Torin. Social inequality and the pursuit of democratic surveillance. In: HAGGERTY, Kevin D.; SAMATAS, Minas. (Ed.). **Surveillance and Democracy**. Abingdon/New York: Routledge, 2010. p. 91-110. p. 97-98.

[227] "*Whereas social sorting typically works through the differential application of the same technological systems to the governance of different populations, there are other ways that surveillance can produce unequal outcomes. What I refer to as "marginalizing surveillance" entails unequal exposure to different surveillance systems based on one's social address. More often than not, this means that some of the most invasive systems of scrutiny and control are disproportionately applied to the poor, to ethnic minorities, or to women. […] Such surveillance does not simply regulate marginalized groups—it actively produces both identities and conditions of marginality."*

[228] MONAHAN, Torin. Social inequality and the pursuit of democratic surveillance. In: HAGGERTY, Kevin D.; SAMATAS, Minas. (Ed.). Surveillance and Democracy. Abingdon/New York: Routledge, 2010. p. 91-110. p. 100.

[229] "*If social sorting lends the appearance of providing incentives for differential treatment based on economic or other status or risk indicators, marginalizing surveillance threatens with disciplinary disincentives for those unable or unwilling to compete in the neoliberal world. This helps to explain why the most invasive and discriminatory forms of marginalizing surveillance focus almost exclusively on the economically or politically disenfranchised, including those who depend on state-supported health care, welfare, public education, public transportation, and even those trying to access polling places in communities with a preponderance of ethnic minorities*".

Os processos de identificação e de classificação por meio do tratamento de dados acontecem de uma forma geral, abrangendo toda a população de um país e, por vezes, estrangeiros, moldando escolhas, comportamentos e oportunidades de um modo geral. No entanto, esse componente da vigilância contemporânea afeta principalmente as minorias sociais, as parcelas da população que já são marginalizadas por um ou outro motivo e que, quando alvos dessa classificação, se veem ainda mais excluídas socialmente. Um exemplo notável diz respeito à crescente identificação de indivíduos com origem árabe ou muçulmana em aeroportos ou em postos de controle de fronteira dos Estados Unidos após os ataques de 11 de setembro de 2001, produzindo consequências negativas para essas pessoas. [230] Nesse sentido, a maioria das manifestações da vigilância contemporânea como forma de controle social são antidemocráticas justamente pelo ímpeto classificatório imposto pela lógica neoliberal, que impõe um controle diferencial entre classes sociais diferentes, produzindo condições e identidades de marginalidade e desigualdade social ou fortalecendo as já existentes.[231] Segundo Monahan, a vigilância contemporânea, instrumentalizada por tecnologias, é antidemocrática tanto em seu design como em sua aplicação, tendo em vista que:

> Eles individualizam, objetificam e controlam pessoas – muitas vezes através do uso de dados – de formas que perpetuam as desigualdades sociais; ofuscam os contextos sociais por sua falta de transparência; as pessoas desconhecem em grande parte o funcionamento de seus sistemas, ou de seus direitos; e resistem à intervenção em seus projetos técnicos e gestão fechados por especialidades técnicas ou agentes institucionais. Especialmente por fecharem o caminho para oportunidades de participação (ou representação) significativas nos *designs* de sistemas que afetam a vida da maioria das pessoas e por agravarem as desigualdades sociais, os sistemas de vigilância ameaçam a democracia (tradução livre).[232] [233]

O poder de controle diferencial produzido pela vigilância, especialmente aquela exercida por governos, pode se traduzir em um poder de discriminação. Ainda, uma das

---

[230] LYON, David. Introduction. In: LYON, David (Ed.). **Surveillance as social sorting**: privacy, risk, and digital discrimination. London/New York: Routledge, 2003. p. 1-9. p. 1.

[231] MONAHAN, Torin. Social inequality and the pursuit of democratic surveillance. In: HAGGERTY, Kevin D.; SAMATAS, Minas. (Ed.). **Surveillance and Democracy**. Abingdon/New York: Routledge, 2010. p. 91-110. p. 100-101.

[232] MONAHAN, Torin. Social inequality and the pursuit of democratic surveillance. In: HAGGERTY, Kevin D.; SAMATAS, Minas. (Ed.). **Surveillance and Democracy**. Abingdon/New York: Routledge, 2010. p. 91-110. p. 105.

[233] "*They individualize, objectify, and control people—often through their use of data—in ways that perpetuate social inequalities; they obfuscate social contexts through their lack of transparency; people are largely unaware of the functioning of their systems, or of their rights; and they resist intervention through their closed technical designs and management by technical experts or institutional agents. Especially by shutting down avenues for meaningful participation (or representation) in design processes that affect most people's lives and by aggravating social inequalities, surveillance systems threaten democracy*"

violações mais evidentes causada pela vigilância é direcionada à um subconjunto da privacidade, denominada privacidade intelectual por Neil M. Richards, que envolve a ideia de que o pensamento crítico é melhor desenvolvido quando não está submetido ao escrutínio da exposição pública ou monitoramento constante e que, portanto, a proteção da privacidade contra a vigilância constante é necessária para promover a liberdade intelectual, manifestação do pensamento, liberdade de consciência e crença e liberdade de associação.[234] Nas palavras de Richards:

> […] a vigilância é prejudicial porque pode impedir o exercício de nossas liberdades civis. Com relação às liberdades civis, considere a vigilância das pessoas quando elas estão pensando, lendo e se comunicando com outras, a fim de se decidir sobre questões políticas e sociais. Tal vigilância intelectual é especialmente perigosa porque pode fazer com que as pessoas não experimentem ideias novas, controversas ou desviantes. Para proteger nossa liberdade intelectual de pensar sem supervisão ou interferência do Estado, precisamos do que eu tenho chamado de 'privacidade intelectual' (tradução livre).[235] [236]

Nesse sentido, a vigilância causa um efeito generalizado de enfraquecimento da participação dos cidadãos no exercício de suas liberdades civis, que são a base de uma sociedade livre. Segundo o autor, quando um indivíduo sabe que se encontra sob constante monitoramento, ele se autocensura, evitando a manifestação de pensamentos que poderiam ser considerados desviantes, o que ameaça o compromisso das sociedades democráticas com as liberdades intelectuais, de pensamento e de crença.[237] Essa é uma teoria da psicologia social introduzida por Noelle-Neumann, denominada "*spiral of silence*" (espiral do silêncio em português). De acordo com a autora a teoria consiste na ideia de que, motivados pelo medo do isolamento, os indivíduos normalmente monitoram seus ambientes sociais buscando indícios de quais opiniões são dominantes, para que então decidam se querem expor suas opiniões publicamente ou não. Se suas opiniões coadunam com a opinião dominante, a chance de se exporem é maior, caso contrário haverá menos vontade de se expor, mantendo-se, assim, em silêncio.[238]

---

[234] RICHARDS, Neil M. The danger of surveillance. In: **Harvard Law Review**, v. 126, 2013. p. 1945-1946.
[235] RICHARDS, Neil M. The danger of surveillance. In: **Harvard Law Review**, v. 126, 2013. p. 1935
[236] "*[…] surveillance is harmful because it can chill the exercise of our civil liberties. With respect to civil liberties, consider surveillance of people when they are thinking, reading, and communicating with others in order to make up their minds about political and social issues. Such intellectual surveillance is especially dangerous because it can cause people not to experiment with new, controversial, or deviant ideas. To protect our intellectual freedom to think without state oversight or interference, we need what I have elsewhere called "intellectual privacy*"
[237] RICHARDS, Neil M. The danger of surveillance. In: **Harvard Law Review**, v. 126, 2013. p. 1948-1949.
[238] NOELLE-NEUMANN, Elisabeth. The spiral of silence: a theory of public opinion. In: **Journal of Communications**, v. 24, n. 2, 1974, pp. 45-51.

A teoria indica, portanto, um silenciamento de opiniões e comportamentos das minorias por meio da autocensura, motivada pelo medo do isolamento, situação essa que se agrava quando o indivíduo em questão é ciente de que está sendo monitorado constantemente.[239] Esse fenômeno é reconhecido pelo próprio Comitê Consultivo de Tecnologia e Privacidade dos Estados Unidos, o qual constatou que "é provável que pessoas ajam de maneira diferente se souberem que sua conduta pode ser observada" (tradução livre)[240] [241]. Conforme observa Lilian Mitrou, em contextos de vigilância constante, as liberdades que constituem a própria substância das democracias constitucionais não podem ser plenamente exercidas, o que impede o desenvolvimento de identidades e ideias de toda uma população.[242]

Além da violação da privacidade e do poder de discriminação, o exercício massivo e totalizante da vigilância também produz poderes de chantagem e persuasão. O conhecimento obtido por meio da vigilância pode ser utilizado para a chantagem de oponentes políticos ou dissidentes, por exemplo. Ou ainda, pode-se utilizar dessas informações para desacreditar indivíduos (oponentes) por meio de sua divulgação. Richards cita como exemplo o notório caso de Martin Luther King Jr., o qual teve suas comunicações privadas monitoradas pelo FBI para fins de chantagem. Com o desenvolvido das TICs o potencial para realização de tal feito atualmente é muito maior, podendo-se citar o exemplo do governo Líbio, o qual obteve informações sobre dissidentes, por meio de tecnologias, com o intuito de chantageá-los ao silêncio, o que se mostrou mais eficiente do que o uso de violência.[243] Conforme observa Richards:

> Quer estas descobertas sejam importantes, incidentais ou irrelevantes, todas elas dão maior poder ao observador. Funcionários inescrupulosos do governo poderiam se envolver em chantagem, seja motivado por considerações políticas ou pecuniárias. Mas mesmo os agentes fiéis do governo que descobrem a atividade ilegal, agora possuem a arma da acusação seletiva [...] (tradução livre).[244] [245]

---

[239] RICHARDS, Neil M. The danger of surveillance. In: **Harvard Law Review**, v. 126, 2013. p. 1948-1949.
[240] U.S DEPARTMENT OF DEFENSE – Technology and Privacy Advisory Commite. **Safeguarding privacy in the fight against terrorism** (report). Washington, 2004. Disponível em: https://cdt.org/wp-content/uploads/security/usapatriot/20040300tapac.pdf. Acesso em: 15 set. 2021. P. 35.
[241] "*People are likely to act differently if they know their conduct could be observed*"
[242] MITROU, Lilian. The impact of communications data retention on fundamental rights and democracy: the case of the EU Data Retention Directive. In: HAGGERTY, Kevin D.; SAMATAS, Minas. (Ed.). **Surveillance and Democracy**. Abingdon/New York: Routledge, 2010. pp. 127-147. p. 138, 143.
[243] RICHARDS, Neil M. The danger of surveillance. In: **Harvard Law Review**, v. 126, 2013. p. 1952-1954; 1956-1957.
[244] RICHARDS, Neil M. The danger of surveillance. In: **Harvard Law Review**, v. 126, 2013. p. 1954-1955.
[245] "*Whether these discoveries are important, incidental, or irrelevant, all of them give greater power to the watcher. Unscrupulous government officials could engage in blackmail, whether motivated by political or pecuniary considerations. But even faithful government agents who discover illegal activity would now possess the weapon of selective prosecution […]*".

O poder advindo do conhecimento obtido pela vigilância também é utilizado para controle de comportamentos por meio da persuasão. De acordo com Richards, a persuasão - ou influência - é um efeito mais sutil do poder em comparação com a chantagem, mas que, no entanto, pode ser mais eficaz. Um exemplo é o uso massivo de câmeras de circuito fechado (*closed-circuit television* ou CCTV) em áreas urbanas para permitir que a polícia tenha maior controle e influência sobre o que ocorre nas ruas da cidade, uma vez que a presença dessas câmeras auxilia na persuasão dos cidadãos em obedecer à lei, além de outros efeitos, como o direcionamento do comportamento público para o comércio e para longe de atividades criminosas ou ativistas. Segundo o autor, na Grã-Bretanha, país onde há mais câmeras de vigilância espalhada pelas cidades, os sistemas de CCTV operam em conexão com ordens judiciais, conhecidas como Ordens de Comportamento Antissocial, para persuadir grupos de adolescentes a ficar fora dos centros comerciais das cidades usando a vídeo-vigilância e o controle policial para que o ritmo e a eficácia do comércio não sejam perturbados.[246] Esse poder de persuasão, por vezes, pode ser usado para fins positivos e em benefício da sociedade ou até sem que cause efeitos positivos ou negativos para a sociedade em geral. No entanto, ele também pode ser utilizado para dissuadir ativistas a exercer seus direitos e liberdades em manifestações pacíficas, por exemplo, o que entraria no campo de violações da privacidade intelectual e liberdades civis.

Atualmente existem diversos exemplos de tecnopolíticas de vigilância no Brasil com grande potencial para violações de direitos e liberdades. Talvez o caso mais relevante no atual contexto, em que o governo vem demonstrando grande interesse por atividades de vigilância da população, seja a criação do Cadastro Base do Cidadão (CBC)[247], uma base de dados que centraliza uma diversidade de dados pessoais de toda a população brasileira, dispensando acordo ou convênio para compartilhamento desses dados entre órgãos do poder público. Apesar de não se configurar como uma tecnologia nova e complexa, os riscos advindos do CBC para a sociedade e para os cidadãos são significativos, especialmente no contexto de expansão da implementação de tecnologias com capacidade para vigilância pelo governo federal e pelos governos estaduais. A sinergia dessas diversas tecnologias fortalece a capacidade do Estado de exercer controle social sobre a população e instrumentaliza aparelhos repressivos.

---

[246] RICHARDS, Neil M. The danger of surveillance. In: **Harvard Law Review**, v. 126, 2013. p. 1955-1956.
[247] BRASIL. Decreto nº 10.046, de 9 de outubro de 2019. Diário Oficial [da] União, Brasília, 09 out. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 15 set. 2021.

Assim, o Cadastro Base do Cidadão se mostra como uma tecnologia central que interrelaciona diversas outras tecnologias de vigilância implementadas no Brasil, permitindo um acesso mais amplo e mais intrusivo aos dados pessoais dos cidadãos a grande parte dos órgãos públicos e construindo uma tecnopolítica de vigilância massiva e totalizante. A escolha pela análise do CBC se deu, portanto, por sua capacidade de, por um lado, facilitar a criação, implementação e garantia de eficácia de políticas públicas e, por outro, centralizar e facilitar a vigilância estatal exercida sobre a população para fins escusos e com efeitos prejudiciais aos direitos fundamentais. Ainda que a vigilância estatal seja necessária mesmo em democracias constitucionais, a intensificação da vigilância por meio da tecnologia trouxe novos riscos que não podem ser ignorados. Considerar violações de direitos e liberdades fundamentais como simples dano colateral inevitável, presente em qualquer esforço de administração e garantia de segurança, ameaça enfraquecer ou até mesmo destruir por completo a democracia.[248]

Nesse sentido, a imposição de limites legais e principiológicos ao exercício da vigilância exercida por meio da coleta e tratamento de dados é essencial para que a implementação dessas tecnopolíticas possa atender suas finalidades legítimas sem violar os direitos e liberdades fundamentais dos cidadãos, aos quais os dados pessoais tratados dizem respeito. Desse modo, no capítulo seguinte realiza-se a análise desses limites, perpassando pelos direitos à privacidade e à proteção de dados pessoais, dois direitos fundamentais protegidos pela Lei Geral de Proteção de Dados Pessoais (LGPD), e, ainda, pela necessidade de uma análise contextual de cada exercício de vigilância.

[248] MITROU, Lilian. The impact of communications data retention on fundamental rights and democracy: the case of the EU Data Retention Directive. In: HAGGERTY, Kevin D.; SAMATAS, Minas. (Ed.). **Surveillance and Democracy**. Abingdon/New York: Routledge, 2010. p. 127-147. p. 143.

3 A LGPD COMO INSTRUMENTO DE LIMITAÇÃO DOS RISCOS DAS TECNOPOLÍTICAS DE VIGILÂNCIA

Da análise do fenômeno da vigilância, pode-se observar que a vigilância estatal é parte integrante e necessária das sociedades, tanto para a garantia de que as leis estão sendo cumpridas (segurança e policiamento), quanto para fins de administração pública (controle e administração da população). Sem essa vigilância, os Estados teriam maior dificuldade em fazer cumprir as normas impostas, bem como em organizar a sociedade para que todos os seus institutos pudessem funcionar.[249] [250] Apesar de ser em si uma prática que exige que a proteção da privacidade seja mitigada, a vigilância estatal se faz necessária inclusive em sociedades democráticas. Por outro lado, por estar intimamente ligada ao exercício do poder, a vigilância reproduz e cria assimetrias dentro da relação em que está inserida e, desse modo, pode criar situações de abuso desse poder. Por esse motivo, a busca por limitar o poder de autoridades de exercer a vigilância sobre os cidadãos, que frequentemente é exercida sem seu consentimento e/ou conhecimento, é antiga, já que, de acordo com Alan Westin, essa busca data dos dias da cidade-estado grega.[251]

Do esforço de limitar esses poderes advém as matérias de proteção da privacidade e proteção de dados pessoais, os quais são os dois grandes balizadores para a atuação dos agentes de vigilância, para que o risco de violação de diversos outros direitos fundamentais (delineados no último capítulo), diretamente relacionados com aqueles dois, possam ser mitigados. Desse modo, realiza-se aqui uma escolha metodológica, qual seja, a de delimitar a discussão aos direitos à proteção de dados pessoais e à privacidade, uma vez que são os dois direitos violados de forma direta pelos sistemas de vigilância e que, quando protegidos, podem evitar a violação de outros direitos e liberdades fundamentais.

No Brasil, o direito à privacidade e o direito à proteção de dados pessoais são ambos reconhecidos como direitos fundamentais, constitucionalmente protegidos. Além disso, para garantir seu cumprimento, regulando o tratamento de dados pessoais, o ordenamento jurídico brasileiro conta com a Lei Geral de Proteção de Dados Pessoais (LGPD - Lei 13.709/2018), a qual entrou em vigor em agosto de 2020.

---

[249] LYON, David. **The Electronic Eye**: The rise of surveillance society. Cambridge: Polity, 1994 (Kindle Edition). p. 91.
[250] WESTIN, Alan F. **Privacy and Freedom**. New York: Ig Publishing, 1967. p. 12
[251] WESTIN, Alan F. **Privacy and Freedom**. New York: Ig Publishing, 1967. p. 35.

Para que se possa verificar se uma tecnopolítica de vigilância é legítima face aos preceitos legais estabelecidos no ordenamento jurídico, faz-se necessário analisá-la sob a luz dos preceitos conceituais e principiológicos delineados pelos documentos legais de garantia dos direitos à privacidade e à proteção de dados pessoais, bem como levar em conta o contexto social e econômico em que essa vigilância está sendo implementada. Uma estrutura de análise da vigilância deve levar em conta sua adequação às garantias legais de proteção da privacidade e dos dados pessoais e os princípios estabelecidos para seu cumprimento, bem como o contexto e as relações em que será implementada.

Assim, nesse capítulo são delineadas as questões necessárias para a análise da legitimidade de uma tecnopolítica de vigilância dentro do ordenamento jurídico brasileiro, para que posteriormente possa ser realizada a análise do Cadastro Base do Cidadão. Para isso, o capítulo divide-se em quatro Seções. Na primeira e na segunda discorre-se sobre a garantia do direito fundamental à privacidade e a garantia da proteção de dados pessoais, respectivamente, e sua importância face ao exercício da vigilância. Na terceira seção discorre-se sobre a necessidade de realização de análise de proporcionalidade entre os direitos do indivíduo que está sob vigilância e a finalidade dessa. E, por fim, na última seção discorre-se sobre a necessidade de análise contextual da aplicação de uma tecnopolítica de vigilância.

3.1 A GARANTIA DO DIREITO FUNDAMENTAL À PRIVACIDADE

A privacidade surgiu no período da desagregação da sociedade feudal. Essa era tida como uma possibilidade estendida apenas à classe burguesa, a qual conseguia realizá-la especialmente graças às transformações socioeconômicas da Revolução Industrial e suas condições materiais de vida. O direito à privacidade nasce, portanto, como um privilégio de uma única classe social, nos moldes do direito à propriedade; privilégio a que a classe operária não tinha acesso. Em sua origem, a privacidade não exprimia exigências uniformemente difundidas pela coletividade, representante de todas as classes. E do mesmo modo, há que se considerar que o conceito de privacidade desaparecia onde as condições de vida da classe burguesa se degradava, bem como era reivindicada pelos estratos mais altos da classe operária.[252]

[252] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 26-28.

A expectativa de privacidade foi se transformando conforme mudanças sociais aconteciam na sociedade industrial. A urbanização e a maior anonimidade da vida na cidade, a difusão de eletricidade e infraestrutura doméstica, a construção de habitações coletivas, a diminuição do número de membros nas famílias, a maior mobilidade do trabalho e da residência, e o surgimento dos meio de comunicação de massa trouxe à tona maior possibilidade de privacidade física e psicológica, além de novos tipos de inconformismo, o qual moveu os advogados Samuel Warren e Louis Brandeis a escrever o artigo *The right to privacy*, instigados, principalmente, por seu aborrecimento com as crescentes invasões de privacidade sociais, como a invasão realizada por jornalistas nas vidas íntimas das pessoas por meio do uso de máquinas fotográficas e da posterior publicação dessas fotos em colunas sociais nos jornais. O artigo refletiu a tendência a desvincular a proteção da privacidade ao direito de propriedade, observando que a proteção da privacidade está relacionada à um direito de natureza pessoal (*inviolate personality*). O trabalho de Warren e Brandeis acabou por se tornar um marco dos debates modernos sobre a privacidade, no entanto, cabe a ressalva de que foi escrito em contexto cultural e jurídico muito diferente do contexto brasileiro atual.[253]

Segundo Rodotà, para que se possa compreender a real dinâmica da reinvindicação da privacidade, deve-se entender qual é a sua função segundo a cultura do grupo que a realiza, bem como segundo a finalidade que justifica a violação da privacidade. Mesmo Warren e Brandeis atribuíam diferentes funções ao conceito. O primeiro visava os privilégios da alta burguesia contra a ação da imprensa; e o segundo visava a privacidade, também, de minorias intelectuais e artísticas contra as indiscrições jornalísticas, tendo em vista que essas poderiam aumentar a impopularidade daquelas minorias. Duplicidade de pontos de vista que ainda assim não traduzia os interesses de todas as classes sociais pertencentes à sociedade. Desse modo, evocar a proteção da privacidade pode assumir significados diversos.[254]

Contudo, alguns motivos contribuíram para que esse modelo de privacidade "elitista" passasse a decair, podendo-se citar as mudanças sociais, econômicas e políticas ocorridas em diversos países por volta do fim da década de 1960 e início da década de 1970, quando o modelo de *welfare state* chega em seu apogeu e a demanda por direitos aumenta significativamente em consequência de movimentos sociais. O desenvolvimento das TICs e o aumento do fluxo de

---

[253] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 1776- 1802.

[254] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 28.

informações, com o consequente aumento da capacidade de processamento e utilização dessas informações, é outro desses motivos.[255] Ainda, em consequência dessas transformações tecnológicas, o poder público passa a buscar maiores quantidades de dados pessoais em busca de eficiência nos seus serviços, o que também contribui para a mudança no modelo de privacidade, já que não é mais somente a classe burguesa que tem sua privacidade violada, mas também uma grande parcela da população em uma diversidade de situações.[256] [257]

A vigilância estatal, a busca por obtenção de conhecimento sobre a sociedade e os cidadãos para finalidades específicas, sofre uma aceleração e uma intensificação com o desenvolvimento dessa capacidade técnica de coleta, armazenamento, tratamento e distribuição de dados. A informação, que já era fundamental para a atuação do Estado, torna-se ainda mais importante, na medida em que a tecnologia passa a ser um meio para obter informações do tratamento de dados brutos. O Estado possui uma capacidade cada vez maior de vigilância de seus cidadãos, com o intuito de obter conhecimento sobre eles para finalidades específicas de controle e gestão, o que acaba por ser feito por meio das novas capacidades tecnológicas de obtenção e tratamento de dados. Essa mudança inicialmente quantitativa (maior quantidade de dados e maior capacidade de tratamento), passa a se tornar uma mudança qualitativa, transformando os eixos de equilíbrio entre poder, informação, pessoa, controle.[258]

Esse crescente interesse dos poderes públicos pela obtenção de dados relevantes ao exercício de suas atribuições combinado às novas capacidades tecnológicas impulsiona a tendência de coleta e fichamento de dados de grandes contingentes populacionais com a finalidade de tomada de decisões, o que dá origem ao "mito" de que essas coletâneas, contendo dados agregados, não seriam um risco à privacidade[259], o que Rodotà objeta ressaltando que:

> Mesmo as coletâneas de dados anônimas podem ser manipuladas de forma gravemente lesiva aos direitos dos indivíduos: tenha-se em mente o uso que pode ser feito dos dados, agregados, que digam respeito a uma minoria racial ou lingüística

[255] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 451.
[256] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 28-29.
[257] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 449- 458.
[258] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 472- 486.
[259] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 32.

> [*sic*]; ou às conseqüências [*sic*] de uma decisão política ou econômica tomada justamente com base na análise dos dados anônimos.[260]

Ainda de acordo com Rodotà, esse mesmo fenômeno que parecia anunciar a morte da privacidade, mostrou ser um dos elementos que auxiliaram na transformação qualitativa do conceito de privacidade, assumindo funções antes desconhecidas. Conforme retratado por Rodotà, as divergências de significado da evocação da privacidade aumentam. Um exemplo dessa divergência diz respeito à resistência, por um lado, de indivíduos pertencentes à uma classe média de fornecer informações pessoais relevantes para a elaboração de programas sociais a autoridades públicas, o que mostra ser uma oposição direta às políticas de intervenção pública, as quais exigem recursos financeiros e, portanto, uma pressão fiscal mais acentuada, atingindo diretamente essa classe. E, por outro lado, uma reação diversa é aquela que reivindica a privacidade contra um controle do comportamento político, manifestando-se, sobretudo, nos grupos de oposição e nos partidos de esquerda, perdendo seu caráter aristocrático e elitista. Nesse último exemplo, pode-se observar que a reivindicação da privacidade ultrapassa as classes burguesa e classe média, deixando de vincular-se ao caráter de privilégio elitista, para traduzir uma reivindicação de paridade de tratamento entre os cidadãos, visto que as possibilidades de discriminação derivados dos registros de massa atingem principalmente as minorias pertencentes à classe operária.[261]

A definição do direito à privacidade como "direito a ser deixado só", portanto, se mostra cada vez mais frágil nas novas dimensões de coleta e tratamento de dados contemporâneas.[262] De acordo com Doneda, "essa concepção foi o marco inicial posteriormente temperado por uma crescente consciência de que a privacidade seria um aspecto fundamental da realização da pessoa e do desenvolvimento da sua personalidade"[263]. Desse modo, essa definição vem dando lugar a outras que possuem como centro de gravidade a possibilidade de cada um controlar o uso de informações que lhe dizem respeito. Esse aspecto já estava presente em definições anteriores, mas apenas como um aspecto secundário. Hoje, no entanto, assume protagonismo,

---

[260] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 32.

[261] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 29-30.

[262] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 32.

[263] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 414-424.

sendo a possibilidade de indivíduos e grupos controlarem o exercício de poder que emana do acesso a informações e do tratamento dessas, no intuito de estabelecer um equilíbrio sociopolítico mais adequado[264], na medida em que a privacidade se torna um aspecto fundamental para o exercício de outras liberdades garantidas constitucionalmente.[265]

O cientista político Alan Westin foi um dos primeiros pesquisadores sobre o tema da privacidade a fazer uma análise sistemática da vigilância realizada por meio de computadores, considerada por muitos uma abordagem seminal e clássica. Durante a década de 1960, o pesquisador já alertava sobre as possibilidades sem precedentes que as novas tecnologias apresentavam aos agentes que realizavam coleta e tratamento de dados pessoais.[266] Sua pesquisa se tornou bastante influente, destacando-se sua obra "*Privacy and Freedom*" de 1967, uma das mais importantes obras sobre privacidade já publicadas, a qual influenciou em muito a transformação do entendimento da privacidade, propondo novo modelo para sua definição, que passa a se basear na autodeterminação informativa, além de influenciar também no desenvolvimento da doutrina da proteção de dados pessoais.[267]

Nesse sentido, para Alan Westin, privacidade pode ser definida como:

> [...] a reivindicação de indivíduos, grupos ou instituições para determinar por si mesmos quando, como e até que ponto a informação sobre eles é comunicada a outros. Vista em termos da relação do indivíduo com a participação social, a privacidade é a retirada voluntária e temporária de uma pessoa da sociedade geral por meios físicos ou psicológicos, seja em estado de solidão ou intimidade de pequenos grupos ou, quando entre grupos maiores, em condição de anonimato ou reserva (tradução livre).[268] [269]

Não é mais possível considerar a privacidade por meio do binômio "recolhimento" e "divulgação", havendo a necessidade de expandir esse conceito, abarcando os diversos significados que o tratamento de dados e as potencialidades dos sistemas informacionais podem

---

[264] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 24.

[265] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 423-431

[266] LYON, David. The Eletronic Eye: The rise of surveillance society. Cambridge: Polity, 1994 (Kindle Edition). p. 186.

[267] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2. Ed. São Paulo: Thomson Reuters Brasil, 2020. Posição 4063-4085.

[268] WESTIN, Alan F. **Privacy and Freedom**. New York: Ig Publishing, 1967. p. 3-4.

[269] "*[...] the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve*".

assumir atualmente, principalmente no âmbito do sistema político.[270] Nesse sentido, de acordo com Doneda o conceito de privacidade pode apontar para elementos diversos, tais como a busca por igualdade, pela liberdade de escolha, pela não discriminação, pelo desenvolvimento da personalidade etc.[271] A invocação da privacidade, além de assumir significados diversos dependendo do contexto social, cultural, político e econômico, passa, também, a superar seu caráter individualista, dando lugar à uma dimensão coletiva, levando em consideração o interesse do indivíduo enquanto pertencente à um grupo social.[272]

Para Alan Westin a privacidade possui 04 (quatro) funções em uma sociedade democrática: i) autonomia pessoal; ii) liberação emocional; iii) autoavaliação; iv) comunicação protegida. A primeira delas diz respeito à salvaguarda da individualidade, que é essencial para o desenvolvimento da autonomia. Apenas em um espaço de reclusão e solitude, com tempo necessário para preparação e desenvolvimento do pensamento antes que leve suas opiniões à público, e sem medo de sofrer penalidades, é que um indivíduo pode desenvolver seus pensamentos e sentimentos e, portanto, desenvolver sua individualidade. Para Westin esse desenvolvimento é especialmente importante para sociedades democráticas, já que qualidades como pensamento independente, diversidade de opiniões, e a crítica são traços desejáveis para a liberdade política. Ainda, a garantia desse espaço privado para o desenvolvimento da individualidade e da autonomia são também necessários para o desenvolvimento da personalidade e para garantir a dignidade da pessoa humana aos cidadãos. Nesse sentido, a privacidade seria necessária para criar um espaço no qual o cidadão possa desenvolver suas ideias e expressá-las sem medo de ser repreendido por isso, desenvolvendo assim sua capacidade de tomar decisões livremente, elemento essencial de uma democracia[273].

A segunda função é a garantia de um espaço para a liberação emocional. De acordo com o autor, a vida em sociedade cria uma miríade de tensões, tanto físicas quanto psíquicas, para os indivíduos, demandando, assim, certos períodos de privacidade para que se possa aliviar essa tensão. Algumas dessas demandas por privacidade citadas pelo autor são: para o alívio da pressão de desempenhar papéis sociais dependendo da relação e do contexto em que se

---

[270] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 23-25.

[271] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 396-398.

[272] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 30.

[273] WESTIN, Alan F. **Privacy and Freedom**. New York: Ig Publishing, 1967. p. 19-20.

encontra, necessitando de um momento de intimidade, quando o indivíduo poderá ser ele mesmo; para que os indivíduos possam se recuperar emocionalmente da constante estimulação emocional comum na vida pública em sociedade; para que indivíduos possam dar vazão à sua raiva contra autoridades dentro de sua intimidade, o que se diferencia da liberdade de expressão, pois são críticas e comentários realizados no calor da emoção e que nem sempre manifestam a verdadeira opinião do indivíduo sobre o assunto, mas que, quando feitas na intimidade, são formas de expressão importantes para o alívio do estresse; ainda, para que o indivíduo que está sofrendo alguma perda, algum choque emocional, períodos de ansiedade etc., possa ter um espaço adequado de intimidade para lidar com esses sentimentos.[274]

A terceira função da privacidade, a de autoavaliação, seria a de garantia de um espaço pessoal em que o indivíduo possa processar suas experiências e ideias, planejar e repensar suas ações, avaliando-as de acordo com seus valores morais, desenvolver processos criativos, examinar que tipo de detalhes de sua vida compartilhar com seus pares etc. De acordo com o autor, é somente em períodos de reflexão individual, em solitude, que os indivíduos podem propriamente desenvolver e avaliar seus pensamentos, ideias e ações.[275]

Por fim, a quarta função da privacidade seria a limitação e a proteção da comunicação. De acordo com Westin, toda comunicação entre indivíduos é parcial e limitada a partir da relação entre reserva e discrição. Assim, a privacidade serve para que o indivíduo compartilhe suas confidencias apenas com aqueles em que confia (comunicação limitada) e que ele sabe que respeitarão a norma social de não violação da confiança (comunicação protegida). Essa privacidade também se encontra nas relações com profissionais os quais são impedidos de quebrar a privacidade da relação com o cliente, como advogados, psiquiatras, psicólogos, entre outros. A privacidade por meio da comunicação limitada também serve para criar limites necessários de distanciamento mental nas relações interpessoais, mantendo sua privacidade e intimidade dentro da relação com outras pessoas.[276]

A privacidade em uma sociedade democrática assume, portanto, relações diretas com direitos de personalidade e liberdades fundamentais. De acordo com Alan Westin, a privacidade física e psicológica é importante para garantir a formação de pensamento crítico, a liberdade de pensamento e de expressão e a liberdade intelectual, fundamentais para a vida democrática. A privacidade também se traduz na possibilidade do cidadão tomar suas próprias decisões no que diz respeito à liberdade religiosa, na medida em que o controle sobre a afiliação religiosa é

[274] WESTIN, Alan F. **Privacy and Freedom**. New York: Ig Publishing, 1967. p. 20-21.
[275] WESTIN, Alan F. **Privacy and Freedom**. New York: Ig Publishing, 1967. p. 21-22.
[276] WESTIN, Alan F. **Privacy and Freedom**. New York: Ig Publishing, 1967. p. 22-23.

proibido por lei; e à liberdade de associação, na medida em que a privacidade dessas associações se faz necessária para garantir o fluxo de ideias independentes, a formação do pensamento crítico sobre assuntos de interesse público e, até mesmo, a crítica ao governo. Por fim, a liberdade para a formação de escolhas relacionadas à vida política só pode ser garantida por meio da privacidade e de outras liberdades já citadas. Dessa forma, a privacidade assume estreita relação com as liberdades fundamentais, já que é um requisito essencial para o exercício dessas, na medida em que se faz necessária para nutrir a criatividade, o desenvolvimento da personalidade, a formação de escolhas individuais e a expressão coletiva.[277]

A privacidade abarca um complexo de interesses, se fazendo necessária, portanto, para que outros direitos e liberdades possam ser exercidos plenamente, realizando o princípio democrático e, portanto, dando origem à direitos, poderes, obrigações e ônus aos envolvidos.[278]

A vigilância, como forma de obtenção de um poder de controle por meio do saber e como instrumento de exercício do poder, produz assimetrias de poder, aumentando o poder de controle da parte que vigia sobre a parte vigiada. A ciência de estar sendo vigiado já cria, por si só, um efeito generalizado de minimização da participação dos cidadãos na vida política, mas, para além disso, esse poder de controle pode se traduzir, eventualmente, em poderes de chantagem e persuasão, conforme já delineado no último capítulo, o que pode levar à barragem do exercício de algumas liberdades fundamentais, como a de expressão e associação, impedindo, por exemplo, que os cidadãos se manifestem contrariamente ao governo.[279] Ainda, com a crescente utilização de técnicas de classificação e *profiling*, a vigilância sustenta e produz desigualdades sociais, intensificando processos de discriminação de algumas parcelas da sociedade.[280]

Assim, há que se considerar a dimensão social que a proteção da privacidade assume frente a esses riscos de discriminação pelo exercício da vigilância realizada por meio da coleta e tratamento de dados. De acordo com Priscilla Regan, a privacidade tem importância não só pela proteção do cidadão como indivíduo, mas também porque indivíduos compartilham uma percepção em comum sobre a importância e o significado da privacidade, bem como porque a privacidade serve como uma limitação sobre como as organizações usam seu poder, uma vez

---

[277] WESTIN, Alan F. **Privacy and Freedom**. New York: Ig Publishing, 1967. p. 14-16.
[278] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 1880-1888.
[279] RICHARDS, Neil M. The danger of surveillance. In: **Harvard Law Review**, v. 126, 2013. p. 1952-1957.
[280] MONAHAN, Torin. Social inequality and the pursuit of democratic surveillance. In: HAGGERTY, Kevin D.; SAMATAS, Minas. (Ed.). **Surveillance and Democracy**. Abingdon/New York: Routledge, 2010. p. 91-110. p. 105-106.

que a vigilância por meio de dados, por exemplo, não afeta a relação de dois indivíduos, mas é usada por organizações governamentais ou privadas, afetando uma miríade de indivíduos conjuntamente. Nesse sentido, Regan identifica três bases que explicam a importância social da privacidade, sendo elas: i) a privacidade é um valor comum, na medida em que todos os indivíduos tem uma percepção comum dela; ii) a privacidade é um valor público, na medida em que ela tem importância para o sistema político; iii) a privacidade é um valor coletivo, na medida em que se torna cada vez mais difícil que um indivíduo tenha algum nível de privacidade garantido sem que as outras pessoas da sociedade tenham um nível similar de privacidade garantida.[281]

Frente à crescente sofisticação do exercício da vigilância e aos riscos da vigilância estatal delineados, a proteção da privacidade torna-se um balizador necessário entre a necessidade do uso da vigilância e os direitos e liberdades individuais e civis dos cidadãos que devem ser garantidos para o desenvolvimento democrático, na tentativa de criar certo equilíbrio entre as partes dessa relação. Ressalta-se que a proteção da privacidade serviria, portanto, não como um impeditivo para o exercício da vigilância estatal sobre a sociedade e os cidadãos, já que, como já mencionado, essa se faz por vezes necessária, mas sim como limitador do exercício dessa vigilância, na tentativa de estabelecer um equilíbrio de poder entre as partes envolvidas no processo, evitando que direitos e liberdades fundamentais sejam violados desproporcional e desnecessariamente.

O ordenamento jurídico brasileiro aborda a proteção da pessoa humana como valor máximo e dá à privacidade valor de direito fundamental. A privacidade é garantida por meio do artigo 5º da Constituição Federal de 1988, o qual prevê a proteção da "intimidade" e da "vida privada", além da "honra" e da 'imagem" (inciso X).[282] Ainda, o Marco Civil da Internet (Lei 12.965/2014) cita como um dos princípios da disciplina do uso da Internet no Brasil, a proteção da privacidade (art. 3º, II).[283] Face aos desenvolvimentos tecnológicos e ao crescente exercício da vigilância por meio da obtenção e tratamento de dados, da dimensão social que a privacidade assume, bem como da necessidade de funcionalização da proteção da privacidade, esse direito passa a se manifestar sobretudo por meio do direito à proteção de dados pessoais, disciplina que é tida independentemente do direito à privacidade, mas que, segundo Doneda, é uma

[281] REGAN, Priscilla. **Legislating Privacy**: Technology, social values, and public policy. Chapel Hill: The University of North Carolina Press, 1995. p. 23, 213.
[282] BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial [da] União**, Brasília, 5 de out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 15 nov. 2021
[283] BRASIL. Lei 12. 965, de 23 de abril de 2014. **Diário Oficial [da] União**, Brasília, 23 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 15 nov. 2021.

"continuação por outros meios" daquela, por assumir a tarefa de abordar uma miríade de interesses significativos, especialmente, na sociedade pós-industrial, assumindo características próprias.[284] Pode-se notar essa atuação coordenada pela leitura do artigo 2º da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018), o qual prevê como fundamento da disciplina de proteção de dados pessoais o respeito à privacidade.[285]

Desse modo, a proteção de dados pessoais torna-se essencial para que o indivíduo possa ter sua esfera privada dentro da vida em sociedade e sob o paradigma da solidariedade.[286]

3.2 O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

O conceito de privacidade, conforme já delineado, transforma-se constantemente de acordo com o contexto social, político, econômico, ambiental e jurídico, bem como de acordo com a posição das partes dentro da sociedade. Conforme a tecnologia e as técnicas de tratamento de dados evoluem, bem como a vigilância passa a ser exercida cada vez mais por meio da coleta e tratamento de dados, novos riscos à privacidade vão se desenvolvendo. A informação vai adquirindo cada vez mais importância para a sociedade pós-industrial. A partir da década de 1970 o conceito jurídico de privacidade vai se associando cada vez mais aos casos de armazenamento de informações em grandes bancos de dados.[287]

O desenvolvimento do processamento de dados automatizado acarreta mudanças quantitativas, na medida em que com maior capacidade de processamento, um maior volume de dados pode ser processado; e qualitativas, na medida em que novos métodos, algoritmos e técnicas estão agora disponíveis para esse fim, auxiliando na obtenção de resultados mais valiosos. O discurso sobre a privacidade vai assumindo, cada vez mais, a dimensão da proteção de dados pessoais[288], que se mostra uma noção mais completa, abarcando interesses que vão

---

[284] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 617-637, 675-681.

[285] BRASIL. Lei 13.709, de 14 de agosto de 2018. **Diário Oficial [da] União**, Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 out. 2021.

[286] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 594-597.

[287] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 1832

[288] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 3668-3680, 3445-3447.

além da intimidade individual e atingem a privacidade com valor social[289], colocado maior ênfase nas relações entre os interesses dos indivíduos e as modalidades de circulação de informações.[290] Assim, a temática da privacidade volta-se à informação e aos dados pessoais, sendo a disciplina de proteção de dados pessoais uma continuação da disciplina da privacidade.[291] Nesse sentido, a questão da privacidade é ampliada na sociedade da informação e nas palavras de Stefano Rodotà:

> Transforma-se em um poder social, o de controlar diretamente os sujeitos públicos e privados que tratam os dados pessoais. Assim, em uma sociedade na qual as informações se tornam a riqueza mais importante, a tutela da privacidade contribui de forma decisiva para o equilíbrio dos poderes. Eis porque o fim da privacidade não representaria somente um risco para as liberdades individuais: ele pode efetivamente conduzir ao fim da democracia. [...] Confirma-se assim que a privacidade, neste seu significado mais amplo, constitui um elemento fundamental da cidadania da nossa época, da "cidadania eletrônica". A sociedade da informação requer novos instrumentos, um novo quadro institucional.[292]

Para que se possa compreender o processo que deu origem à noção jurídica de proteção de dados pessoais, faz-se válido retomar alguns casos que capitalizaram essa discussão. Os casos do *National Data Center* e do SAFARI foram o primeiro contato do Direito com essa problemática, a qual posteriormente veio a se desenvolver como a proteção dos dados pessoais. O primeiro caso ocorreu nos Estados Unidos da América, em 1965, quando o Escritório do Orçamento (*Bureau of Budget*) norte-americano apresentou a proposta de construir uma central única para o armazenamento de informações pessoais dos cidadãos norte-americanos (*National Data Center*), as quais ficariam disponíveis para diversos órgãos da administração pública federal, com vistas ao aumento de eficiência do governo, sem considerações sobre a privacidade dos cidadãos. Essa proposta acabou causando revolta em diversos setores da sociedade, os quais levantaram questões a respeito da equação entre a assimetria de poder e a liberdade do indivíduo. Essa concentração excessiva de dados em um único local pode causar uma assimetria de poder muito grande entre governo e cidadão, o que causa o receio de afronta à democracia. Frente à essa movimentação, o Congresso norte-americano realizou audiências com o intuito

---

[289] Ver REGAN, Priscilla. **Legislating Privacy**: Technology, social values, and public policy. Chapel Hill: The University of North Carolina Press, 1995. p. 212-243.

[290] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 44-45.

[291] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 4045-4049.

[292] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 144-145.

de discutir os efeitos da centralização das informações em um único banco de dados, acabando por recomendar que o banco de dados nacional não fosse criado sem que a proteção da privacidade dos cidadãos fosse garantida ao máximo nível possível. Essa recomendação fundamentou-se, principalmente, na proteção da dignidade e da personalidade dos indivíduos. Após a recomendação do Congresso, o projeto foi encerrado, sem, no entanto, procurar regular o tratamento de dados sensíveis ou a necessidade de tratamento de dados pessoais pelo governo.[293]

O caso norte-americano inspirou outros países a criarem iniciativas semelhantes ao *National Data Center,* como é o caso da França. Em 1970 o *Instituit National de la Statistique* idealizou o SAFARI (*Système Automatisé pour les Fichiers Administratifs et le Rèpertoire des Individus*), que consistia na transferência dos dados pessoais de cidadãos que estivessem em posse da administração pública para sistemas informatizados, além de criar um número único de identificação para cada indivíduo, atribuído no momento do nascimento, com validade perante o Estado. Assim como no caso norte-americano, o projeto tinha por intuito melhorar a eficiência da administração pública, no entanto, também não veio acompanhado de uma análise dos riscos à privacidade dos cidadãos que o sistema poderia vir a causar. Desse modo, o SAFARI não foi bem recebido pela sociedade francesa e em 1974 o primeiro-ministro francês, por meio de uma medida administrativa, interditou a realização de interconexões de dados entre ministérios, encerrando o projeto SAFARI.[294]

É digno de nota, ainda, o caso do censo alemão. A República Federal da Alemanha possuía uma lei federal sobre a proteção de dados pessoais desde 1977, já existindo, portanto, uma cultura de proteção de dados no país. Nesse cenário, o censo alemão, que deveria ser finalizado em 1983, provocou questionamentos em diversos setores da sociedade a respeito do método da coleta de informações utilizado e o destino dos dados coletados, o que deu causa à uma célebre sentença do Tribunal Constitucional Alemão. A controvérsia se deu, principalmente, tendo em vista que a lei que organizava o censo previa: a possibilidade de que os dados coletados fossem correlacionados com dados do registro civil; a possibilidade de que os dados, desde que não identificados, pudessem ser transmitidos às autoridades federias; e a existência de multa pecuniária para aqueles que se recusassem a responder o questionário de

---

[293] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 3815-3878.

[294] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 3883-3908.

coleta de dados, bem como um favorecimento a quem denunciasse tais pessoas. Apesar da insegurança que a lei do censo passava aos cidadãos, a lei de proteção de dados não foi capaz de enfrentar os pontos controversos daquela. Além disso, em 1978, um juiz administrativo havia decidido que as leis referentes à coleta de dados para fins estatísticos seriam superiores à lei de proteção de dados pessoais em caso de conflito. Assim, perante tais controvérsias e inseguranças, o Tribunal Constitucional reconheceu a incompatibilidade da Lei do Censo à Lei Fundamental, suspendendo provisoriamente o censo.[295] A sentença do Tribunal tornou-se referência na matéria de proteção de dados pessoais.

Importa ressaltar alguns dos motivos que levaram o Tribunal a decidir a respeito da inconstitucionalidade da lei do censo. Um deles diz respeito à questão da finalidade da coleta de dados. A sentença observou que caso os dados coletados fossem utilizados tanto para fins administrativos, quanto para fins estatísticos, restaria caracterizada uma dualidade de finalidades incompatíveis – na medida em que o rigor estatístico não pode coexistir com a necessidade de órgãos administrativos de identificar titulares de dados -, impedindo que o cidadão, titular dos dados pessoais, tomasse ciência sobre o uso efetivo de seus dados.[296]

Ainda, o Tribunal Constitucional desmistifica a noção de que alguns tipos de dados seriam irrelevantes. Segundo o disposto na sentença, o determinante não é somente a natureza da informação em si, mas também a sua necessidade e a finalidade de sua utilização, tendo em vista que um dado que de início pode parecer irrelevante para a privacidade, aparentando não possuir importância alguma, pode adquirir novo valor dependendo de seu tratamento, do seu cruzamento com outros dados, e das finalidades desse tratamento. Nesse sentido:

> O fato de informações dizerem respeito a processos íntimos não decide por si só se elas são sensíveis ou não. É muito mais necessário o conhecimento do contexto de utilização, para que se constate a importância do dado em termos de direito da personalidade: Só quando existe clareza sobre a finalidade para a qual os dados são solicitados e quais são as possibilidades de uso e ligação [destes com outros] que existem, pode-se saber se a restrição do direito de autodeterminação da informação (no caso) é admissível. Deve-se distinguir entre dados referentes à pessoa, que são levantados e manipulados de forma individualizada e não anônima (v. item "a" abaixo), e aqueles que são destinados a fins estatísticos (v. item "b" abaixo).[297]

---

[295] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 3905-3936.

[296] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 3934-3963.

[297] MARTINS, Leonardo (org.). **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Tradução de Beatriz Hennig et al. Montevideo/Berlin: Konrad-Adenauer-Stiftung E. V., 2005. p. 239.

Por fim, ressalta-se o uso da expressão "autodeterminação informativa" na sentença, designando o direito dos indivíduos a controlar quando e dentro de quais limites seus dados podem ser utilizados por terceiros.[298] De acordo com a sentença, a autodeterminação individual sobre a informação pressupõe a garantia da liberdade de decisão sobre ações relativas à suas informações, sendo as restrições à esse direito permitidas apenas em casos em que o interesse público é predominante, necessitando de uma base legal constitucional e observando sempre o princípio da proporcionalidade com o fim de evitar riscos de violação do direito da personalidade.[299] Segundo o Tribunal:

> Daí resulta: O livre desenvolvimento da personalidade pressupõe, sob as modernas condições do processamento de dados, a proteção do indivíduo contra levantamento, armazenagem, uso e transmissão irrestritos de seus dados pessoais. Esta proteção, portanto, é abrangida pelo direito fundamental do Art. 2 I c. c. Art. 1 I GG. O direito fundamental garante o poder do cidadão de determinar em princípio ele mesmo sobre a exibição e o uso de seus dados pessoais.[300]

O conceito de autodeterminação informativa não é em si uma inovação, tendo em vista que já se encontrava presente na doutrina norte-americana. No entanto, ressalta-se sua importância para a disciplina de proteção de dados pessoais, orientando-a até os dias atuais, não só na Alemanha, quanto em outros países do sistema jurídico romano-germânico, estando, inclusive, presente na LGPD como um de seus fundamentos (art. 2º, II)[301]. O direito à autodeterminação informativa é concebido como um direito fundamental, estando correlacionado ao direito geral de personalidade.[302]

Em consequência à essa decisão, uma nova lei sobre o censo foi promulgada com o fim de corrigir os pontos contestados. De modo geral, a decisão teve grande influência sobre a disciplina de proteção de dados pessoais em diversos pontos, sendo um deles a solidificação do entendimento de que a proteção de dados pessoais requer embasamento constitucional. A

---

[298] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 3955-3963.

[299] MARTINS, Leonardo (org.). **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Tradução de Beatriz Hennig et al. Montevideo/Berlin: Konrad-Adenauer-Stiftung E. V., 2005. p. 235, 237.

[300] MARTINS, Leonardo (org.). **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Tradução de Beatriz Hennig et al. Montevideo/Berlin: Konrad-Adenauer-Stiftung E. V., 2005. p. 235, 238.

[301] BRASIL. Lei 13.709, de 14 de agosto de 2018. **Diário Oficial [da] União**, Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 nov. 2021.

[302] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 3968-3971.

decisão influenciou, também, uma mudança de entendimento da matéria na Europa, a qual até então se fundamentava na doutrina da "liberdade informática", sendo essa uma leitura do direito à autodeterminação informativa que se aproxima com o direito à privacidade, dizendo respeito à um direito de conhecimento e controle dos dados pessoais. Ambas as doutrinas influenciaram a matéria grandemente, no entanto, ambas sofreram críticas.[303]

Em relação à autodeterminação informativa a crítica diz respeito a uma interpretação em chave liberal, segundo a qual a autodeterminação estaria ligada ao ato de consentir do titular dos dados, o que daria ensejo a interpretações negociais e patrimoniais, afastando-o do âmbito dos direitos de personalidade. Em relação à liberdade informática, a principal crítica diz respeito ao fato de que, ao fazer referência à liberdade, utiliza-se um conceito muito amplo e afastado da trajetória histórica e dos avanços dos direitos fundamentais, o que torna possível uma leitura "hipertrofiada" da possibilidade de autodeterminação. Uma segunda crítica refere-se à referência à informática, uma vez que, ainda que uma consciência da tecnologia seja necessária ao jurista, estruturar categorias gerais em torno de fenômenos tecnológicos específicos, como a informática, pode minimizar seus efeitos e acelerar sua obsolescência.[304] Nas palavras de Doneda:

> Particularmente em relação à informática, a crítica que podemos fazer (valendo-nos das décadas que nos separam) é a de que os efeitos das tecnologias informáticas penetraram de tal modo em várias instâncias da vida dos cidadãos, sejam usuários diretos ou não de computadores, que separar os fenômenos relativos à informática de outros ("tradicionais", digamos) tornou-se ao mesmo tempo impossível e irrelevante. Deve-se, por outro lado, reforçar as categorias tradicionais com vistas aos fenômenos advindos com a tecnologia e com a informática, pois separá-los seria, hoje, contraproducente. A tal ponto a informática está presente no nosso cotidiano que individuar os casos nos quais ela é aplicada é tarefa destinada ao mais retumbante fracasso.[305]

Diante dessas críticas, uma melhor expressão para a matéria, segundo o autor, seria a expressão "proteção de dados pessoais", tendo em vista que a partir dela pode-se inferir tanto a problemática da privacidade, quanto a da informação, estando isenta de interpretações

---

[303] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 3971-3992.

[304] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 3992-4026.

[305] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 4015-4026.

patrimonialistas e tendo como referência os direitos de personalidade.[306] Além de ser essa a expressão utilizada pela legislação brasileira sobre a matéria, sendo a autodeterminação informativa um dos fundamentos da disciplina de proteção de dados pessoais segundo a LGPD[307], conforme já mencionado.

A proteção de dados pessoais, portanto, surge para atualizar a proteção da privacidade, aprofundando-a e expandindo-a frente aos novos riscos e aos novos interesses exemplificados pelos casos descritos, os quais demonstram o impulso tecnocrático da administração pública a partir da década de 1960. Nesse sentido, observa-se a influência desses casos na disciplina, uma vez que eles foram o impulso inicial da matéria, a qual teve suas primeiras iniciativas legislativas[308] logo depois, marcadas pela ideia de que direitos e liberdades fundamentais corriam riscos de violação pela coleta irrestrita de dados pessoais por parte do Estado. Essas primeiras legislações abarcavam princípios de proteção abstratos, centrados no processamento de dados, bem como algumas regras específicas dirigidas aos agentes que realizavam o tratamento dos dados. A opção pelos princípios mais generalizados se deu, principalmente, pela falta de experiência com tecnologias e suas consequências. No entanto, ainda que existissem normas abstratas, o conteúdo das leis era muito condicionado pelas tecnologias disponíveis no momento, o que fez com que essas se tornassem ultrapassadas rapidamente, principalmente devido à multiplicação dos centros de processamento de dados.[309]

Nesse sentido, surge a segunda geração de leis sobre a disciplina a partir da segunda metade da década de 1970, sendo a primeira delas a lei francesa *Informatique et Libertés* de 1978. A principal diferença entre essas e as lei de primeira geração é o fato de que essas se centravam, principalmente, em torno da privacidade e da proteção de dados pessoais como liberdades negativas e não mais em torno do fenômeno tecnológico em si. Desse modo, foram criados instrumentos para que o próprio cidadão pudesse identificar o uso indevido de suas

---

306 DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 4023-4033.

307 BRASIL. Lei 13.709, de 14 de agosto de 2018. **Diário Oficial [da] União**, Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 nov. 2021.

308 As primeiras legislações sobre a matéria foram: a Lei de *Hesse* (estado alemão) de 1970, uma lei estadual; o *Datalag* 1973:289 (Estatuto para bancos de dados), a primeira lei nacional de proteção de dados, datada de 1973, na Suécia; e o *Privacy Act* norte-americano de 1974. Tais documentos são conhecidos hoje como leis de "primeira geração". (DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 4081-4089).

309 DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 4066-4115.

informações pessoais e propor sua tutela. Estas leis, por sua vez, também passaram a apresentar alguns problemas, uma vez que a coleta de dados pessoais passou a ser cada vez mais intensa, tanto pelo Estado, quanto por entes privados, e, assim, o fornecimento desses pelos cidadãos tornou-se indispensável para a sua participação na vida em sociedade. Assim, o exercício individual dessa liberdade tinha consequências amplas, pois a interrupção de fornecimento de dados pessoais poderia impedir a própria socialização das pessoas.[310]

Essas questões motivaram o surgimento de uma terceira geração de leis a partir da década de 1980. Essas continuaram voltadas ao cidadão, no entanto, procuraram garantir a efetividade da liberdade do indivíduo em fornecer ou não seus dados pessoais. Essas leis consideravam a proteção de dados como um processo complexo, levando em consideração o contexto da solicitação dos dados, bem como estabelecendo mecanismos de proteção ao indivíduo em casos em que a liberdade de decidir sobre o fornecimento ou não de seus dados é cerceada por condicionantes, ou seja, para impedir que a socialização dos cidadãos dependesse necessariamente de sua concordância em fornecer seus dados pessoais, como era feito anteriormente. Assim, essas leis pretendiam incluir o cidadão no processo de tratamento de dados pessoais, não só na simples permissão ou não da coleta dos dados, mas em suas demais fases. O marco inicial dessa geração de leis foi a decisão do Tribunal Constitucional Alemão de 1983 anteriormente mencionado, o que demonstra a importância dessa sentença alemã para a matéria de proteção de dados pessoais.[311]

No entanto, essa geração também apresentou problemas, na medida em que nem todo mundo estava disposto a exercer seu direito à autodeterminação informativa devido aos custos econômicos e sociais envolvidos. Assim, surgem as leis de quarta geração, as quais tentam suprir as inúmeras desvantagens do enfoque individual, procurando fortalecer a posição do cidadão em relação à entidade que processa os dados, na tentativa de equilibrar a relação, bem como reduzindo a importância da decisão individual de autodeterminação informativa até então existente. Ainda, disseminam a criação de autoridades independentes para a fiscalização da atuação da lei, bem como a disseminação de normativas conexas a elas, mas que estabeleçam normas específicas para determinados setores onde são realizados o processamento de dados

---

[310] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 4113-4142.

[311] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 4140-4163.

(como o setor de saúde ou de fornecimento de crédito ao consumidor), abarcando as particularidades de cada setor. [312]

Esse histórico de leis auxiliou no desenvolvimento de alguns princípios base para a proteção de dados pessoais, os quais encontram expressão em dois documentos de relevância internacional: a Convenção do Conselho da Europa de 18 de janeiro de 1981 e a Recomendação da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) de 23 de setembro de 1980; esses princípios são o núcleo de proteção de dados que todo ordenamento deve abarcar, estando presentes em diversas leis, tratados, convenções e acordos privados, ainda que adaptados.[313] São eles:

a. Princípio da correção na coleta e no tratamento de dados para garantir a exatidão dos dados;[314]
b. Princípio da exatidão dos dados coletados, os quais devem ser fiéis à realidade, exigindo-se sua atualização;[315] [316]
c. Princípio da finalidade da coleta e tratamento de dados[317], que deve ser informada ao titular dos dados antes de sua ocorrência, e que se desdobra em:
    i. princípio da pertinência entre a finalidade perseguida e os dados colhidos;
    ii. princípio da utilização não-abusiva dos dados coletados em relação à finalidade;
    iii. princípio do direito ao esquecimento, que diz respeito à eliminação ou a transformação dos dados que não são mais necessários em dados anônimos.[318]

---

[312] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 4157-4184.

[313] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 59

[314] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 59.

[315] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 59.

[316] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 4221-4226.

[317] Esse princípio apresenta utilidade prática, na medida em que, por meio dele restringe-se a transferência de dados pessoais a terceiros, bem como pode-se estruturar critérios de razoabilidade para avaliar a utilização de certos dados para certas finalidades. (DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 4221-4226.)

[318] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 59

d. Princípio da publicidade dos bancos de dados pessoais, os quais devem, necessariamente, ser de conhecimento público e devem possuir autorização prévia para funcionar;[319] [320]
e. Princípio do acesso individual (ou livre acesso) aos bancos de dados pessoais pelos indivíduos titulares desses dados, com o intuito de obter ciência sobre quais dados pessoais seus foram coletados, obtendo cópia dos registros, e tendo a possibilidade de controle sobre os dados, que poderão ser corrigidos, complementados ou eliminados, quando forem obsoletos ou tenham sido coletados ilegitimamente;[321] [322]
f. Princípio da segurança física e lógica dos dados, os quais devem ser protegidos contra riscos de extravio, destruição, modificação, acessos ou transmissões não autorizadas etc.[323] [324]

Da leitura desses princípios pode-se observar que a proteção de dados passa de uma enunciação negativa e passiva, na qual o indivíduo apenas poderia acionar seus direito diante de um órgão *ad hoc* após haver uma violação; para uma enunciação positiva e dinâmica, a qual oferece ao indivíduo mecanismos de controle direto e contínuo sobre os agentes de coleta e tratamento de dados pessoais, independentemente da existência concreta de uma violação, já que o indivíduo possui além do direito de controle, o direito de acesso aos seus dados. Combinado com a característica de instituição de órgãos criados especificamente para verificar e garantir a efetividade das normas, é dado à proteção de dados cada vez mais um enfoque funcional.[325]

---

[319] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 59.
[320] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 4217-4218.
[321] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 59.
[322] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 4226-4233.
[323] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 59.
[324] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 4233-4234.
[325] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 60-61.

No ordenamento jurídico brasileiro o que se observa é que a Constituição Federal de 1988, de início, contemplava a questão da informação apenas por meio de garantias à liberdade de expressão (art. 5º, IV e IX[326] e art. 220[327]) e do direito à informação (art. 5º, XIV, XXXIII e XXXIV, b[328] e art. 220), bem como por meio da garantia de acesso e retificação de dados por meio da ação de *habeas data* (art. 5º, LXXII[329]). Além de contemplar o direito à privacidade como garantia da inviolabilidade da vida privada, da intimidade, honra e imagem (art. 5º, X[330]) e da correspondência, das comunicações telefônicas, telegráficas ou de dados (art. 5º, XII[331]). No entanto, não há a garantia do direito à proteção de dados conforme entendido pela doutrina, de um direito de controle sobre os próprios dados, bem como de princípios que regem o tratamento de dados pessoais, evitando riscos ao indivíduo.[332]

---

[326] Art. 5º. IV - é livre a manifestação do pensamento, sendo vedado o anonimato;
IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença; (BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial [da] União**, Brasília, 5 de out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 15 nov. 2021).

[327] Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição.
§ 1º Nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação social, observado o disposto no art. 5º, IV, V, X, XIII e XIV.
§ 2º É vedada toda e qualquer censura de natureza política, ideológica e artística. (BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial [da] União**, Brasília, 5 de out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 15 nov. 2021).

[328] Art. 5º. XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;
XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado;
XXXIV - são a todos assegurados, independentemente do pagamento de taxas: b) a obtenção de certidões em repartições públicas, para defesa de direitos e esclarecimento de situações de interesse pessoal; (BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial [da] União**, Brasília, 5 de out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 15 nov. 2021).

[329] Art. 5º. XXII - conceder-se-á "habeas-data":
a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo; (BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial [da] União**, Brasília, 5 de out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 15 nov. 2021).

[330] Art. 5º. 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. Constituição da República Federativa do Brasil de 1988. **Diário Oficial [da] União**, Brasília, 5 de out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 15 nov. 2021).

[331] 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; (BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial [da] União**, Brasília, 5 de out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 15 nov. 2021).

[332] BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial [da] União**, Brasília, 5 de out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 15 nov. 2021

De início, apenas a privacidade estaria expressamente tutelada constitucionalmente, sendo que a proteção de dados pessoais encontrava respaldo em previsões esparsas e que não estabeleciam garantias de proteção de dados pessoais como entendidas internacionalmente, especialmente por meio dos princípios já elencados. A sistemática da Constituição de 1988 em relação à matéria fortalecia uma interpretação que simplificava os fundamentos da tutela de dados pessoais, na medida em que as informações eram protegidas somente em relação à sua comunicação. No entanto, garantir uma tutela apenas para a comunicação ou interceptação de dados não abrange a complexidade dos riscos que o tratamento de dados pessoais cria para os indivíduos, especialmente com o desenvolvimento do poder computacional. De acordo com Doneda, isso poderia impedir a aplicação da tutela da privacidade ou de outros direitos fundamentais que foram violados, não de forma direta, mas por meio da utilização abusiva de dados pessoais, que é o caso de algumas técnicas de vigilância por meio da coleta e tratamento de dados já mencionadas, as quais criam incontáveis riscos de violação à diversos direitos fundamentais.[333]

Frente aos crescentes riscos e a tutela insuficiente à proteção de dados pessoais, percebe-se um grande avanço na matéria dentro do ordenamento jurídico brasileiro ao passar dos anos, especialmente com a promulgação das Leis 12.965/2014[334] e 13.709/2018[335] (Marco Civil da Internet e Lei Geral de Proteção de Dados Pessoais respectivamente). A primeira lei já previa algumas garantias relacionadas à proteção de dados pessoais, no entanto, quem solidificou a matéria foi a segunda, tendo em vista que trata da proteção de dados pessoais em qualquer relação que envolva o tratamento de dados, por qualquer meio, tendo como fundamentos (art. 2º): i) o respeito à privacidade; ii) a autodeterminação informativa; iii) a liberdade de expressão, informação, comunicação e opinião; iv) a inviolabilidade da intimidade, da honra e da imagem; v) o desenvolvimento econômico e tecnológico e a inovação; vi) a livre iniciativa, a livre concorrência e a defesa do consumidor; vii) os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.[336]

---

[333] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. Edição do Kindle. Posição 7045-

[334] BRASIL. Lei 12. 965, de 23 de abril de 2014. Diário Oficial [da] União, Brasília, 23 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 15 nov. 2021.

[335] BRASIL. Lei 13.709, de 14 de agosto de 2018. **Diário Oficial [da] União**, Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 out. 2021.

[336] BRASIL. Lei 13.709, de 14 de agosto de 2018. **Diário Oficial [da] União**, Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 nov. 2021.

A LGPD vem para fortalecer a proteção de inúmeros direitos fundamentais, como a privacidade, a liberdade de expressão, a liberdade de informação, de opinião e comunicação, a inviolabilidade da intimidade, da honra e da imagem, e o desenvolvimento da personalidade, por meio de normas principiológicas e normas técnicas de proteção de dados pessoais, para dar funcionalidade à matéria e permitir a verificação de cumprimento da lei.[337]

Nesse sentido, de acordo com Patrícia Peck Pinheiro:

> O espírito da lei foi proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, trazendo a premissa da boa-fé para todo o tipo de tratamento de dados pessoais, que passa a ter que cumprir uma série de princípios, de um lado, e de itens de controles técnicos para governança da segurança das informações, de outro lado, dentro do ciclo de vida do uso da informação que identifique ou possa identificar uma pessoa e esteja relacionada a ela, incluindo a categoria de dados sensíveis.[338]

Desse modo, a legislação prevê preceitos principiológicos, os quais devem ser cumpridos por meio das normas técnicas obrigacionais impostas aos agentes responsáveis pelo tratamento, incluindo a administração pública, em observação aos direitos dos titulares de dados pessoais, com a finalidade de proteger uma série de direitos fundamentais por meio da garantia do direito à proteção de dados pessoais. Assim, para a análise da legalidade e legitimidade de uma tecnopolítica de vigilância implementada pelo Estado que envolva a coleta e o tratamento de dados pessoais em seu exercício, deve ser verificado o seu atendimento às obrigações impostas à administração pública, aos direitos dos titulares de dados e aos preceitos principiológicos da LGPD.

De acordo com o art. 6º da LGPD, o tratamento de dados pessoais deve observar, além dos princípios anteriormente mencionados (princípio da correção, da exatidão ou qualidade dos dados, da finalidade, da publicidade ou transparência, do livre acesso e da segurança), os seguintes princípios[339]:

a) Princípio da adequação, segundo o qual deve haver compatibilidade entre o tratamento e a finalidade informada ao titular;

---

337 PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais**. 3ª ed. São Paulo: Saraiva Jur, 2021. Edição do Kindle. p. 22, 43.
338 PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais**. 3ª ed. São Paulo: Saraiva Jur, 2021. Edição do Kindle. p. 21.
339 BRASIL. Lei 13.709, de 14 de agosto de 2018. **Diário Oficial [da] União**, Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 nov. 2021.

b) Princípio da necessidade, segundo o qual os dados coletados e o tratamento devem ser limitados ao mínimo necessário, sendo proporcional e não excessivo, para a realização de sua necessidade;
c) Princípio da prevenção, segundo o qual deve, necessariamente, haver a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
d) Princípio da não discriminação, segundo o qual fica vedado o tratamento de dados pessoais para fins discriminatórios, ilícitos ou abusivos; e
e) Princípio da responsabilização e prestação de contas, segundo o qual, o agente deve demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, bem como sua eficácia.

Para que o tratamento de dados pessoais seja legítimo, esses princípios devem ser atendidos.[340] Ainda, a lei traz alguns requisitos para que o tratamento possa ser realizado, importando destacar, entre eles, as hipóteses em que o tratamento é permitido (art. 7º), sendo elas: mediante o consentimento do titular; para o cumprimento de obrigação legal ou regulatória do controlador; para a realização de estudos por órgão de pesquisa; para a execução de contrato ou procedimentos preliminares; para o exercício regular de direitos em processos judicial, administrativo ou arbitral; para a proteção da vida ou incolumidade física do titular ou terceiro; para a tutela da saúde por profissionais de saúde, serviços de saúde ou autoridade sanitária; para atender os interesses legítimos do controlador ou terceiro; para proteção do crédito; e, por fim, para a execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.[341]

Em relação aos dados pessoais sensíveis, o tratamento só poderá ocorrer (artigo 11): se o titular ou seu responsável legal consentir; para cumprimento de obrigação legal ou regulatória pelo controlador; quando necessário à execução de políticas públicas previstas em leis ou regulamentos; para a realização de estudos por órgão de pesquisa; para o exercício regular de direitos, em contrato ou processo judicial, administrativo ou arbitral; para a proteção da vida ou incolumidade física do titular ou terceiro; para tutela da saúde feita exclusivamente por

[340] PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais**. 3ª ed. São Paulo: Saraiva Jur, 2021. Edição do Kindle. p. 43.
[341] BRASIL. Lei 13.709, de 14 de agosto de 2018. **Diário Oficial [da] União**, Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 nov. 2021.

profissionais de saúde, serviços de saúde ou autoridade sanitária; para garantia da prevenção à fraude e à segurança do titular, em processos de identificação ou autenticação de cadastro.[342]

A coleta e o tratamento de dados realizado pelo Estado durante o exercício de vigilância geralmente possui duas finalidades: controle e administração da população e policiamento e segurança. Essa última, no entanto, não é tutelada pela LGPD, tendo em vista que o art. 4º elenca o tratamento de dados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais como hipóteses em que a lei não se aplica, ficando a regulamentação dessas hipóteses e outras a cargo de lei específica.[343]

Em relação a finalidade de controle e administração, tem-se que essa se coaduna com a hipótese de tratamento de dados pessoais prevista nos artigos 7º, III e 11, II, b da LGPD, os quais trazem como hipóteses legais para o tratamento de dados aquele realizado pela administração pública quando necessário à execução de políticas públicas previstas em leis ou regulamentos. Nesse sentido, ao implementar tecnopolíticas de vigilância para fins de melhoria da eficácia na administração e criação e execução de políticas públicas, que envolvam o tratamento de dados, o poder público deve observar o disposto na lei, especialmente o capítulo IV, o qual trata especificamente sobre o tratamento de dados pessoais pelo poder público, bem como os preceitos principiológicos do artigo 6º da lei, já mencionados.[344]

O capítulo IV da LGPD traz regras para a realização de tratamento de dados pessoais por órgãos públicos (artigos 23-30), bem como a previsão de responsabilidade desses órgãos em caso de violação dessas regras (artigos 31 e 32). Destaca-se que o tratamento de dados pessoais pelo poder público deve ser realizado, necessariamente, para o atendimento da finalidade pública do órgão, na persecução do interesse público e com a finalidade de executar as competências legais ou cumprir as atribuições legais do serviço público (art. 23, *caput*). Ainda, o órgão público deve informar a hipótese legal (daquelas previstas nos artigos 7º e 11º) em que realizam o tratamento de dados pessoais, bem como a finalidade, os procedimentos e as práticas utilizadas durante o tratamento, em veículo de fácil acesso, de preferência em seu

[342] BRASIL. Lei 13.709, de 14 de agosto de 2018. **Diário Oficial [da] União**, Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 nov. 2021.
[343] BRASIL. Lei 13.709, de 14 de agosto de 2018. **Diário Oficial [da] União**, Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 nov. 2021.
[344] BRASIL. Lei 13.709, de 14 de agosto de 2018. **Diário Oficial [da] União**, Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 nov. 2021.

sítio eletrônico (artigo 23, I); além de indicar um encarregado do tratamento nos termos do art. 39[345] da mesma lei (artigo 23, III).[346]

Observa-se, portanto, a importância que a lei dá à transparência dos processos de tratamento de dados pessoais, bem como ao direito à informação dos titulares dos dados, os quais devem não só ter ciência que seus dados foram coletados e estão sendo tratados, mas devem, também, conhecer a finalidade desse tratamento e os procedimentos, práticas e técnicas de tratamento utilizados no exercício. Ainda, a lei garante ao titular um direito de controle sobre seus próprios dados pessoais, outorgando à ele o direito de obter do controlador, a qualquer momento e mediante requisição: a confirmação da existência de tratamento (artigo 18, I); acesso aos dados (artigo 18, II); correção de dados inexatos, desatualizados ou incompletos (artigo 18, III); a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade legal (artigo 18, IV); a portabilidade dos dados a outro fornecedor de serviço ou produto (artigo 18, V); a eliminação de dados tratados com consentimento do titular (artigo 18, VI); a informação de quais entidades tiveram acesso aos seus dados por meio do compartilhamento (artigo 18, VII); a informação sobre a possibilidade de não fornecer consentimento e sobre as consequências disso (artigo 18, VIII); e a revogação do consentimento (artigo 18, IX).[347] Desse modo, a lei impõe um cuidado preventivo com os dados pessoais quando do tratamento.

Em seu artigo 26, a lei dispõe sobre o uso compartilhado de dados pessoais pelo poder público, o qual deve atender à finalidade específica de execução de políticas públicas e atribuição legal pelos órgãos e entidades públicas, sempre respeitados os princípios de proteção de dados pessoais. Fica vedado ao poder público transferir esses dados a entidades privadas, exceto nos casos: em que houver execução descentralizada de atividade pública que exija essa transferência, a qual deverá ser feita exclusivamente para esse fim (artigo 26, §1º, I) ; em que esses dados forem acessíveis publicamente (artigo 26, §1º, III); em que houver previsão legal ou contrato, convênios ou instrumentos congêneres (artigo 26, §1º, IV); em que a transferência objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a

[345] "Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria". (BRASIL. Lei 13.709, de 14 de agosto de 2018. **Diário Oficial [da] União**, Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 nov. 2021.)

[346] BRASIL. Lei 13.709, de 14 de agosto de 2018. **Diário Oficial [da] União**, Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 nov. 2021.

[347] BRASIL. Lei 13.709, de 14 de agosto de 2018. **Diário Oficial [da] União**, Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 nov. 2021.

segurança e a integridade dos dados, sendo vedado o tratamento para outras finalidades (artigo 26, §1º, V).[348]

Todos esses mecanismos mencionados têm por intuito controlar a prática de coleta e tratamento de dados de forma irrestrita. O regime de proteção de dados pessoais, estabelecido pela LGPD, é procedimental, o que significa que ele é voltado ao estabelecimento de garantias que instituem certo equilíbrio e confiança entre o titular dos dados e o agente de tratamento desses dados, bem como que estabeleça obrigações procedimentais a esses agentes, ao invés de proibir o tratamento de dados pessoais. Portanto, diante do aumento crescente no exercício da vigilância estatal, da evolução quantitativa e qualitativa da vigilância, bem como dos riscos de violação de direitos fundamentais por meio da coleta e tratamento de dados irrestritos para o exercício dessa vigilância, a lei e a disciplina da proteção de dados pessoais vêm para assegurar que o titular desses dados tenha uma série de direitos, ligados à um poder maior de controle sobre seus próprios dados, visando à garantia de seus direitos e liberdades fundamentais, e evitando que a vigilância necessária à atuação do Estado seja excessiva e demasiadamente autoritária, ferindo direitos da personalidade e mitigando processos democráticos.

Faz-se oportuno ressaltar, no entanto, que apesar da grande contribuição da LGPD para a matéria, a previsão de que a proteção de dados pessoais garantida pela lei não se aplica aos casos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (art. 4º, III da LGPD)[349], bem como o estabelecimento de que o Estado, por intermédio da Autoridade Nacional de Proteção de Dados, pode dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência" (art. 40 da LGPD)[350], indicam que o poder público, por meio de seus órgãos e entidades, possui poderes tanto fiscalizatórios, quanto regulatórios. Como bem colocado por Boff e Leal, questiona-se quem controla o Estado, isto é, quem controla o controlador?[351]

---

[348] BRASIL. Lei 13.709, de 14 de agosto de 2018. **Diário Oficial [da] União**, Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 nov. 2021.

[349] BRASIL. Lei 13.709, de 14 de agosto de 2018. **Diário Oficial [da] União**, Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 nov. 2021.

[350] BRASIL. Lei 13.709, de 14 de agosto de 2018. **Diário Oficial [da] União**, Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 nov. 2021.

[351] BOFF, Salete Oro; LEAL, Dionis Janner. Dados pessoais, psicopoder e responsabilização: análise a partir da lei brasileira de proteção de dados. In: **Revista da Faculdade de Direito da UERJ**, Rio de Janeiro, n 39, jun. 2021, pp. 151-170. p. 161.

Confirmando a importância da proteção de dados pessoais, tem-se que esse direito teve sua autonomia em relação ao direito à privacidade reconhecida por decisão do Plenário do Supremo Tribunal Federal na Ação Direta de Inconstitucionalidade nº 6.387/DF[352], a qual impugnava a Medida Provisória 954 de 17 de abril de 2020[353]. Em seu voto, a Ministra Relatora Rosa Weber deferiu a cautelar, suspendendo a eficácia da medida, fundamentando que:

> A Constituição da República confere especial proteção à intimidade, à vida privada, à honra e à imagem das pessoas ao qualificá-las como invioláveis, enquanto direitos fundamentais da personalidade, assegurando indenização pelo dano material ou moral decorrente de sua violação (**art. 5º, X**). O assim chamado direito à privacidade (*right to privacy*) e os seus consectários direitos à intimidade, à honra e à imagem emanam do reconhecimento de que a personalidade individual merece ser protegida em todas as suas manifestações.
> A fim de instrumentalizar tais direitos, a Constituição prevê, no **art. 5º, XII,** a **inviolabilidade do "*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 penal*".
> [...]
> Tais informações, relacionadas à **identificação – efetiva ou potencial – de pessoa natural**, configuram **dados pessoais** e integram, nessa medida, o 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**). Sua manipulação e tratamento, desse modo, hão de observar, sob pena de lesão a esses direitos, os limites delineados pela proteção constitucional.
> 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**.
> [...]
> Independentemente do seu conteúdo, mutável com a evolução tecnológica e social, no entanto, permanece como denominador comum da privacidade e da autodeterminação o entendimento de que a privacidade somente pode ceder diante de justificativa consistente e legítima. Em seus dizeres, "*a invasão injustificada da privacidade individual deve ser repreendida e, tanto quanto possível, prevenida*". (grifo do autor).[354]

Assim, há o reconhecimento de que o direito à proteção de dados pessoais é um direito autônomo, bem como deve ser reconhecido como um direito fundamental, diretamente

---

[352] BRASIL. Supremo Tribunal Federal. **ADI 6.387 MC / DF**. Plenário. Relator: Min. Rosa Weber. Data de julgamento: 07/05/2020.

[353] A medida provisória 954/2020, a qual teve sua vigência encerrada no dia 14 de agosto de 2020, dispunha "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". (BRASIL. Congresso Nacional. Ato declaratório do Presidente da Mesa do Congresso Nacional nº 112 de 2020. **Diário Oficial [da] União**, 20 ago. 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Congresso/adc-112-mpv954.htm. Acesso em: 15 nov. 2021).

[354] BRASIL. Supremo Tribunal Federal. **ADI 6.387 MC / DF**. Plenário. Relator: Min. Rosa Weber. Data de julgamento: 07/05/2020. Decisão Monocrática concessiva da liminar da Relatora Ministra Rosa Weber de 24/04/2020, P. 20-21.

relacionado com os direitos de liberdade, da privacidade e do livre desenvolvimento da personalidade, devendo, portanto, ser observado, sob pena de lesão a esses direitos. Ainda, corroborando a decisão da Ministra Rosa Weber, o direito à proteção de dados pessoais teve seu *status* de direito fundamental reconhecido por meio de aprovação, em 20 de outubro de 2021, da Proposta de Emenda à Constituição (PEC) 17/2019[355], a qual propôs a inclusão do direito à proteção de dados pessoais, inclusive nos meios digitais, na Constituição Federal como um direito fundamental, incluído entre as cláusulas pétreas, remetendo privativamente à União a função de legislar sobre o tema. Assim, no dia 10 de fevereiro de 2022, o Congresso Nacional promulgou a Emenda Constitucional 115/22, acrescentando ao artigo 5º da Constituição Federal o inciso LXXIX, que assegura o direito à proteção de dados pessoais.[356] [357]

Observa-se que, assim como o direito à privacidade, a disciplina de proteção de dados pessoais está diretamente relacionada aos direitos de personalidade, sendo, portanto, um direito que surgiu para dar continuação ao direito à privacidade, expandindo-o e atualizando-o frente aos novos riscos. Diante das novas técnicas de exercício de vigilância, as quais revolvem em torno da coleta e tratamento de dados, o surgimento da disciplina mostrou-se de extrema necessidade para garantir certo equilíbrio na relação entre cidadão e Estado nos contextos de vigilância. Desse modo, a partir dos regramentos técnicos e principiológicos impostos pela LGPD, a verificação da legalidade e legitimidade de uma tecnopolítica de vigilância deve levar em conta uma análise de proporcionalidade entre os aspectos dessa vigilância e os direitos dos cidadãos que serão minimizados pelo exercício daquela.

3.3 A NECESSIDADE DE ANÁLISE DE PROPORCIONALIDADE ENTRE OS DIREITOS DO TITULAR E A FINALIDADE DA VIGILÂNCIA

O regime de proteção de dados pessoais, conforme delineado no tópico anterior, é, sobretudo, procedimental por não estabelecer proibições de tratamento de dados, mas tentar garantir a efetivação desse tratamento de forma adequada, estabelecendo aos agentes de tratamento de dados pessoais obrigações relativas ao procedimento. Um conceito importante

---

[355] BRASIL. Senado Federal. **Proposta de Emenda à Constituição (PEC) 17 de 2019**. Brasília, 03 de jun. de 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757. Acesso em: 15 nov. 2021.

[356] SENADO inclui proteção de dados pessoais como direito fundamental na Constituição. **Senado Federal notícias**, 20 out. 2021. Disponível em: https://www12.senado.leg.br/noticias/materias/2021/10/20/senado-inclui-protecao-de-dados-pessoais-como-direito-fundamental-na-constituicao. Acesso em: 21 out. 2021

[357] BRASIL. Congresso Nacional. Emenda Constitucional n 115. **Diário Oficial [da] União**, Brasília, 10 fev. 2022. Disponível em: https://www.in.gov.br/web/dou/-/emenda-constitucional-n-115-379516387. Acesso em: 29 mar. 2022.

para a disciplina, portanto, é o de "devido processo informacional", o qual tem por intuito "conferir ao indivíduo o direito de evitar exposições de seus dados sem possibilidades mínimas de controle, sobretudo em relação a práticas de tratamento de dados capazes de sujeitar o indivíduo a julgamentos preditivos e peremptórios".[358]

Especialmente nas relações entre Estado e indivíduo, em que há grande assimetria de poder, tendo em vista que o Estado possui força coercitiva e o poder de controlar o acesso dos cidadãos à bens e serviços básicos, tem-se que esse equilíbrio que se propõe alcançar por meio das salvaguardas procedimentais e dos princípios que norteiam a proteção de dados pessoais se faz ainda mais importante e necessário. O atendimento ao interesse público não pode servir para justificar todo e qualquer tratamento de dados pessoais dos cidadãos pelo Estado, pois a lógica do antagonismo entre interesse público e privacidade e proteção de dados é errônea, já que a privacidade e a proteção de dados, conforme já discutido, evoluíram em sua concepção, admitindo-se seu valor social, e não apenas individual, o que significa que não se trata de uma análise entre um interesse privado e o interesse público, que privilegiaria o segundo, mas sim entre dois interesses públicos.[359]

Desse modo, faz-se necessário a realização de um sopesamento efetivo entre dois interesses públicos, que deve ser realizada caso a caso, verificando a necessidade e a proporcionalidade desse tratamento, bem como o atendimento aos demais princípios de proteção de dados, para que não haja abusos. O interesse público e os demais princípios, portanto, devem ser lidos conjuntamente, sendo critérios que devem ser atendidos cumulativamente para que o tratamento de dados pelo poder público seja legítimo.[360]

Nesse mesmo sentido, a já citada sentença do Tribunal Constitucional Alemão aduz que, ainda que a relativização do direito à autodeterminação informacional seja possível, faz-se necessário observar o princípio da proporcionalidade:

> Além disso, o legislador deve observar em sua regulamentação o princípio da proporcionalidade. Este princípio, que é provido de dignidade constitucional, resulta da própria essência dos direitos fundamentais, que, como expressão da pretensão jurídica geral de liberdade do cidadão frente ao Estado, só podem ser limitados pelo

[358] BRASIL. Supremo Tribunal Federal. **ADI 6.387 MC / DF**. Plenário. Relator: Min. Rosa Weber. Data de julgamento: 07/05/2020. Voto do Min. Gilmar Mendes, p. 114.
[359] BRASIL. STF. **ADI 6.649/DF**, número único 0111621-15.2020, Conselho Federal da Ordem dos Advogados do Brasil – CFOAB (requerente), Presidente da República, 23 dez. 2020. Intervenção da Associação Data Privacy Brasil de Pesquisa na qualidade de Amicus Curie, petição 616/2021, 07 jan. 2021. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=6079238. Acesso em: 15 out. 2021.
[360] BRASIL. STF. **ADI 6.649/DF**, número único 0111621-15.2020, Conselho Federal da Ordem dos Advogados do Brasil – CFOAB (requerente), Presidente da República, 23 dez. 2020. Intervenção da Associação Data Privacy Brasil de Pesquisa na qualidade de Amicus Curie, petição 616/2021, 07 jan. 2021. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=6079238. Acesso em: 15 out. 2021. P. 27-28

> poder público quando isso for imprescindível para proteção de interesses públicos (BVerfGE 19, 342 [348]; jurisprudência consolidada). Em face dos já expostos riscos criados pelo uso do processamento eletrônico de dados, o legislador deve, mais do que antes, tomar precauções organizacionais e processuais que combatam o perigo de uma violação do direito da personalidade (cf. BVerfGE 53, 30 [65]; 63, 131 [143]).[361]

Há a necessidade, portanto, de realização de teste de proporcionalidade quando do tratamento de dados pessoais pelo poder público, ainda que para atendimento de interesse público. Gillian Black e Leslie Stevens formularam um modelo que pode ser utilizado para a averiguação acerca da proporcionalidade do tratamento em relação aos riscos que ele apresenta para os direitos dos titulares dos dados, condicionando a legitimidade do tratamento ao atendimento aos princípios da adequação, necessidade e proporcionalidade, os quais estão previstos em documentos internacionais relativos à proteção de dados pessoais, bem como na legislação brasileira (LGPD), conforme já observado.

De acordo com os autores, todo tratamento de dados pessoais requer que o agente de tratamento verifique a existência de um certo equilíbrio entre a necessidade do tratamento e os direitos dos indivíduos de não ter seus dados pessoais tratados excessivamente ou desnecessariamente. Para realizar a análise da legitimidade do tratamento, faz-se necessário, de início, verificar qual é a hipótese legal em que o tratamento de dados pessoais se enquadra, ou seja, por que o tratamento está sendo realizado? O que o legitimou?[362] No caso brasileiro, para responder essas perguntas, o tratamento deve se enquadrar em uma das hipóteses legais elencadas no art. 7º da LGPD:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> 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;

---

[361] MARTINS, Leonardo (org.). **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Tradução de Beatriz Hennig et al. Montevideo/Berlin: Konrad-Adenauer-Stiftung E. V., 2005. p. 235, 239.

[362] BLACK, Gillian; STEVENS, Leslie. Enhancing data protection and data processing in the public sector: the critical role of proportionality and the public interest. In: **Scripted**, v. 10, issue 1, p. 93-122, April 2013. p. 97

> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência
> 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.[363]

Dependendo de quem for o agente de tratamento de dados pessoais, se público ou privado, algumas hipóteses previstas nesse artigo serão mais relevantes que outras. Para o poder público tem-se que a legislação estabeleceu duas bases legais explicitamente direcionadas a ele: i) execução de políticas públicas (art. 7º, III); ii) execução de competências legais ou atribuições legais do serviço público (artigo 23). Apesar de não haver previsão explícita na lei quanto à possibilidade ou não de invocação de outras bases legais para legitimar o tratamento de dados pessoais pelo Estado, segundo Mirian Wimmer, o princípio da legalidade, que norteia as atividades públicas e impõe que essas atividades devam ter amparo legal, determina certa cautela na invocação das demais bases legais além daquelas especificamente direcionados ao poder público.[364] Além disso, algumas das hipóteses não se fazem apropriadas para legitimar o tratamento de dados pessoais pelo Estado, como é o caso do consentimento, uma vez que há assimetria de poder nas relações entre Estado e cidadão, bem como que esse último, frequentemente, depende do tratamento de dados realizado pelo poder público, para ter acesso à serviços públicos e benefícios sociais.[365] Nesse sentido, a parte introdutória da *General Data Protection Regulation* (GDPR), no § 43, trata sobre a questão, dispondo que:

> A fim de garantir que o consentimento seja dado livremente, o consentimento não deve fornecer uma base jurídica válida para o tratamento de dados pessoais em casos específicos em que haja um desequilíbrio claro entre o titular dos dados e o responsável pelo tratamento, em particular quando o responsável pelo tratamento é uma autoridade pública e, portanto, é improvável que o consentimento tenha sido dado livremente em todas as circunstâncias dessa situação específica. Presume-se que o consentimento não é dado livremente se não permitir que um consentimento separado seja dado para diferentes operações de processamento de dados pessoais, apesar de ser apropriado no caso individual, ou se a execução de um contrato, incluindo a

[363] BRASIL. Lei 13.709, de 14 de agosto de 2018. **Diário Oficial [da] União**, Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 nov. 2021.
[364] WIMMER, Miriam. Proteção de dados pessoais no Poder Público: incidência, bases legais e especificidades. In: **Revista do Advogado**: Lei Geral de Proteção de Dados Pessoais, n. 144, p. 126-133, nov. 2019. p. 131-132.
[365] BLACK, Gillian; STEVENS, Leslie. Enhancing data protection and data processing in the public sector: the critical role of proportionality and the public interest. In: **Scripted**, v. 10, issue 1, p. 93-122, April 2013. p. 98.

> prestação de um serviço, for dependente no consentimento, apesar de tal consentimento não ser necessário para tal desempenho. (tradução livre).[366] [367]

Desse modo, o tratamento de dados pessoais pelo poder público deve se basear em uma das outras hipóteses abarcadas pelo art. 7º, as quais, por sua vez, exigem que seja demonstrado que esse tratamento está realmente atendendo a finalidade a que se propôs, já que as demais hipóteses legais previstas no referido artigo são todas baseadas em uma necessidade. De acordo com os autores, primeiramente deve-se questionar se o agente que irá tratar os dados realmente possui um objetivo legítimo para o tratamento de dados pessoais, dentre esses elencados pela lei. Nessa linha de raciocínio, adotada pelos pesquisadores Black e Stevens, o conceito de necessidade é fundamental para determinar a legitimidade do tratamento de dados pessoais.[368] Nesse ponto, portanto, de acordo com o Ministro Gilmar Mendes em decisão monocrática sobre medida cautelar da ADPF 695/DF (Caso Denatran), avalia-se se o tratamento de dados está de acordo com o objetivo de execução de política pública ou para o exercício de uma obrigação legal do órgão público envolvido, por exemplo, as quais são as duas hipóteses de tratamento de dados pessoais expressamente direcionadas ao poder público.[369]

Ainda, segundo Black e Stevens, num segundo momento, a avaliação da necessidade do tratamento deve abarcar o equilíbrio entre os dados pessoais usados durante o tratamento e as finalidades que se pretende alcançar com o seu tratamento. Para os autores, deve ser levada em conta a questão referente à adequação desse tratamento com a finalidade buscada. O tratamento só será necessário, portanto, quando há adequação entre as finalidades legítimas do tratamento e os dados pessoais utilizados para alcançar essa finalidade. Nesse ponto, o que se avalia é: i) quais dados pessoais estão envolvidos nesse tratamento?; ii) existem dados pessoais sensíveis

---

[366] EUROPEAN UNION. **Regulation (EU) 2016/679 of the European Parliament and of the Council**, of 27 apr. 2016. Disponivel em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 15 nov. 2021.

[367] "*In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance*".

[368] BLACK, Gillian; STEVENS, Leslie. Enhancing data protection and data processing in the public sector: the critical role of proportionality and the public interest. In: **Scripted**, v. 10, issue 1, p. 93-122, April 2013. p. 99, 119.

[369] BRASIL. Supremo Tribunal Federal. **ADPF 695 MC/DF**. Decisão monocrática. Relator: Min. Gilmar Mendes. Data de julgamento: 24/06/2020. p. 40

sendo tratados?; iii) quais são os riscos envolvidos na coleta, tratamento e compartilhamento desses dados?; iv) e qual a possibilidade real de dano aos titulares dos dados?[370]

Por fim, deve-se identificar os interesses públicos envolvidos no tratamento de dados pessoais pelo Estado. Por não haver uma definição única e exata sobre o que é interesse público, essa avaliação deve ser feita caso a caso. Essa avaliação é especialmente importante nos casos de tratamento de dados pessoais pelo Estado, tendo em vista que esse tratamento realizado pelo poder público quase sempre terá uma finalidade que atende certo interesse público. Desse modo, o balanceamento entre o interesse público envolvido na finalidade do tratamento e os direitos à privacidade e à proteção de dados pessoais deve sempre ser realizado anteriormente ao início das atividades de tratamento, de modo a garantir que esse não seja excessivo, violando direitos fundamentais.[371]

Nesse ponto, deve-se ressaltar que a avaliação entre o interesse público envolvido na coleta e tratamento de dados pessoais e a proteção da privacidade e dos dados pessoais deve levar em conta que esse segundo interesse não é somente um direito individual, mas, como já mencionado, também possui valor coletivo. Portanto, o impasse se dá entre dois interesses coletivos. Isso porque, quando se leva em consideração que os direitos à privacidade e à proteção de dados pessoais são direitos fundamentais individuais, eles sempre serão superados e preteridos por uma série de interesses categorizados como interesse público, tendo em vista que o direito de um, comumente, é superado pelo direito de muitos.[372]

Quando o Estado for avaliar a legitimidade do tratamento de dados pessoais, deverá resolver o seguinte conflito: tratamento de dados pessoais para provisão de serviços públicos X proteção da privacidade e dos dados pessoais. Admitindo, portanto, que os direitos à privacidade e à proteção de dados possuem valor social, esse conflito se traduz para: proteção do interesse público X proteção do interesse público. Não havendo, assim, um modo claro e único de resolver o conflito. Black e Stevens propõe um modelo cooperativo para solução do problema, avaliando como o atendimento à cada interesse pode trazer benefícios para o outro. Desse modo, o uso de dados pessoais tem que ser justificado com base na necessidade e no

[370] BLACK, Gillian; STEVENS, Leslie. Enhancing data protection and data processing in the public sector: the critical role of proportionality and the public interest. In: **Scripted**, v. 10, issue 1, p. 93-122, April 2013. p. 119-120.
[371] BLACK, Gillian; STEVENS, Leslie. Enhancing data protection and data processing in the public sector: the critical role of proportionality and the public interest. In: **Scripted**, v. 10, issue 1, p. 93-122, April 2013. p. 112-114, 117.
[372] BLACK, Gillian; STEVENS, Leslie. Enhancing data protection and data processing in the public sector: the critical role of proportionality and the public interest. In: **Scripted**, v. 10, issue 1, p. 93-122, April 2013. p. 114-115.

atendimento ao interesse público do tratamento de dados, e essas justificativas serão, então, ponderadas em relação ao interesse público em proteger a privacidade e os dados pessoais.[373]

Assim, o terceiro passo dessa avaliação diz respeito à proporcionalidade do tratamento de dados pessoais quando se leva em conta os interesses públicos envolvidos. Nesse ponto, questiona-se: o interesse público em tratar dados pessoais supera o interesse individual em proteger a privacidade e o interesse público mais amplo em proteger os dados pessoais? Para responder a essa questão, os autores elencam uma série de considerações a serem feitas em relação aos dados pessoais envolvidos, tais como[374]:

a) O tratamento de dados pessoais é o meio menos intrusivo para atingir a finalidade buscada pelo órgão público?
b) O tratamento de dados pessoais está em conformidade com os outros princípios da proteção de dados pessoais?
c) O processamento requer apenas o uso de dados pessoais, e não dados pessoais sensíveis?
d) A anonimização dos dados pode ser utilizada? E, em caso afirmativo, a técnica proposta é considerada a mais eficaz?
e) O tratamento de dados foi aprovado por um órgão de supervisão competente?
f) Foi realizada uma avaliação de impacto na privacidade e proteção de dados para avaliar e mitigar os riscos inerentes ao tratamento em questão?
g) Existe um interesse público identificável no tratamento de dados pessoais?
h) Existe um interesse público identificável no fornecimento do serviço público em questão?

Para os autores, responder essas questões pode auxiliar os agentes de tratamento de dados pessoais a avaliarem se o tratamento que intentam realizar é um método proporcional para atingir um objetivo legítimo. Respostas positivas à essas questões são indicativas, geralmente, de um tratamento legítimo, já respostas negativas podem indicar que o atendimento ao interesse público em proteger os dados pessoais deve prevalecer. Assim, por meio dessa avaliação de 3 passos, pode-se determinar se o tratamento de dados pessoais dos cidadãos deve

[373] BLACK, Gillian; STEVENS, Leslie. Enhancing data protection and data processing in the public sector: the critical role of proportionality and the public interest. In: **Scripted**, v. 10, issue 1, p. 93-122, April 2013. p. 117-118.
[374] BLACK, Gillian; STEVENS, Leslie. Enhancing data protection and data processing in the public sector: the critical role of proportionality and the public interest. In: **Scripted**, v. 10, issue 1, p. 93-122, April 2013. p. 120.

ou não ser realizado, levando em conta todos os interesses envolvidos, bem como os riscos derivados do tratamento. Ainda, por meio do teste, os agentes de tratamento podem constituir uma relação maior de confiança com os cidadãos, os quais sentem que seus direitos estão sendo levados em conta e protegidos.

Por fim, os autores ainda citam benefício para o próprio setor público envolvido no tratamento e no aumento da cultura de proteção de dados, já que, em suas palavras:

> De maneira crítica, esse engajamento deve levar a uma cultura de proteção de dados mais robusta no setor público - uma cultura que, infelizmente, como foi demonstrado acima, é inexistente. Quando o setor público tem mais confiança em sua própria capacidade de tomar decisões legítimas em relação ao processamento de dados pessoais, os riscos associados às violações diminuirão. Consequentemente, a ação de fiscalização e as multas devem diminuir, juntamente com a perda de tempo da equipe investigando as violações, enquanto a tomada de decisões mais rápida e transparente deve aumentar, juntamente com uma maior uniformidade em todo o setor público. (tradução livre).[375] [376]

Uma avaliação tal como essa proposta por Gillian Black e Leslie Stevens, a qual passou pelo crivo do STF na decisão democrática sobre medida cautelar proferida pelo Ministro Gilmar Mendes, se faz necessária para determinar a necessidade, a adequação e a proporcionalidade de um tratamento de dados pessoais de cidadãos realizado pelo Estado, uma vez que o regime de proteção de dados pessoais não se trata de um obstáculo para o tratamento de dados pelo poder público, mas sim uma forma de nortear seus procedimentos para que ao passo que haja o aumento de eficiência dos órgãos públicos, os direitos fundamentais dos titulares dos dados estejam protegidos.

Complementarmente, faz-se necessário também uma análise contextual da aplicação da tecnopolítica de vigilância movido pelo tratamento de dados pessoais, para que se possa, inclusive, determinar os interesses públicos envolvidos, bem como os reais riscos derivados do tratamento aos titulares dos dados pessoais.

---

[375] BLACK, Gillian; STEVENS, Leslie. Enhancing data protection and data processing in the public sector: the critical role of proportionality and the public interest. In: Scripted, v. 10, issue 1, p. 93-122, April 2013. p. 122.

[376] "*Critically, this engagement should lead to a more robust data protection culture in the public sector – a culture which has been demonstrated above to be sadly lacking. Where the public sector has greater confidence in its own ability to take legitimate decisions regarding the processing of personal data, the risks associated with breaches will diminish. Consequently, enforcement action and fines should diminish, together with wasted staff time investigating the breaches, while faster, more transparent decision-making should increase, coupled with greater uniformity across the public sector*"

3.4 A NECESSIDADE DE ANÁLISE CONTEXTUAL DA APLICAÇÃO DA TECNOPOLÍTICA DE VIGILÂNCIA

Partindo dos conceitos teóricos delineados durante o primeiro capítulo, tem-se que a vigilância pode servir a diferentes propósitos, as vezes mais de um ao mesmo tempo, e que no Século XXI, frente ao desenvolvimento das técnicas utilizadas para o exercício da vigilância e das tecnologias que o auxiliam, bem como frente as mudanças no cenário social, politico, econômico e cultural, as questões sobre a vigilância tornam-se cada vez mais importantes, integrando não só o âmbito do poder e da política em larga escala, mas os próprios processos da vida cotidiana, tornando-se líquida e pervasiva. Variados sistemas e tecnologias com capacidade para vigilância se integram, atuando juntos, e, assim, a vigilância contemporânea é caracterizada por uma série de práticas e sistemas que atuam em conjunto, aumentando a sua capacidade e a sua intensidade, formando o que Haggerty e Ericson chamam de *surveillant assemblages*. Essa comunhão de tecnologias, práticas e sistemas de vigilância não só aumentam a capacidade, intensidade e a extensão do exercício da vigilância, mas na medida em que permeia toda a vida em sociedade, seus riscos também se intensificam e se distribuem.

Atualmente, toda vigilância requer uma avaliação cuidadosa, levando em conta os preceitos legais e doutrinários sobre a proteção de dados pessoais e da privacidade. Mas, para além disso, toda vigilância também requer a análise do contexto em que está sendo exercida e do conjunto de sistemas que a integra, já que os processos de vigilância são complexos e podem ser realizados por diferentes instituições, com propósitos diferentes e, consequentemente, com efeitos muito variados, alguns benignos ou neutros, outros extremamente prejudiciais à sociedade como um todo ou à um grupo social específico, reduzindo suas oportunidades, excluindo-os parcial ou totalmente da vida social e da vida política ou colocando-os em uma situação ruim de modo geral. [377]

Nesse sentido, denota-se a importância dos limites colocados pela doutrina da proteção à privacidade e aos dados pessoais ao exercício da vigilância. No entanto, ainda que a legislação esteja em voga, uma miríade de consequências negativas pode vir a acontecer aos indivíduos vigiados, titulares dos dados pessoais. Isso porque, o contexto em que o exercício da vigilância está sendo realizado afeta o seu resultado. Dependendo da finalidade da vigilância, de quem a exerce, sobre quem ela é exercida, qual é a relação de poder existente entre as partes, e do contexto social, econômico e político em geral, os efeitos criados pelo exercício dessa vigilância

[377] LYON, David. **Surveillance Studies**: An overview. Cambridge: Polity Press, 2007. p. 159-162.

variam drasticamente.[378] A coleta e o tratamento de dados pessoais de cidadãos, ainda que feita por meio das mesmas técnicas, realizada por um instituto como o Instituto Brasileiro de Geografia e Estatística (IBGE) e por um órgão como a Agência Brasileira de Inteligência (ABIN) apresentam conotações completamente diferentes, com consequências e riscos completamente diferentes, por exemplo. Da mesma forma que uma mesma tecnologia com capacidade para vigilância, como as câmeras com reconhecimento facial instaladas em locais públicos, podem significar coisas diversas para dois grupos sociais diferentes. Desse modo, contar com uma avaliação estanque do exercício da vigilância, que analise apenas o tipo de dado que está sendo coletado e tratado, ou apenas a técnica que está sendo utilizada para tratamento, pode levar a violações de direitos fundamentais. Ter consciência do contexto em que a vigilância será empregada é essencial.

Como bem destacou o Tribunal Constitucional Alemão ao julgar a Lei do Censo de 1983, bem como reafirmou o Ministro Luiz Fux em voto proferido na ADI 6.387/DF, não existem mais dados irrelevantes, tendo em vista que se faz necessário avaliar o contexto da utilização, para então constatar a importância dos dados. Nesse sentido:

> Neste mister não se pode apenas condicionar o tipo de dados [que podem ser levantados, transmitidos etc.]. Decisivos são sua utilidade e possibilidade de uso. Estas dependem, por um lado, da finalidade a que serve a estatística e, por outro lado, das possibilidades de ligação e processamento próprias da tecnologia de informação. Com isso, um dado em si insignificante pode adquirir um novo valor: desse modo, não existem mais dados "insignificantes" no contexto do processamento eletrônico de dados.379

Essa necessidade de uma análise contextual se coaduna com os preceitos principiológicos da doutrina do Direito à Proteção de Dados Pessoais, bem como com a análise de proporcionalidade trazidas nos tópicos anteriores, formando uma base de avaliação para os processos de vigilância.

Como aduz o referido Tribunal Alemão, atualmente, com o auxílio do processamento eletrônico, os dados de um banco de dados podem ser combinados com dados de outros, ampliando a utilidade que se retira desses dados e obtendo informações novas sobre os titulares dos dados, ampliando as possibilidades de consulta e influência sobre comportamentos dos indivíduos, sem que esses saibam com exatidão o uso que está sendo feito de seus dados e

---

[378] LYON, David. **Surveillance Studies**: An overview. Cambridge: Polity Press, 2007. p. 181-185.
[379] MARTINS, Leonardo (org.). **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Tradução de Beatriz Hennig et al. Montevideo/Berlin: Konrad-Adenauer-Stiftung E. V., 2005. p. 239.

possam ter controle sobre eles.[380] A coleta e o tratamento massivos de dados pessoais, mesmo aqueles que a priori são considerados irrelevantes, auxiliados pelos modernos mecanismos de tratamento automatizados, tornam possível a geração de perfis precisos sobre indivíduos, e podem aprofundar a assimetria informacional e de poder entre os que tem a capacidade de coleta e tratamento de dados, no caso os órgãos púbicos, e os titulares desses dados, os cidadãos, que sofrem com a assimetria de poder.[381]

Desse modo, deve-se questionar não só a natureza do dado, mas sim o risco do tratamento desse dado no contexto em que essa atividade será realizada, para qual finalidade ela será realizada, quem está envolvido nessa relação, e as expectativas do titular em relação a como e para quais finalidade seus dados serão utilizados. Essa avaliação é importante especialmente no contexto em que os dados pessoais estão sendo tratados pelo Estado, já que sua relação com os cidadãos já é profundamente marcada por assimetrias de poder e dependência. A coleta e o tratamento de dados pessoais dos cidadãos pelo Estado já trazem, por si só, sérios riscos de violação de direitos e liberdades fundamentais, uma vez que as informações obtidas por meio dessas atividades podem ser utilizadas para vigilância, controle e discriminação de grupos inteiros da sociedade. Há que se considerar que o tratamento de dados pessoais dos cidadãos pelo Estado comumente é feito para a tomada de decisão sobre questões relacionadas à prestação de serviços públicos e concessão de benefícios sociais e bens básicos, o que afeta diretamente a vida de muitos indivíduos da sociedade, os quais dependem desses serviços, bens e benefícios para viver com dignidade.[382] A avaliação contextual da coleta e tratamento de dados pessoais se faz de extrema importância, vez que analisar a legitimidade de um tratamento de dados sem considerar o contexto em que ele está inserido é ignorar que hoje, frente aos avançados algoritmos de tratamento de dados existentes, não se pode mais considerar que um dado não é relevante o suficiente para ser protegido.

A professora de ciência da informação Helen Nissenbaum, que é conhecida por seus estudos sobre privacidade e a criação do conceito de 'contextual integrity', - muito citado em um número de estudos sobre práticas de vigilância e os problemas de privacidade e proteção de

---

[380] MARTINS, Leonardo (org.). **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Tradução de Beatriz Hennig et al. Montevideo/Berlin: Konrad-Adenauer-Stiftung E. V., 2005. p. 237.

[381] BRASIL. STF. **ADI 6.649/DF**, número único 0111621-15.2020, Conselho Federal da Ordem dos Advogados do Brasil – CFOAB (requerente), Presidente da República, 23 dez. 2020. Intervenção da Associação Data Privacy Brasil de Pesquisa na qualidade de Amicus Curie, petição 616/2021, 07 jan. 2021. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=6079238. Acesso em: 15 out. 2021. P. 17

[382] BRASIL. STF. **ADI 6.649/DF**, número único 0111621-15.2020, Conselho Federal da Ordem dos Advogados do Brasil – CFOAB (requerente), Presidente da República, 23 dez. 2020. Intervenção da Associação Data Privacy Brasil de Pesquisa na qualidade de Amicus Curie, petição 616/2021, 07 jan. 2021. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=6079238. Acesso em: 15 out. 2021. p. 25

dados pessoais -, ressalta a importância do contexto em que o tratamento de dados pessoais é realizado, como, por exemplo, a posição social do titular do dado pessoal, seu gênero, idade, etnia, raça etc. Em uma era em que os dados pessoais fluem livremente e são usados para diversas finalidades, faz-se de extrema importância conhecer o contexto do titular dos dados e a finalidade de uso desses dados, analisando de que forma o tratamento desses dados pessoais pode afetar os direitos de seu titular. Para a professora, o contexto não pode ser ignorado, já que as pessoas revelam informações e compartilham dados em contextos específicos e esperam que seus dados sejam usados de forma apropriada para aquele contexto. Ignorar isso é permitir a violação de direitos do titular.[383]

A análise de Nissenbaum, portanto, reforça a importância do contexto para as práticas de vigilância. Sua abordagem da matéria diz respeito a garantir o fluxo apropriado dos dados pessoais e argumentar que os dados devem ser governados de acordo com sua integridade contextual, ou seja, respeitando o contexto em que foram compartilhados e as expectativas do seu titular para aquele determinado contexto.[384] Nesse sentido, a implementação de tecnopolíticas de vigilância realizadas por meio da coleta e tratamento de dados pessoais devem ter certa sensibilidade ao contexto de vida dos titulares desses dados, do contexto em que os dados foram coletados, bem como do contexto em que serão utilizados para atingir a finalidade do tratamento.[385]

A própria Lei Geral de Proteção de Dados Pessoais utiliza-se de uma abordagem voltada ao juízo sobre o grau de sensibilidade dos dados a serem tratados, o contexto da atividade de tratamento e as expectativas do titular em relação ao uso de seus dados pessoais. De acordo com a disciplina de proteção de dados da LGPD, a análise contextual do tratamento de dados pessoais envolve a delimitação de uma finalidade específica, a qual deve ser comunicada ao titular dos dados pessoais, e a análise da necessidade e da adequação dos dados coletados para atingir essa finalidade almejada.[386] Assim, a teoria cunhada pela professora Helen Nissenbaum é um marco teórico fundamental para determinar o escopo da proteção de dados pessoais nas

---

[383] LYON, David. **The culture of surveillance**: Watching as a way of life. Cambridge/Medford: Polity, 2018. p. 143, 188-189.
[384] STODDART, Eric. A surveillance of care: Evaluating surveillance ethically. In: BALL, Kirstie; HAGGERTY, Kevin D.; LYON, David (Ed.). **Routledge Handbook of Surveillance Studies**. London/New York: Routledge, 2012, pp. 369-376. p. 371-372.
[385] LYON, David. **The culture of surveillance**: Watching as a way of life. Cambridge/Medford: Polity, 2018. p. 188-189.
[386] BRASIL. Lei 13.709, de 14 de agosto de 2018. **Diário Oficial [da] União**, Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 out. 2021.

atividades de tratamento de dados, incluindo-se aí a implementação de tecnopolíticas de vigilância que se utiliza da coleta e tratamento de dados para atingir seus propósitos.

Segundo a teoria da professora, cada contexto específico em que um indivíduo se encontra possui suas próprias normas de distribuição de fluxo informacional (*norms of information flow*), as quais são normas que advém do contexto social, cultural, histórico, político e econômico, e devem ser observadas a partir das expectativas dos indivíduos sobre o fluxo de suas informações dentro de cada contexto. Essas normas se dividem, ainda, em normas de conveniência (*appropriateness*) e normas para distribuição de informação (*distribution of information*). As primeiras, como o próprio nome diz, servem para indicar quais informações é apropriado revelar sobre um indivíduo em determinado contexto. Geralmente, essa norma leva em conta o tipo ou a natureza das informações pessoais que, dentro de determinado contexto, sua revelação é permitida, esperada ou até exigida. Como exemplo, a autora cita que em uma consulta médica é não só apropriado, mas mandatório, que o paciente compartilhe com o médico informações sobre suas condições físicas, no entanto, geralmente não é adequado compartilhar com o médico detalhes sobre sua performance no trabalho. Tudo dependerá do contexto que se está analisando.[387]

As segundas, normas de distribuição de informação, referem-se à distribuição, transferência ou compartilhamento de informações de um indivíduo para um terceiro dentro de determinado contexto. Em uma amizade, por exemplo, o padrão é que informações compartilhadas em segredo não sejam repassadas à terceiros. Em uma relação entre médico e paciente, o médico deve respeitar as normas sobre confidencialidade de informações de saúde do paciente.[388] Ressalta-se que ambas as normas devem ser respeitadas para que a privacidade não seja violada, pois para Nissenbaum, a privacidade contextual é violada quando qualquer uma das normas é violada. O que importa é não só que a informação seja apropriada ou inapropriada para determinado contexto, mas também, que a distribuição dessa informação respeite as normas contextuais de distribuição de informação.[389]

A autora propõe, assim, que essas normas sejam sempre avaliadas em relação às novas práticas que as violam ou ameaçam, para que se possa definir se são dignas de preservação, em termos de quão bem elas conseguem promover os valores internos de cada contexto e valores

---

[387] NISSENBAUM, Helen. Privacy as contextual integrity. In: **Washington Law Review**, v. 79, n. 1, pp. 119-157, 2004. p. 137-139.
[388] NISSENBAUM, Helen. Privacy as contextual integrity. In: **Washington Law Review**, v. 79, n. 1, pp. 119-157, 2004. p. 140-143.
[389] NISSENBAUM, Helen. Privacy as contextual integrity. In: **Washington Law Review**, v. 79, n. 1, pp. 119-157, 2004. p. 138, 140-141

fundamentais sociais, políticos e morais, como: prevenção de ameaças relacionadas à proteção da informação; autonomia; liberdade; democracia etc.[390]

A mesma lógica se aplica aos órgãos públicos em relação aos dados dos cidadãos. Pode ser que seja apropriado, ou mesmo exigido, que o cidadão revele determinados dados ao Detran, por exemplo. No entanto, o compartilhamento desses dados pelo Detran para outro órgão público, como, por exemplo, a Abin, pode ser considerado uma violação de privacidade, já que não respeita as normas esperadas de distribuição da informação, pois os dados foram retirados de seu contexto inicial, sem a participação do titular, para serem usados para finalidades desconhecidas.

Nas palavras de Helen Nissenbaum:

> Uma das principais formas pelas quais a integridade contextual difere de outras abordagens teóricas da privacidade é que ela reconhece um conjunto mais rico e abrangente de parâmetros relevantes. Ao abordar se colocar registros públicos online é problemático, se mover registros de arquivos ou bancos de dados independentes para a rede marca uma mudança significativa, isso nos força a olhar além do fato de as informações em questão serem públicas. Para estabelecer se a integridade contextual é violada, é necessário um exame das normas vigentes de adequação e fluxo para ver se e de que forma as novas práticas propostas estão de acordo. (tradução livre).[391] [392]

Evidenciando a superação da dicotomia público versus privado na proteção da privacidade e dos dados pessoais, o que importa para essa análise é se a atividade de coleta, tratamento ou compartilhamento, violou a integridade contextual, e não somente a natureza da informação ou do dado. Desse modo, a coleta, o tratamento e o compartilhamento de dados pessoais devem ser feitos de modo apropriado ao contexto em que estão localizados, o que envolve: a delimitação da finalidade específica do tratamento; a adequação entre o tratamento e a finalidade; e o uso apenas dos dados necessários para alcançar a finalidade – princípios que regem a LGPD[393].

---

[390] NISSENBAUM, Helen. Privacy as contextual integrity. In: **Washington Law Review**, v. 79, n. 1, pp. 119-157, 2004. p 146.

[391] NISSENBAUM, Helen. Privacy as contextual integrity. In: **Washington Law Review**, v. 79, n. 1, pp. 119-157, 2004. p. 151.

[392] "*One of the key ways contextual integrity differs from other theoretical approaches to privacy is that it recognizes a richer, more comprehensive set of relevant parameters. In addressing whether placing public records online is problematic, whether moving records from filing cabinets or stand-alone databases onto the net marks a significant change, it forces us to look beyond whether the information in question is public. To establish whether contextual integrity is breached requires an examination of governing norms of appropriateness and flow to see whether and in what ways the proposed new practices measure up*".

[393] BRASIL. Lei 13.709, de 14 de agosto de 2018. **Diário Oficial [da] União**, Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 nov. 2021.

No mesmo sentido, o professor, pesquisador e consultor em gestão da informação e tecnologia da informação Roger Clarke, quem cunhou o termo "*dataveillance*"[394], já mencionado nos tópicos anteriores, propõe uma série de questionamentos que servem para a realização de uma análise mais completa da legitimidade e adequação das atividades de vigilância.[395] Com o intuito de aferir as dimensões das práticas de vigilância, Clarke elenca 07 (sete) perguntas, sendo elas[396]:

a) A quem é direcionada a vigilância?
b) Quem é o beneficiário dessa prática de vigilância?
c) Quem está exercendo a vigilância?
d) Por que se está vigiando?
e) Como é feita a vigilância?[397]
f) Onde é feita a vigilância?
g) Quando é/foi feita a vigilância?

Essas questões, que de início aparentam ser questões simples, permitem: i) avaliar mais facilmente o contexto de implementação da vigilância, identificando as normas propostas por Helen Nissenbaum; ii) determinar qual é a dimensão da assimetria de poder existente na relação entre os indivíduos envolvidos na atividade de vigilância; iii) verificar qual é a finalidade da vigilância, bem como a necessidade e a adequação dos dados tratados para atingir a finalidade almejada, na linha dos conceitos principiológicos da LGPD; iv) bem como, detectar os reais riscos advindos dessa atividade para os cidadãos por meio da identificação da forma de vigilância – de como é feita a vigilância.

Denota-se, assim, que para se fazer cumprir os preceitos principiológicos da doutrina de proteção de dados pessoais, o estudo do contexto de aplicação da tecnopolítica de vigilância se revela essencial, ainda que não haja uma estrutura determinada de como fazê-lo. Desse modo, todas essas considerações delineadas nesse capítulo devem ser levadas em conta quando da determinação da legitimidade de uma tecnopolítica de vigilância, que depende da coleta e

---

394 CLARKE, Roger. **Dataveillance**: 15 years on. March 2003. Disponível em: http://www.rogerclarke.com/DV/DVNZ03.html. Acesso em: 10 set. 2021.
395 CLARKE, Roger. A framework for surveillance analysis. 16 feb. 2012. Disponível em: http://www.rogerclarke.com/DV/FSA.html. Acesso em: 07 out. 2021
396 CLARKE, Roger. A framework for surveillance analysis. 16 feb. 2012. Disponível em: http://www.rogerclarke.com/DV/FSA.html. Acesso em: 07 out. 2021
397 Em relação a como é feita a vigilância, se faz necessário conhecer as formas de vigilância existentes na pós-modernidade, as quais foram abordadas no primeiro capítulo, interessando aqui, especialmente, a vigilância de dados (*dataveillance*), a vigilância corporal e a vigilância omnipresente e/ou omnisciente.

tratamento de dados pessoais dos cidadãos, implementada pelo Estado, superando a lógica de que todo e qualquer interesse público envolvido no exercício dessa vigilância, bem como sua necessidade, sempre prevalecerão sobre os direitos à privacidade e à proteção de dados pessoais.

Com base em toda a análise teórica desenvolvida nos últimos dois capítulos, realiza-se, no capítulo seguinte, uma análise do Cadastro Base do Cidadão (CBC) para demonstrar as complexidades de um sistema de vigilância implementado dentro de uma democracia, o qual por um lado tem por intuito facilitar a administração de políticas públicas e serviços públicos em benefício dos cidadãos, mas que, por outro, pode constituir-se como uma tecnopolítica de vigilância massiva que viola direitos fundamentais. Essa análise objetiva verificar como uma tecnopolítica de vigilância que é efetivamente implementada sem dar a devida atenção aos balizadores legais, doutrinários e principiológicos aqui delineados pode vir a ferir os direitos e liberdades fundamentais dos cidadãos e, consequentemente, os preceitos democráticos. Para isso, são analisados o decreto que cria o CBC, o contexto social e político em que ele é implementado, como ele pode ser caracterizado como um sistema de vigilância e quais os riscos que apresenta para os direitos e liberdades fundamentais derivados dos direitos à proteção de dados pessoais e à privacidade.

4 O CADASTRO BASE DO CIDADÃO COMO UM INSTRUMENTO DE TECNOPOLÍTICA DE VIGILÂNCIA

Em 2019, sem que houvesse consulta pública, o Governo Federal instituiu, por meio do Decreto 10.046/2019[398], o Cadastro Base do Cidadão (CBC), o qual tem por intuito a integração de diversas bases de dados dos cidadãos mantidas por órgãos públicos, seja da Administração Pública Federal ou dos demais poderes da União. A tentativa de integração de dados mantidos por entes públicos não é nova, uma vez que, já no governo Temer, foi publicado o Decreto 8.789/2016[399], o qual dispensava a necessidade de acordos e convênios entre instituições públicas para o compartilhamento de dados, com o intuito de melhorar seu processamento, bem como reduzir a inconsistência nas bases de dados públicas.[400]

O decreto publicado em 2019 pelo governo Bolsonaro revogou o decreto de Temer (nº 8.789/2016), ampliando o compartilhamento de dados dos cidadãos, que incluem dados sensíveis, como dados biométricos e características biológicas e comportamentais mensuráveis, retirando a necessidade de um órgão solicitar ao outro o acesso à sua base de dados, além de adicionar nova finalidade para o compartilhamento, qual seja: "aumento da qualidade e eficiência das operações internas da administração pública federal", finalidade essa que tem o potencial de legitimar uma variedade de usos dos dados por órgãos públicos federais, o que abre campo para excessos e abusos de direitos e liberdades fundamentais, especialmente quando se considera que o Decreto conta com terminologias e previsões que não estão de acordo com a Lei Geral de Proteção de Dados Pessoais (LGPD).[401]

A centralização de bases de dados remete à um projeto proposto durante o regime de Ditadura militar no Brasil, denominado Renape, o que incita preocupações em relação ao caráter autoritário com o qual essa base centralizada pode ser utilizada, formando um verdadeiro estado de vigilância e controle social e, consequentemente, violando direitos e liberdades que são pilares da democracia, especialmente quando órgãos como o Comando do Exército (CEX),

---

[398] BRASIL. Decreto nº 10.046, de 9 de outubro de 2019. **Diário Oficial [da] União**, Brasília, 09 out. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 15 set. 2021.

[399] BRASIL. Decreto nº 8.789, de 29 de junho de 2016. **Diário Oficial [da] União**, Brasília, 30 jun. 2016. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2016/Decreto/D8789.htm. Acesso em: 15 out. 2021.

[400] ANASTÁCIO, Kimberly; SANTOS, Bruna; VARON, Joana. **Cadastro Base do Cidadão**: a megabase de dados. Rio de Janeiro: Coding Rights, 2020. Disponível em: https://www.codingrights.org/docs/megabase.pdf. Acesso em: 24 set. 2021. p. 4-6.

[401] ANASTÁCIO, Kimberly; SANTOS, Bruna; VARON, Joana. **Cadastro Base do Cidadão**: a megabase de dados. Rio de Janeiro: Coding Rights, 2020. Disponível em: https://www.codingrights.org/docs/megabase.pdf. Acesso em: 24 set. 2021. p. 6.

a Agência Brasileira de Inteligência (Abin) e o Ministério de Justiça e Segurança Pública (MJSP) - que conta com a Secretaria de Operações Integradas (SEOPI), a qual ficou conhecida como Abin paralela -, já possuem acesso à essa base centralizada.[402]

A preocupação referente ao CBC se intensifica ao se considerar duas outras questões: (i) interesse crescente do setor privado em estabelecer acordos de compartilhamento de bases de dados do setor público; e (ii) contexto governamental em que o CBC é implementado, em que o atual poder executivo federal apresentou, em diversas ocasiões, grande interesse por atividades de vigilância da população, o que se torna ainda mais preocupante tendo em vista que o poder executivo federal age de forma contrária à pautas identitárias e de proteção à direitos da população minoritária e marginalizada.[403]

No intuito de demonstrar como o CBC é um grande exemplo de tecnopolítica de vigilância que habilita a ascensão de um tecnoautoritarismo no Brasil, bem como de analisar sua incompatibilidade com os preceitos legais e principiológicos necessários para estabelecer um equilíbrio no exercício da vigilância, sob pena de violação dos direitos à privacidade e à proteção de dados pessoais e dos demais direitos e liberdades fundamentais que deles derivam e que são protegidos pela Constituição Federal de 1988[404], pelas leis nº 12.965/2014[405] e nº 13.709/2018[406] (Marco Civil da Internet e Lei Geral de Proteção de Dados Pessoais respectivamente) e por outros tratados e convenções internacionais aderidos pelo Brasil, divide-se o presente capítulo em cinco partes. No primeiro subtópico analisa-se o Decreto 10.046/2019[407] que cria o Cadastro Base do Cidadão para explicar seu funcionamento. No segundo, analisa-se o contexto de implementação do CBC tendo em vista o interesse vigilantista do atual governo, citando exemplos de tecnopolíticas de vigilância já implementados, bem como tentativas de compartilhamento de dados entre entes públicos. No terceiro elucida-se

---

[402] ANASTÁCIO, Kimberly; SANTOS, Bruna; VARON, Joana. **Cadastro Base do Cidadão**: a megabase de dados. Rio de Janeiro: Coding Rights, 2020. Disponível em: https://www.codingrights.org/docs/megabase.pdf. Acesso em: 24 set. 2021. p. 11-12.

[403] ANASTÁCIO, Kimberly; SANTOS, Bruna; VARON, Joana. **Cadastro Base do Cidadão**: a megabase de dados. Rio de Janeiro: Coding Rights, 2020. Disponível em: https://www.codingrights.org/docs/megabase.pdf. Acesso em: 24 set. 2021. p. 4.

[404] BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial [da] União**, Brasília, 5 de out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 15 out. 2021

[405] BRASIL. Lei 12.965, de 23 de abril de 2014. **Diário Oficial [da] União**, Brasília, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 15 out. 2021.

[406] BRASIL. Lei 13.709, de 14 de agosto de 2018. **Diário Oficial [da] União**, Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 nov. 2021.

[407] BRASIL. Decreto nº 10.046, de 9 de outubro de 2019. **Diário Oficial [da] União**, Brasília, 09 out. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 15 set. 2021.

como e por que o CBC pode ser entendido como um sistema de vigilância com base na discussão teórica desenvolvida no primeiro capítulo. No quarto, é realizado uma análise da (in)adequação do Decreto e do Cadastro em relação à Lei Geral de Proteção de Dados Pessoais (LGPD), com base na discussão desenvolvida no capítulo anterior. E, por fim, no quinto e último subtópico elenca-se os riscos de violação aos direitos à proteção de dados pessoais e à privacidade, além das liberdades que deles derivam, advindos da implementação do CBC.

4.1 O DECRETO 10.046/2019 E O CADASTRO BASE DO CIDADÃO

O Decreto 10.046 de 9 de outubro de 2019 estabelece mecanismos de governança para o compartilhamento de dados entre órgãos e entidades da administração pública federal direta, autárquica e fundacional e os demais Poderes da União, define termos, estabelece classificações de dados, determina os níveis de compartilhamento e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. De acordo com o art. 1º. do referido decreto, as normas e diretrizes para o compartilhamento de dados entre órgãos públicos tem o intuito de simplificar a oferta de serviços públicos; gestar e otimizar a formulação, implementação, avaliação e monitoramento de políticas públicas; possibilitar a análise das condições de acesso e manutenção de benefícios sociais e fiscais; promover melhorias na qualidade e fidedignidade dos dados armazenados pela administração pública federal; e, aumentar a qualidade e a eficiência de operações internas da administração pública federal.[408]

O Cadastro Base do Cidadão é, portanto, uma base de dados consistente na agregação de diversas bases de dados de órgãos públicos, que cresce na medida em que novas bases vão sendo integradas, visando unificar e melhorar as informações sobre os cidadãos brasileiros dentro do governo. De acordo com o disposto no artigo 16 do decreto, o CBC tem a finalidade de aprimorar a gestão de políticas públicas; aumentar a confiabilidade dos cadastros de cidadãos já existentes na administração pública; viabilizar a criação de meio unificado de identificação do cidadão para a prestação de serviços públicos; disponibilizar uma interface unificada de atualização cadastral dos cidadãos, suportada por soluções tecnológicas interoperáveis das entidades e órgãos participantes do CBC; facilitar o compartilhamento de dados cadastrais dos

[408] BRASIL. Decreto nº 10.046, de 9 de outubro de 2019. **Diário Oficial [da] União**, Brasília, 09 out. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 15 set. 2021.

cidadãos entre órgãos da administração pública e realizar o cruzamento de informações dessas diversas bases de dados integradas a partir do número de inscrição no CPF.[409]

Segundo o artigo 17 do decreto, o CBC será composto pela base integradora e pelos componentes de interoperabilidade necessários ao intercâmbio de dados dessa com as bases temáticas, servindo como a base de dados referência para os órgãos e entidades do Poder Executivo federal. O decreto considera, de acordo com o art. 2º, como base integradora a "base de dados que integra os atributos biográficos e biométricos das bases temáticas", e como base temática a "base de dados de determinada política pública que contenha dados biográficos ou biométricos que possam compor a base integradora". Ainda de acordo com o art. 2º do decreto, consideram-se atributos biográficos os "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"; atributos biométricos as "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"; e dados cadastrais as "informações identificadoras perante os cadastros de órgãos públicos", como os atributos biográficos, o número de inscrição no CPF, o número de inscrição no CNPJ, o Número de Identificação Social (NIS), o número de inscrição no PIS, o número de inscrição no Pasep, o número do Título de Eleitor; a razão social, nome fantasia, data de constituição da pessoa jurídica, tipo societário, composição societária e a CNAE, bem como outros dados públicos relativos à pessoa jurídica ou à empresa individual.[410]

De início, a base integradora será disponibilizada com os dados biográficos constantes da base temática do CPF, sendo eles: o número de inscrição no CPF, situação cadastral, nome completo, nome social, data de nascimento, sexo, filiação, nacionalidade, naturalidade, indicador de óbito, data de óbito, data de inscrição ou última alteração do cadastro; sendo que o número de inscrição no CPF será utilizado como atributo chave para a realização da incorporação de outros dados biográficos, biométricos e cadastrais, provenientes de bases temáticas, na base integradora.[411] Desse modo, o Cadastro Base do Cidadão será uma base de

---

[409] BRASIL. Decreto nº 10.046, de 9 de outubro de 2019. **Diário Oficial [da] União**, Brasília, 09 out. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 15 set. 2021.

[410] BRASIL. Decreto nº 10.046, de 9 de outubro de 2019. **Diário Oficial [da] União**, Brasília, 09 out. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 15 set. 2021.

[411] BRASIL. Decreto nº 10.046, de 9 de outubro de 2019. **Diário Oficial [da] União**, Brasília, 09 out. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 15 set. 2021.

dados de referência, "íntegra e precisa" nos termos do decreto, composta a partir da integração de dados cadastrais, biográficos e biométricos oriundos de diversas bases de dados mantidas por entidades e órgãos públicos, sendo o número de CPF o fator que integra todos os outros dados e que permite a fácil localização de diversos dados sobre um cidadão específico.

O órgão responsável por viabilizar o CBC, orientar os órgãos responsáveis pelas bases temáticas e arcar com os custos de criação e atualização do CBC é a Secretaria de Governo Digital, vinculada à Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia, sendo que a responsabilidade pelos custos de manutenção e atualização das bases temáticas é das próprias entidades e órgãos públicos responsáveis por elas. Ainda, a gestão do CBC está vinculada ao Comitê Central de Governança de Dados, criado pelo mesmo decreto, composto exclusivamente por membros do governo e ao qual compete a criação de diretrizes e orientação sobre o compartilhamento de dados, a resolução de controvérsias, a avaliação de políticas de segurança da informação sobre o compartilhamento e integração de dados entre os entes públicos, bem como a definição de outros cadastros bases de referência, como o Cadastro Base de Endereço, instituído pela Resolução nº 5/2021 do Comitê[412].[413]

O decreto estabelece, ainda, 03 (três) níveis de compartilhamento que orientam o compartilhamento dos dados entre os órgãos públicos, sendo eles: (i) compartilhamento amplo, compartilhamento restrito e (iii) compartilhamento específico. De acordo com o decreto, o compartilhamento amplo será feito "quando se tratar de dados públicos que não estão sujeitos a nenhuma restrição de acesso, cuja divulgação deve ser pública e garantida a qualquer interessado, na forma da legislação", o compartilhamento restrito "quando se tratar de dados protegidos por sigilo, nos termos da legislação, com concessão de acesso a todos os órgãos e entidades de que trata o art. 1º para a execução de políticas públicas, cujo mecanismo de compartilhamento e regras sejam simplificados e estabelecidos pelo Comitê Central de Governança de Dados" e o compartilhamento específico "quando se tratar de dados protegidos por sigilo, nos termos da legislação, com concessão de acesso a órgãos e entidades específicos,

---

[412] COMITÊ CENTRAL DE GOVERNANÇA DE DADOS. Ministério da Economia. Resolução CCGD/ME nº 5, de 12 de janeiro de 2021. **Diário Oficial [da] União**, Brasília, 15 jan. 2021. Disponível em: https://in.gov.br/web/dou/-/resolucao-ccgd/me-n-5-de-12-de-janeiro-de-2021-299084556. Acesso em: 15 out. 2021.

[413] BRASIL. Decreto nº 10.046, de 9 de outubro de 2019. **Diário Oficial [da] União**, Brasília, 09 out. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 15 set. 2021.

nas hipóteses e para os fins previstos em lei [...]".[414] A categorização dos níveis de compartilhamento deve ser feita pelo gestor de dados, observando o disposto na legislação, dentro de prazo a ser definido pelo Comitê Central de Governança de Dados, o qual também fica responsável por emitir diretrizes para o compartilhamento de dados.[415]

De acordo com relatório sobre o Cadastro Base do Cidadão, elaborado pelo *Coding Rights*, a pandemia do Covid-19 atrasou o processo de implementação do CBC e de categorização dos dados pelos órgãos e entidades públicas. Segundo informações fornecidas ao *Coding Rights* via Lei de Acesso à Informação[416], após 10 meses da publicação do decreto, apenas a Receita Federal do Brasil fazia parte do cadastro de forma plena e, desse modo, os únicos dados presentes no cadastro seriam os da base cadastral do CPF, conforme já previsto no próprio decreto. No entanto, outros quatro órgãos estavam em processo de adesão, sendo eles: a Agência Brasileira de Inteligência (Abin); a Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES); o Ministério da Agricultura, Pecuária e Abastecimento (MAPA); e a Agência Nacional de Saúde Suplementar (ANS). Ainda, até a data de fornecimento dessas informações, 27 órgãos já haviam solicitado acesso aos dados do CBC[417], sendo eles:

i) Abin;
ii) ANS;
iii) CAPES;
iv) MAPA;
v) Agência Espacial Brasileira (AEB);
vi) Advocacia-Geral da União (AGU);
vii) Agência Nacional de Cinema (ANCINE);
viii) Agência Nacional de Transportes Aquaviários (ANTAQ);
ix) Agência Nacional de Vigilância Sanitária (ANVISA);

---

[414] BRASIL. Decreto nº 10.046, de 9 de outubro de 2019. **Diário Oficial [da] União**, Brasília, 09 out. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 15 set. 2021.

[415] ANASTÁCIO, Kimberly; SANTOS, Bruna; VARON, Joana. **Cadastro Base do Cidadão**: a megabase de dados. Rio de Janeiro: Coding Rights, 2020. Disponível em: https://www.codingrights.org/docs/megabase.pdf. Acesso em: 24 set. 2021. p. 7.

[416] BRASIL. Lei nº 12.527, de 18 de novembro de 2011. **Diário Oficial [da] União**, Brasília, 18 nov. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 15 out. 2021.

[417] ANASTÁCIO, Kimberly; SANTOS, Bruna; VARON, Joana. **Cadastro Base do Cidadão**: a megabase de dados. Rio de Janeiro: Coding Rights, 2020. Disponível em: https://www.codingrights.org/docs/megabase.pdf. Acesso em: 24 set. 2021. p. 11-12.

x) Comando do Exército (CEX);
xi) Controladoria-Geral da União (CGU);
xii) DATASUS;
xiii) FIOCRUZ;
xiv) Fundo Nacional de Desenvolvimento da Educação (FNDE);
xv) Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis (IBAMA);
xvi) Instituto Nacional de Colonização e Reforma Agrária (INCRA);
xvii) Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP);
xviii) Instituto Nacional da Propriedade Industrial (INPI);
xix) Ministério da Cidadania (MC);
xx) Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC);
xxi) Ministério da Economia (ME);
xxii) Ministério da Infraestrutura (MINFRA);
xxiii) Ministério da Justiça e Segurança Pública (MJSP);
xxiv) Ministério da Mulher, da Família e dos Direitos Humanos (MMFDH);
xxv) Superintendência Nacional de Previdência Complementar (PREVIC);
xxvi) Secretaria de Governo Digital do Ministério da Economia (SGD/ME);
xxvii) Superintendência de Seguros Privados (SUSEP).

Ressalta-se que foram solicitados, por meio da Lei de Acesso à Informação, atualizações em relação ao estágio de implementação do cadastro, especialmente em relação à quais órgãos já solicitaram acesso à base integradora. De acordo com resposta recebida em 18 de outubro de 2021, além daqueles já citados, os seguintes órgãos já solicitaram acesso ao cadastro:

i) Agência Nacional de Energia Elétrica (ANEEL);
ii) Agência Nacional de Mineração (ANM);
iii) Agência Nacional de Transportes Terrestres (ANTT);
iv) Conselho Administrativo de Defesa Econômica (CADE);
v) Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPQ);
vi) Departamento Nacional de Infraestrutura de Transportes (DNIT);
vii) Escola Nacional de Administração Pública (ENAP);
viii) Instituto Brasileiro de Geografia e Estatística (IBGE);
ix) Instituto Chico Mendes de Conservação da Biodiversidade (ICMBio);

x) Instituto Federal de Educação, Ciência e Tecnologia do Amazonas (IFAM);
xi) Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte (IFRN);
xii) Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO);
xiii) Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul (IFRS);
xiv) Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina (IFSC);
xv) Instituto Federal de Educação, Ciência e Tecnologia de São Paulo (IFSP);
xvi) Instituto Federal de Educação, Ciência e Tecnologia Sul Rio-Grandense (IFSul);
xvii) Instituto Federal de Educação, Ciência e Tecnologia Goiano (IFG);
xviii) Instituto Nacional de Metrologia, Qualidade e Tecnologia (INMETRO);
xix) Instituto Nacional de Tecnologia da Informação (ITI);
xx) Ministério da Defesa (MD);
xxi) Ministério do Desenvolvimento Regional (MDR);
xxii) Secretaria de Gestão do Ministério da Economia (ME/SEGES);
xxiii) Ministério da Educação (MEC);
xxiv) Ministério da Infraestrutura (MINFRA);
xxv) Ministério da Saúde (MS);
xxvi) Ministério do Turismo (MTUR);
xxvii) Procuradoria-Geral da Fazenda Nacional (PGFN);
xxviii) Superintendência Nacional de Previdência Complementar (PREVIC);
xxix) Polícia Rodoviária Federal (PRF);
xxx) Departamento de Operações Compartilhadas da Secretaria do Governo Digital (SGD/DEOPC);
xxxi) Departamento de Serviços Públicos Digitais da Secretaria do Governo Digital (SGD/DESPD);
xxxii) Secretaria do Tesouro Nacional (STN);
xxxiii) Superintendência do Desenvolvimento da Amazônia (SUDAM);
xxxiv) Superintendência da Zona Franca de Manaus (SUFRAMA);
xxxv) Universidade Federal de Lavras (UFLA);
xxxvi) Universidade Federal do Paraná (UFPR);
xxxvii) Universidade Federal de Santa Catarina (UFSC);
xxxviii) Universidade Federal de Uberlândia (UFU).

Por fim, ressalta-se que o Decreto 10.046/2019 é objeto de Arguição de Descumprimento de Preceito Fundamental (ADPF 695/DF)[418] proposta pelo Partido Socialista Brasileiro (PSB) e de Ação Direta de Inconstitucionalidade (ADI 6.649/DF)[419] proposta pelo Conselho Federal da Ordem dos Advogados do Brasil (CFOAB), sob argumento de violação direta dos artigos 1º, caput, inciso III e 5º, caput, incisos X, XII e LXXII da Constituição Federal[420], que asseguram, respectivamente, a dignidade da pessoa humana; a inviolabilidade da intimidade, da privacidade e da vida privada, da honra e da imagem das pessoas; o sigilo dos dados; a garantia do *habeas data*, a proteção de dados pessoais e a autodeterminação informativa. O Conselho Federal da OAB, na ADI 6.649/DF alega que o referido Decreto, sob o argumento de facilitar o acesso dos brasileiros aos serviços públicos federais, erige uma ferramenta de vigilância estatal extremamente poderosa, que inclui dados pessoais, familiares, laborais, dados biométricos e "características biológicas e comportamentais mensuráveis da pessoa natural". Ainda, além da inconstitucionalidade material com fundamento nos artigos citados, o decreto ostenta inconstitucionalidade formal por invadir matérias de competência privativa de lei, exorbitando os poderes normativos concedidos por Lei Fundamental ao Presidente da República. Por fim, o Decreto 10.046/2019 contraria a ordem constitucional por ser contrário à decisão do Plenário do STF que reconheceu a autonomia do direito fundamental à proteção de dados pessoais (ADI 6.387/DF)[421].

Diante dos aspectos apresentados, tem-se que a forma como o Cadastro Base do Cidadão irá operar, bem como suas finalidades, são próprias de um sistema de vigilância estatal visando a melhoria da administração pública. Antes, porém, de analisar CBC em face das proposições teóricas de vigilância apresentadas no primeiro capítulo, faz-se necessário salientar o contexto vigilantista em que o CBC está sendo implementado, isto é, sendo um sistema que facilita o compartilhamento de dados pessoais entre órgãos públicos, o CBC pode vir a instrumentalizar outros sistemas de vigilância estatal já implementados e reforçar o caráter vigilantista que o

---

[418] BRASIL. STF. **ADPF 695/DF**, número único 0095712-30.2020, Partido Socialista Brasileiro -PSB (requerente), União, 16 jun. 2020. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5938693. Acesso em: 15 out. 2021

[419] BRASIL. STF. **ADI 6.649/DF**, número único 0111621-15.2020, Conselho Federal da Ordem dos Advogados do Brasil – CFOAB (requerente), Presidente da República, 23 dez. 2020. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=6079238. Acesso em: 15 out. 2021.

[420] BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial [da] União**, Brasília, 5 de out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 15 out. 2021

[421] BRASIL. STF. **ADI 6.387/DF**, número único 0090566-08.2020, Conselho Federal da Ordem dos Advogados do Brasil – CFOAB (requerente), Presidente da República, 20 abr. 2020. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165. Acesso em: 15 out. 2021.

Estado brasileiro já vem apresentando, seja fornecendo dados do cadastro para órgãos que possuem outros sistemas de vigilância em uso, seja integrando dados advindos de sistemas de vigilância no Cadastro Base do Cidadão. Desse modo, faz-se necessário, para os objetivos dessa pesquisa, delinear algumas outras tecnopolíticas de vigilância em exercício atualmente no Brasil.

4.2 CONTEXTO DE IMPLEMENTAÇÃO DO CBC

A publicação do Decreto 10.046/2019 – e, portanto, a criação do Cadastro Base do Cidadão, considerado aqui um sistema de vigilância - foi realizado sem que houvesse consulta pública prévia e, aparentemente, sem a realização de relatório de impacto à proteção de dados pessoais, em um contexto em que a vigilância massiva e distribuída da população se faz de grande interesse dos poderes públicos federais e estaduais, os quais vêm investindo em tecnologias com capacidade para a vigilância sob justificativa de aumento da eficácia de segurança pública, melhoria na prestação de serviços públicos e aperfeiçoamento da criação e gestão de políticas públicas. Um dos principais investimentos dos estados e municípios brasileiros em tecnologias para aumento da segurança pública é destinado a tecnologias de videomonitoramento, abrangendo tanto a expansão da infraestrutura de câmeras urbanas (câmeras de circuito fechado de televisão ou CFTV), quanto a compra de softwares de Inteligência Artificial de identificação e reconhecimento facial e de placa.[422]

Entre as tecnologias de vídeo-monitoramento mais utilizadas, portanto, estão as câmaras de circuito fechado, as câmeras com tecnologia de reconhecimento facial e as câmeras com tecnologia de reconhecimento de placas. Dentre essas a tecnologia que causa mais controvérsia e preocupação é a de reconhecimento facial, utilizada, atualmente, não só para fins de segurança pública, mas também para finalidades como detecção de fraudes no acesso a serviços públicos e gestão de frequência escolar em instituições públicas. As câmeras de reconhecimento facial vêm sendo implementadas no Brasil desde pelo menos 2011, conforme relatório elaborado pelo Instituto Igarapé[423], chegando a 20 estados brasileiros em 2021. Esse tipo de tecnologia vem causando grande preocupação a respeito dos impactos negativos vinculados à violação de direitos e garantias constitucionais, principalmente de jovens e negros das periferias brasileiras.

---

[422] FRANCISCO, Pedro Augusto P.; HUREL, Louise Marie; LOBATO, Luisa Cruz. Videomonitoramento: web report. Instituto Igarapé, 2019. Disponível em: https://igarape.org.br/videomonitoramento-webreport/#intro. Acesso em: 12 out. 2021.

[423] INSTITUTO IGARAPÉ. Reconhecimento facial no Brasil: infográfico. Instituto Igarapé, 2019. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Acesso em: 09 out. 2021.

Entre os principais problemas das câmeras com tecnologia de reconhecimento facial identificados pelo Instituo Igarapé estão:

a) limitações técnicas, tendo em vista que as condições do ambiente e da instalação, bem como imagens de baixa resolução, mudanças na posição do rosto e expressões faciais, afetam o funcionamento da tecnologia e suas taxas de acerto; essa tecnologia é mais propensa a erro quando comparada com sistemas de reconhecimento de íris ou impressões digitais;
b) dificuldades na implementação e operação da tecnologia, tendo em vista a escassez de pessoal capacitado para operação do sistema e a necessidade de manutenção dos equipamentos a curto e longo prazo;
c) enviesamento dos resultados obtidos pela tecnologia por motivos de enviesamento histórico dos dados utilizados, utilização de dados desatualizados ou utilização de bancos de dados que não contém diversidade étnica e racial.[424]

Em relação ao problema referente aos resultados discriminatórios obtidos por essa tecnologia, observou-se que 90,5% dos presos por monitoramento facial no Brasil até 2019 eram negros. Nesse sentido, deve-se levar em conta que há riscos às populações já marginalizadas tanto em casos de erros de reconhecimento facial do sistema, como falsos positivos, causando constrangimentos e prisões arbitrárias, quanto em casos em que o sistema é extremamente eficaz e não apresenta erros no reconhecimento facial, tendo em vista que os dados utilizados, especialmente quando advindos de bancos de dados policiais, são historicamente enviesados pelo racismo estrutural, o que se torna ainda mais perigoso em países marcados pelo racismo e a desigualdade, como o é o Brasil.[425] Frente à essas questões, muitas cidades ao redor do mundo optaram por banir o uso de tecnologia de reconhecimento facial por autoridades públicas. Nos Estados Unidos da América, cidades como São Francisco, Oakland, Somerville, Berkeley, Cambridge e Boston baniram o uso de reconhecimento facial por autoridades públicas e na França e na Suécia foi proibida a sua utilização em escolas.[426] No entanto, o Brasil, indo na contramão, continua a investir nesse tipo de tecnologia, tanto para a

[424] FRANCISCO, Pedro Augusto P.; HUREL, Louise Marie; LOBATO, Luisa Cruz. Videomonitoramento: web report. Instituto Igarapé, 2019. Disponível em: https://igarape.org.br/videomonitoramento-webreport/#intro. Acesso em: 12 out. 2021.
[425] CROCKFORD, Kade. How is face recognition surveillance technology racist? ACLU, 16 jun. 2020. Disponível em: https://www.aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist/. Acesso em 14 out. 2021.
[426] FERNANDES, Elora Raad; TEFFÉ, Chiara Spadaccini. Reconhecimento facial: laissez-faire, regular ou banir? Migalhas, 16 jul. 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-vulnerabilidade/330766/reconhecimento-facial--laissez-faire--regular-ou-banir. Acesso em: 14 out. 2021.

finalidade de segurança pública, tendo o governo federal regulamentado o uso de dinheiro do Fundo Nacional de Segurança Pública para "fomento à implantação de sistemas de vídeo-monitoramento com soluções de reconhecimento facial (...)"[427], quanto para facilitação do processo de check-in e embarque em aeroportos brasileiros, projeto encabeçado pelo Ministério da Infraestrutura em parceria com a Serpro.[428]

Relacionado ao uso de câmeras de reconhecimento de placas de veículos, um sistema que causa preocupação em relação à violação de direitos é o Córtex, uma tecnologia implementada pela Secretaria de Operações Integradas (Seopi)[429], setor da Secretaria Nacional de Segurança Pública do Ministério da Justiça e Segurança Pública, consistente em uma inteligência artificial que utiliza o reconhecimento de placas de veículos por milhares de câmeras instaladas em todo o Brasil para realizar o rastreamento de alvos móveis em tempo real. Por meio do Córtex, os agentes possuem acesso à diversos bancos de dados sobre cidadãos e empresas, como a Relação Anual de Informações Sociais (Rais) do Ministério da Economia, o bando de dados do Departamento Nacional de Trânsito (Denatran), o Sistema Nacional de Informações de Segurança Pública (Sinesp), o cadastro nacional de CPFs, o cadastro nacional de foragidos, o banco de dados de boletins de ocorrência, o banco nacional de perfis genéticos, o banco de dados do Alerta Brasil da Polícia Rodoviária Federal e do Sistema Integrado Nacional de Identificação de Veículos em Movimento (Sinivem). Assim, tais agentes conseguem saber toda a movimentação de um indivíduo pela cidade, bem como quem o acompanhou, tudo a partir da placa do carro, além de conseguir cruzar esse histórico de movimentação com dados pessoais relativos à emprego, salário, ficha criminal etc.[430]

Ressalta-se que, conforme informações fornecidas por fontes anônimas ao *The Intercept* Brasil, cerca de dez mil pessoas das forças de segurança e setores de inteligência dos governos federal, estaduais e municipais possuem acesso ao Córtex. Essa tecnologia destina-se à melhora

---

[427] BRASIL. Ministério da Justiça e Segurança Pública. Portaria nº 793, de 24 de outubro de 2019. **Diário Oficial [da] União**, Brasília, 25 out. 2019. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-793-de-24-de-outubro-de-2019-223853575. Acesso em: 14 out. 2021.

[428] ANASTÁCIO, Kimberly; SANTOS, Bruna; VARON, Joana. **Cadastro Base do Cidadão**: a megabase de dados. Rio de Janeiro: Coding Rights, 2020. Disponível em: https://www.codingrights.org/docs/megabase.pdf. Acesso em: 24 set. 2021. p. 26.

[429] De acordo com o Decreto nº 9.662/2019, compete à Seopi realizar serviços de inteligência para combate ao crime organizado, atuando de maneira análoga aos demais órgãos de inteligência brasileiros como a Agência Brasileira de Inteligência (Abin), o Gabinete de Segurança Institucional (GSI) e o Centro de Inteligência do Exército (CIE). (BRASIL. Decreto nº 9.662, de 1º de janeiro de 2019. Diário Oficial [da] União, Brasília, 01 jan. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9662.htm. Acesso em: 14 out. 2021).

[430] REBELLO, Aiuri. Da placa do carro ao CPF: conheça o Córtex, sistema de vigilância do governo que integra de placa de carro a dados de emprego. The Intercept Brasil, 21 set. 2020. Disponível em: https://theintercept.com/2020/09/21/governo-vigilancia-cortex/. Acesso em: 14 out. 2021.

da segurança pública e combate ao crime, no entanto, a falta de transparência em relação a quem tem acesso ao sistema, quem fiscaliza seu uso, quais são os dispositivos de controle utilizados e quais normativas legais o regulam, transformaram o Córtex em um sistema com grande potencial de vigilância de cidadãos, organizações da sociedade civil, movimentos sociais, lideranças políticas e manifestantes, em uma escala sem precedentes, e com pouco ou nenhum controle, tornando-se, assim, mais um exemplo de tecnopolítica de vigilância que apresenta riscos aos direitos e liberdades dos cidadãos brasileiros.

Outro exemplo do notável interesse vigilantista do Estado brasileiro é a destinação de R$ 96 milhões, aprovado pelo conselho gestor do Fundo Nacional de Segurança Pública em 2020, para um projeto da Polícia Federal que pretende reunir em um único banco de dados informações criminais de todo o país.[431] O projeto conta com a implementação do sistema ABIS (Solução Automatizada de Identificação Biométrica), que possibilita a identificação de pessoas com a coleta, o armazenamento e o cruzamento de dados biométricos. Ainda, segundo o próprio site do Ministério da Justiça e Segurança Pública, o sistema está projetado para armazenar inicialmente dados de 50,2 milhões de pessoas, mas é prevista a possibilidade de expansões posteriores que poderão conter dados de até 200 milhões de indivíduos, quase o total da população brasileira[432], que em 2021 chegou a 213,3 milhões segundo estimativa do IBGE.[433]

Além disso, importa destacar algumas ações realizadas pelo atual governo federal ao longo do ano de 2020, as quais denotam o grande interesse no exercício de vigilância estatal sobre os cidadãos, por vezes com finalidades políticas, a despeito dos riscos que essa vigilância possa apresentar para direitos e liberdades fundamentais, revelando um caráter tecnoautoritário[434] por parte do atual governo[435]. Em 17 de abril de 2020 foi editada a Medida Provisória 954 que determinava o compartilhamento de dados (como nomes, números de telefone e endereços dos consumidores) por empresas de telecomunicações com o IBGE para

---

[431] ANASTÁCIO, Kimberly; SANTOS, Bruna; VARON, Joana. **Cadastro Base do Cidadão**: a megabase de dados. Rio de Janeiro: Coding Rights, 2020. Disponível em: https://www.codingrights.org/docs/megabase.pdf. Acesso em: 24 set. 2021. p. 26.

[432] POLÍCIA Federal implementa nova Solução Automatizada de Identificação Biométrica. **Gov.br**, 06 jul. 2021. Disponível em: https://www.gov.br/pf/pt-br/assuntos/noticias/2021/07/policia-federal-implementa-nova-solucao-automatizada-de-identificacao-biometrica. Acesso em: 14 out. 2021.

[433] IBGE. Estimativas da população – 2021. **IBGE**, 01 jul. 2021. Disponível em: https://www.ibge.gov.br/estatisticas/sociais/populacao/9103-estimativas-de-populacao.html?=&t=resultados. Acesso em: 14 out. 2021.

[434] O tecnoautoritarismo refere-se aos "processos de expansão do poder estatal, por meio do uso de tecnologias de comunicação da informação de ponta, com o objetivo de incrementar as capacidades de vigilância e controle sobre a população, mediante violação de direitos individuais ou ampliação importante dos riscos de violação a direitos fundamentais". (DATA PRIVACY BRASIL; LAUT. Retrospectiva tecnoautoritarismo - 2020. **LAUT**, 26 jan. 2021. Disponível em: https://laut.org.br/retrospectiva-tecnoautoritarismo-2020/. Acesso em: 15 out. 2021).

[435] DATA PRIVACY BRASIL; LAUT. Retrospectiva tecnoautoritarismo - 2020. **LAUT**, 26 jan. 2021. Disponível em: https://laut.org.br/retrospectiva-tecnoautoritarismo-2020/. Acesso em: 15 out. 2021

fins de produção da Pesquisa Nacional por Amostra de Domicílios Contínua no período da pandemia.[436] A medida provisória foi suspensa pelo STF e posteriormente teve sua vigência encerrada em 14 de agosto de 2020 por ferir a privacidade dos cidadãos e não ser clara quanto as finalidades do compartilhamento de dados.[437][438]

Em 06 de junho de 2020, o site *The Intercept* teve acesso à documentos que revelaram que a Agência Brasileira de Inteligência (Abin), vinculada ao governo federal, fez convênio – baseado no Decreto 10.046/2019, objeto do presente estudo - com o Serviço Federal de Processamento de Dados para obter o compartilhamento de dados pessoais de todos os indivíduos que possuem Carteira Nacional de Habilitação (CNH), permitindo à Abin acessar dados como nome, filiação, CPF, endereço, telefone, foto e dados dos veículos de mais de 76 milhões de pessoas.[439] O PSB entrou com ação no STF para suspensão do referido acordo por violar direitos e liberdades constitucionais, visto que os dados seriam compartilhados sem a concordância dos titulares, sem atender aos requisitos de transparência da LGPD, e sem prever o compartilhamento de dados para fins de inteligência ou segurança pública, sendo a finalidade exata do uso dos dados desconhecida.[440] Desse modo, em 24 de junho de 2020, o governo revogou a autorização da Abin para obtenção dos dados solicitados.[441]

Ainda em junho de 2020 o Ministério da Justiça e Segurança Pública, por meio da Secretaria de Operações Integradas (Seopi) – conhecida como Abin paralela -, abriu ação sigilosa para criação de dossiê sobre 579 pessoas identificadas como fascistas – dentre elas professores e policiais -, o qual continha fotografias e endereços de redes sociais em alguns casos, tendo sido baseado em manifesto antifascista assinado por servidores de segurança pública em maio. [442] Em 20 de agosto de 2020, o Supremo Tribunal Federal, em julgamento da

---

[436] BRASIL. Medida Provisória n 954, de 17 de abril de 2020. **Diário Oficial [da] União**, 17 abr. 2020. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm. Acesso em: 15 out. 2021.

[437] TEIXEIRA, Matheus. Supremo anula medida do governo que obrigava teles a compartilhar dados com o IBGE. **Folha de São Paulo**, 7 mai. 2020. Disponível em: https://www1.folha.uol.com.br/mercado/2020/05/supremo-anula-medida-do-governo-que-obrigava-teles-a-compartilhar-dados-com-o-ibge.shtml. Acesso em: 15 out. 2021.

[438] BRASIL. CONGRESSO NACIONAL. Ato declaratório do presidente da mesa do Congresso Nacional nº 112, de 19 de ago. 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Congresso/adc-112-mpv954.htm. Acesso em: 15 out. 2021.

[439] DIAS, Tatiana; MARTINS, Rafael Moro. Documentos vazados mostram que Abin pediu ao Serpro dados e foto de todas as CNHs do país. **The Intercept Brasil**, 6 jun. 2020. Disponível em: https://theintercept.com/2020/06/06/abin-carteira-motorista-serpro-vigilancia/. Acesso em: 15 out. 2021.

[440] PSB pede suspensão de compartilhamento de dados da CNH entre Serpro e Abin. **Portal STF**, 18 jun. 2020. Disponível em: http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=445873&ori=1. Acesso em: 15 out. 2021.

[441] GOVERNO revoga autorização dada Abin para acesso a dados da CNH. **Istoé**, 24 jun. 2020. Disponível em: https://istoe.com.br/governo-revoga-autorizacao-dada-abin-para-acesso-a-dados-da-cnh/. Acesso em: 15 out. 2021.

[442] VALENTE, Rubens. Ação sigilosa do governo mira professores e policiais antifascistas. **UOL**, 24 jul. 2020. Disponível em: https://laut.org.br/retrospectiva-tecnoautoritarismo-2020/. Acesso em: 15 out. 2021.

ação apresentada pelo Partido Rede Sustentabilidade, a qual acusava o governo de promover o "aparelhamento estatal" com o objetivo de realizar "perseguições políticas e ideológicas", declarou a inconstitucionalidade da produção do dossiê pelo Ministério da Justiça e determinou a suspensão dos atos do governo ligados à produção e compartilhamento de dossiês sobre cidadãos e servidores públicos.[443]

Já em dezembro, destaca-se o monitoramento de jornalistas, parlamentares e formadores de opinião pelo governo federal, categorizando-os entre "detratores", "neutros" e "favoráveis" em documento que contêm números de telefone, endereços de e-mail, dados de histórico profissional e posicionamento em assuntos sensíveis. [444] A lista foi produzida pela empresa BR+ Comunicação por meio de um contrato fechado com o governo federal e utilizado pelo Ministério da Economia, o qual foi encerrado após a divulgação do documento.[445] Paralelamente a isso foi revelado que a Secretaria Especial de Comunicação Social (Secom) também monitorava o comportamento de parlamentares de oposição e da base aliada do governo por meio das redes sociais.[446] Em resposta, o presidente Bolsonaro, o ministro da Secretaria de Governo e o chefe da Secom foram intimados a apresentarem documentos sobre esse monitoramento de redes sociais de parlamentares e jornalistas.[447]

Já em 2021, houve a abertura da licitação nº 3/2021, pelo Ministério de Justiça e Segurança Pública, para compra de "Solução de Inteligência em Fontes abertas, Mídias Sociais, Deep e Dark Web [...] em atendimento 'as necessidades operacionais da Diretoria de Inteligência da Secretaria de Operações Integradas (DINT/SEOPI)"[448], licitação essa que não envolve órgãos oficiais de inteligência e investigação, como o Gabinete de Segurança

---

[443] STF determina suspensão de dossiê do governo sobre servidores antifascistas. **Conectas**, 20 ago. 2020. Disponível em: https://www.conectas.org/noticias/stf-determina-suspensao-de-dossie-do-governo-sobre-servidores-antifascistas?utm_campaign=newsletter_-_agosto_2020_pt&utm_medium=email&utm_source=RD+Station. Acesso em: 15 out. 2021.

[444] VALENTE, Rubens. Relatório do governo separa em grupos jornalistas e influenciadores. **UOL**, 01 dez. 2020. Disponível em: https://noticias.uol.com.br/colunas/rubens-valente/2020/12/01/governo-bolsonaro-jornalistas-redes-sociais.htm. Acesso em: 15 out. 2021.

[445] VALENTE, Rubens. Ministério encerra vínculo com agência que fez lista de "detratores". **UOL**, 04 dez. 2020. Disponível em: https://noticias.uol.com.br/colunas/rubens-valente/2020/12/04/ministerio-economia-lista-jornalistas-influenciadores.htm. Acesso em: 15 out. 2021.

[446] MACHADO, Guilherme. Planalto monitora redes sociais de parlamentares e jornalistas com dinheiro público. **Época**, 20 nov. 2020. Disponível em: https://oglobo.globo.com/epoca/guilherme-amado/planalto-monitora-redes-sociais-de-parlamentares-jornalistas-com-dinheiro-publico-24755889. Acesso em: 15 out. 2021.

[447] MEGALE, Bela. Juiz intima Bolsonaro, Ramos e Wajngarten a apresentarem documentos sobre monitoramento de redes sociais de parlamentares e jornalistas. **O Globo**, 04 dez. 2020. Disponível em: https://blogs.oglobo.globo.com/bela-megale/post/juiz-intima-bolsonaro-ramos-e-wajngarten-apresentarem-documentos-sobre-monitoramento-de-redes-sociais-de-parlamentares-e-jornalistas.html. Acesso em: 15 out. 2021.

[448] MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. Pregão Eletrônico nº 3/2021. **Gov.br**, 2021. Disponível em: https://www.gov.br/mj/pt-br/acesso-a-informacao/licitacoes-e-contratosv1/licitacoes-e-contratos-segen/cglic/cpl/copy64_of_pregoes-02_2021. Acesso em: 15 out. 2021.

Institucional (GSI) e a Agência Brasileira de Inteligência (Abin), distorcendo, assim, o equilíbrio entre esses órgãos de inteligência.[449]

Soma-se a tudo isso o fato da pandemia do Covid-19 ter acelerado os investimentos em tecnologias de vigilância em todo o mundo, bem como normalizado a vigilância estatal e corporativa sobre os cidadãos.[450] Desse modo, face ao contexto de vigilantismo estatal em que o Cadastro Base do Cidadão está sendo implementado, observa-se que ele consiste tanto em um sistema de vigilância em si mesmo, quanto é um instrumento que pode vir a facilitar e a potencializar outros sistemas de vigilância, o que será melhor delineado no próximo tópico.

4.3 O CBC COMO UM SISTEMA DE VIGILÂNCIA

Conforme delineado no primeiro capítulo, a vigilância deve ser analisada a partir do conceito de dispositivo de Michel Foucault, o qual refere-se à junção de 03 (três) componentes: (i) um conjunto de elementos heterogêneos; (ii) uma função estratégica; (iii) jogos de poder e configurações de saber.[451] Nesse sentido, tem-se que a vigilância pode ser conceituada como uma série de práticas de monitoramento sistemático de um indivíduo ou grupo de indivíduos, com o objetivo de obter conhecimento (configurar um saber) para agir sobre esse indivíduo ou grupo, influenciando comportamentos, escolhas e processos sociais, conduzindo condutas e administrando a população. Essas práticas têm por propósito a influência, gestão, proteção ou administração do objeto da vigilância, para que se possa garantir a manutenção de uma relação de poder existente entre vigia e vigiado.[452] Nas palavras de David Lyon:

> Tudo envolve a obtenção de conhecimento daqueles que trabalham ou vivem dentro desse contexto social, e esse conhecimento se torna o meio de supervisão e administração. Ao organizar o conhecimento de um determinado grupo dentro dos arquivos relevantes, essas práticas tornam os grupos sujeitos à intervenção ou direção. [...] A classificação também é crucial, como técnica de poder, porque torna várias

[449] VALENÇA, Lucas. Carlos Bolsonaro intervém em compra de aparelho espião e cria crise militar. **UOL**, 19 mai. 2021. Disponível em: https://noticias.uol.com.br/politica/ultimas-noticias/2021/05/19/briga-entre-militares-e-carlos-bolsonaro-racha-orgaos-de-inteligencia.htm. Acesso em: 15 out. 2021.
[450] KLEIN, Naomi. Coronavírus pode construir uma distopia tecnológica. **The Intercept Brasil**, 13 mai. 2020. Disponível em: https://theintercept.com/2020/05/13/coronavirus-governador-nova-york-bilionarios-vigilancia/. Acesso em: 15 out. 2021.
[451] FOUCAULT, Michel. **Microfísica do poder**. Organização, introdução e revisão técnica de Roberto Machado. 11ª ed. São Paulo: Paz e Terra, 2021. p. 364-365.
[452] LYON, David. **Surveillance Studies**: An Overview. Cambridge: Polity, 2007. p. 14-15, 23.

> entidades conhecidas de maneiras particulares, para que possam ser gerenciadas de acordo. (tradução livre).[453] [454]

Ressalta-se que a vigilância é exercida em contextos e relações de poder variadas - como dentro de um contexto militar, um contexto comercial/industrial, um contexto de administração estatal e o censo, e de um contexto policial e de controle de criminalidade-, e, sendo assim, seu exercício pode se dar de diferentes formas. Na sociedade de controle exercem protagonismo, independentemente do contexto, a vigilância por meio da coleta e tratamento de dados[455] e a vigilância omnipresente/omnisciente[456], as quais exibem mais plenamente as características de massividade e continuidade da vigilância contemporânea, uma vez que a vigilância por meio de sistemas de dados, bem como a vigilância omnipresente/omnisciente, que integra múltiplas formas de vigilância, exercendo-a pela totalidade de um espaço e a todo tempo, permitem um saber completo sobre o(s) sujeito(s) vigiados, bem como criam uma suspeita categórica e generalizada. Isso acontece uma vez que a vigilância se dirige à toda uma população, sem suspeitos prévios e, dessa forma, sua finalidade é identificar sujeitos que possam vir a ser considerados suspeitos, invertendo a lógica do direito à presunção de inocência e influenciando e controlando o comportamento de todo um grupo, de forma generalizada[457].

Esses termos conceituais são importantes para que se possa entender o Cadastro Base do Cidadão tanto como um dispositivo de vigilância, quanto como um mecanismo facilitador e ampliador de outras técnicas de vigilância, os quais quando combinados constroem um aparato de vigilância massiva direcionada ao cidadão – uma tecnopolítica de vigilância. Inicialmente, cabe delimitar o contexto ostensivo dessa vigilância, qual seja: administração estatal. Portanto, a relação de poder em que a vigilância é exercida é aquela existente entre Estado e cidadão, na qual, por meio da vigilância, são configurados alguns saberes. Ainda, a função estratégica ostensiva desse dispositivo de vigilância, ou seja, a finalidade para a qual esses saberes serão utilizados, seria a desburocratização do compartilhamento de dados pessoais dos cidadãos brasileiros para aprimoramento da gestão de políticas públicas e prestação de serviços públicos.

---

[453] LYON, David. **Surveillance Studies**: An overview. Cambridge/Malden: Polity, 2007. p.87-88.

[454] "*All involve obtaining knowledge of those working or living within that social context, and that knowledge becomes the means of supervision and administration. By organizing knowledge of a particular group within the relevant files, these practices render the groups amenable to intervention or direction. […] Classification is crucial as well, as a technique of power, because it makes several entities known in particular ways, so that they can be acted on accordingly*".

[455] CLARKE, Roger. Information technology and dataveillance. In: **Communications of the ACM**, v. 31, n. 5, 1988. p. 498-512. p. 499

[456] CLARKE, Roger. A framework for surveillance analysis. 16 feb. 2012. Disponível em: http://www.rogerclarke.com/DV/FSA.html. Acesso em: 07 out. 2021

[457] MARX, Gary T. **Undercover**: Police surveillance in America. Berkeley/Los Angeles/London: University of California Press, 1988. p. 219.

De acordo com Foucault, a vigilância administrativa das populações "é uma das necessidades de todo poder" estatal, a qual dá ensejo a um saber ligado à gestão da população e do Estado em si.[458] O propósito dessa vigilância, portanto, seria a gestão e a administração da população e dos serviços e políticas públicas, em prol do cidadão.

A vigilância exercida por Estados para esses fins, dentro do contexto de administração pública, sempre existiu de uma forma ou de outra. Registros da população para tributação, por exemplo, ocorriam em sociedades antigas, como o Império Romano, e à medida que as formas de vigilância estatal se desenvolviam durante os séculos XIX e XX, elas tinham o propósito, pelo menos ostensivo – como é aqui o caso -, de criar registros para delimitar titularidade de direitos e obrigações, por exemplo.[459] Assim, a vigilância estatal administrativa não é nova, mas vem se desenvolvendo ao longo dos séculos, ganhando novas técnicas e práticas, sendo exemplos dessas novas técnicas as novas formas de vigilância já citadas – vigilância por meio de sistemas de dados e vigilância omnipresente e omnisciente. Conforme se observa no presente caso, a principal forma de vigilância exercida no âmbito do Cadastro Base do cidadão é a vigilância exercida por meio de sistemas de dados, na medida em que o cadastro possibilita a realização das técnicas de tratamento de dados como o *profiling*[460], "*front-end verification*"[461] e *data matching*[462], bem como objetiva facilitar o acesso a transações armazenadas por outras organizações, sendo esses elementos caracterizadores de uma *dataveillance* conforme descrito por Clarke.[463] Ainda, tem-se que o cadastro é um mecanismo facilitador da vigilância por meio de dados no âmbito estatal, tendo em vista que: (i) ele serve como uma base integradora de dados pessoais dos cidadãos, composta, inicialmente, por alguns atributos biográficos e cadastrais e eventualmente, por atributos biométricos, conforme outras bases de dados pessoais

---

[458] FOUCAULT, Michel**. A sociedade punitiva**: curso no Collège de France (1972-1973). Tradução de Ivone C. Benedetti. São Paulo: WMF Martins Fontes, 2015. p. 212.

[459] LYON, David. **Surveillance Studies**: An Overview. Cambridge: Polity, 2007. p. 30-31.

[460] *Profiling*, como já mencionado, é a técnica que permite inferir um conjunto de características de determinada classe de pessoas a partir de experiências e comportamento passados, criando um perfil para permitir classificá-lo e compará-lo com outros indivíduos que possuem conjuntos de características semelhantes. (CLARKE, Roger. Profiling: a hidden challenge to the regulation of data surveillance. In: **Journal of Law and Information Science**, v. 4, n.2, Dec. 1993. Disponível em: http://www.rogerclarke.com/DV/PaperProfiling.html. Acesso em: 10 set. 2021)

[461] A técnica *front-end verification* diz respeito ao processo de realizar a verificação cruzada de dados contidos em um formulário de requerimento com dados de outros sistemas e bases, a fim de facilitar o processamento de uma transação. (CLARKE, Roger. **Introduction to dataveillance and information privacy, and definitions of terms**. July 2016. Disponível em: http://www.rogerclarke.com/DV/Intro.html#DV. Acesso em: 10 set. 2021).

[462] A técnica de *data matching* consiste na expropriação de dados mantidos por um ou mais bases de dados pessoais com a finalidade de compará-los. (CLARKE, Roger. **Introduction to dataveillance and information privacy, and definitions of terms**. July 2016. Disponível em: http://www.rogerclarke.com/DV/Intro.html#DV. Acesso em: 10 set. 2021).

[463] CLARKE, Roger. A framework for surveillance analysis. 16 feb. 2012. Disponível em: http://www.rogerclarke.com/DV/FSA.html. Acesso em: 07 out. 2021.

dos cidadãos mantidas por órgãos públicos forem sendo acrescidas à base integradora; (ii) ele permite que o dado coletado para um propósito específico seja utilizado para outro totalmente diverso, sem o conhecimento de seu titular; sendo esses dois elementos facilitadores da vigilância por meio de dados, segundo Clarke.[464]

Retomando o conceito de dispositivo de Foucault, em suma, tem-se como elementos heterogêneos do Cadastro Base do Cidadão o decreto que o criou, as bases de dados que o compõe, as práticas de coleta, armazenamento e tratamento de dados pessoais – em suas diversas técnicas -, os discursos que o legitimam, bem como os outros sistemas de vigilância implementados por poderes públicos que podem vir a funcionar conjuntamente com ele. Ainda, tem-se como função estratégica a sua finalidade ostensiva, qual seja: a desburocratização do compartilhamento de dados pessoais dos cidadãos brasileiros para aprimoramento da gestão de políticas públicas e prestação de serviços públicos, melhorando, portanto, a administração pública frente as crescentes complexidades da sociedade. E, por fim, a relação de poder em que o cadastro se insere é aquela existente entre Estado e cidadão, da qual são retirados saberes de gestão. Assim, além de ser um facilitador da vigilância de dados estatal, compondo outras tecnopolíticas de vigilância, o Cadastro Base do Cidadão pode ser caracterizado como um dispositivo de vigilância em si mesmo, na medida em que ele conta com práticas de monitoramento da população por meio de sistemas de dados, com o objetivo de obter conhecimento (configurar um saber) sobre os cidadãos e com a finalidade de poder agir sobre a população, inicialmente – e ostensivamente – administrando-a e gerindo políticas e serviços públicos em seu benefício.

Aqui se fala na ostensividade da finalidade de administração pública, tendo em vista que o Cadastro Base do Cidadão abre azo para a integração de bases de dados mantidas por órgãos públicos militares, policiais e do serviço de inteligência, além de permitir que esses mesmos órgãos realizem a consulta da base de dados integradora e suas bases temáticas integradas (Cadastro Base do Cidadão) – o que pode se observar a partir da lista de órgãos que já solicitaram acesso ao cadastro, da qual constam a Abin e o Comando do Exército. Desse modo, por mais que a finalidade do cadastro seja voltada à gestão de políticas públicas, não se descarta a possibilidade do uso desse cadastro para fins de persecução penal, influência e controle social e, até mesmo, para criação de dossiês e perseguição política de indivíduos que são contrários ao governo atual – prática já realizada, conforme observado no tópico anterior.

---

[464] CLARKE, Roger. A framework for surveillance analysis. 16 feb. 2012. Disponível em: http://www.rogerclarke.com/DV/FSA.html. Acesso em: 07 out. 2021.

O CBC é, portanto, ele próprio um sistema de vigilância, mas que se integra com - e instrumentaliza - outros sistemas de vigilância estatais, bem como que pode vir a instrumentalizar e facilitar ações vigilantistas de variados órgãos públicos, a exemplo daquelas citadas no tópico anterior. Essa combinação de sistemas e tecnologias com capacidade de vigilância existente hoje no Brasil é precisamente o que Haggerty e Ericson chamam de *surveillant assemblages*, termo cunhado com base no conceito de *assemblage* de Deleuze e Guattari.[465] Segundo os autores Haggerty e Ericson, a vigilância contemporânea não tem por intuito moldar, punir ou controlar o corpo num primeiro momento, como se pretende na sociedade disciplinar, mas conhecê-lo para poder influenciá-lo, no sentido do que ressalta Byung Chul-Han, e, para isso, ele deve ser dividido em uma série de fluxos, transformado em uma série de dados que podem ser capturados e comparados e de onde informações úteis para a administração da população, dos corpos, possam ser retiradas. Esses fluxos de dados são armazenados e tratados em bases de dados com o intuito de desenvolver estratégias de governança e controle. A vigilância contemporânea depende dessa combinação de diversos sistemas e práticas que atuam juntos, com objetivos comuns, aumentando a capacidade e a intensidade da vigilância.[466]

Esse conglomerado de elementos com capacidade de vigilância é fluido e transcende limites institucionais, já que são integrações de variados sistemas e práticas, e, assim, um sistema que possuía uma finalidade pode vir a ser usado para outra totalmente diferente, o que também ocorre com os dados coletados no processo de monitoramento, já que, havendo a integração de diversos sistemas de vigilância, um dado coletado durante o monitoramento realizado por um sistema, com um intuito específico, pode ser utilizado para outro totalmente diverso quando da integração desses sistemas de vigilância, fenômeno comum atualmente, uma vez que bases de dados são vendidas ou compartilhadas entre organizações, como é o caso do Cadastro Base do Cidadão, que integra diversas bases de dados de órgãos públicos.[467]

---

[465] O conceito *assemblages*, cunhado por Deleuze e Guattari, que pode ser traduzido para "reunião" ou "agenciamento", se aproxima, de certa forma, do conceito de dispositivo cunhado por Foucault, tendo em vista que consiste em uma multiplicidade de objetos heterogêneos que podem trabalhar em conjunto, como uma entidade funcional. Assim, essa reunião/multiplicidade compreende um conjunto de fluxos de fenômenos, podendo esses serem divididos entre discursivos e não-discursivos, assim como os elementos do dispositivo. Desse modo, esses agenciamentos são parte de uma tentativa de organização de um espaço, por meio de processos de captura desses fluxos, para que se possa governar. (PATTON, Paul. Metamorpho-Logic: bodies and powers in A Thousand Plateaus. In: **Journal of the British Society for Phenomenology**, v. 25, no. 2, may 1994, p. 157-169) (HAGGERTY, Kevin D.; ERICSON, Richard V. The surveillant assemblage. In: British Journal of Sociology, v. 51, n. 4, dec. 2000, pp. 605-622. p. 608-609).

[466] HAGGERTY, Kevin D.; ERICSON, Richard V. The surveillant assemblage. In: British Journal of Sociology, v. 51, n. 4, dec. 2000, pp. 605-622. p. 608-612.

[467] HAGGERTY, Kevin D.; ERICSON, Richard V. The surveillant assemblage. In: British Journal of Sociology, v. 51, n. 4, dec. 2000, pp. 605-622. p. 616-617.

De acordo com os autores, as análises de vigilância tendem a focar nas capacidades de vigilância de uma diversidade de tecnologias e práticas individualizadamente, ressaltando os riscos cumulativos que esses sistemas e práticas impõem em relação à direitos e liberdades civis. No entanto, deve-se voltar o olhar para a atuação desses sistemas e práticas em conjunto, o que aumenta exponencialmente suas capacidades de vigilância. Se faz necessário, portanto, analisar a vigilância contemporânea como uma reunião, um agenciamento, de sistemas, tecnologias e práticas com capacidade para vigilância, os quais, invariavelmente, funcionam em conjunto, já que as organizações que fazem uso do exercício da vigilância procuram sempre integrar novas práticas, sistemas e instrumentos a esse exercício. Desse modo, a análise do Cadastro Base do Cidadão como um sistema de vigilância deve levar em conta, também, os outros sistemas, tecnologias e práticas que possuem capacidade de vigilância e estão em operação hoje no Brasil, conforme pontuado no tópico anterior, sendo o cadastro parte de uma grande tecnopolítica de vigilância que envolve todos esse conjunto de outros elementos.[468]

Esse olhar para todo o conjunto de sistemas de vigilância também deve ser utilizado quando da análise dos riscos que essas tecnopolíticas apresentam para os direitos e liberdades fundamentais dos cidadãos. Não se nega aqui que esse tipo de vigilância – a vigilância estatal administrativa – é necessária para a manutenção do poder do Estado e gestão populacional, assegurando que a distribuição de benefícios públicos seja correta, bem como que a criação de políticas públicas e a oferta de serviços públicos sejam adequadas ao contexto social, político e econômico do país. No entanto, deve-se ressaltar os potenciais de violação de direitos fundamentais e direitos humanos que algumas dessas tecnopolíticas de vigilância possuem, por variados motivos, mas principalmente por não respeitarem balizadores legais, como os preceitos legais e principiológicos da LGPD, bem como os preceitos constitucionais, discutidos no capítulo anterior. Ainda, o potencial de violação de direitos e liberdades é ainda maior quando há essa junção de diversas técnicas, práticas, tecnologias e tecnopolíticas de vigilância direcionadas ao monitoramento do cidadão, como se mostrou ser o caso do Brasil atualmente. Nesse sentido, cabe delinear aqui, primeiramente, a inadequação do Decreto 10.046/2019 e do Cadastro Base do Cidadão aos preceitos legais dispostos na LGPD, discutidos no segundo capítulo, e, porteriormente, os riscos aos direitos à proteção de dados pessoais e à privacidade, e, consequentemente, às liberdades deles derivam.

[468] HAGGERTY, Kevin D.; ERICSON, Richard V. The surveillant assemblage. In: British Journal of Sociology, v. 51, n. 4, dec. 2000, p. 605-622.

4.4 A (IN)ADEQUAÇÃO DO DECRETO 10.046/2019 E DO CBC À LGPD

Conforme discutido nos capítulos anteriores, a presença de balizadores legais e principiológicos é essencial quando da implementação de uma tecnopolítica de vigilância, tendo em vista os grandes riscos de violação a direitos e liberdades fundamentais em potencial apresentados pelo exercício da vigilância. No entanto, partindo da discussão desenvolvida no segundo capítulo sobre os preceitos legais e principiológicos dos direitos à privacidade e à proteção de dados pessoais, percebe-se que o referido Decreto 10.046/2019[469], bem como o Cadastro Base do Cidadão, vão de encontro com esses balizadores legais e principiológicos, representando uma ameaça à direitos e liberdades fundamentais dos cidadãos brasileiros.

A Constituição Federal, em seu artigo 37[470], estabelece que a Administração Pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios, deve atender, entre outros, ao princípio da legalidade em sua atuação, isto é, a atuação do Estado se restringe àquilo que lhe é permitido por lei. Considerando que o Decreto 10.046/2019 dispõe sobre as normas e diretrizes do compartilhamento de dados entre os órgãos e entidades da administração pública federal direta, autárquica e fundacional e os demais Poderes da União, tem-se que ele deve atender aos preceitos da Lei 13.709/2018[471], a Lei Geral de Proteção de Dados Pessoais (LGPD), tendo em vista que é ela que regula o tratamento de dados pessoais no Brasil, conforme delineado no segundo capítulo, inclusive aquele realizado pelo poder público (capítulo IV). No entanto, observa-se que o Decreto 10.046/2019 e o próprio Cadastro Base do Cidadão vão de encontro aos preceitos da LGPD, restringindo de forma indevida a privacidade e a proteção de dados pessoais.

A primeira incongruência encontrada entre o decreto e a LGPD diz respeito à algumas definições presentes nos referidos documentos. Antes mesmo da publicação da LGPD, os termos "dados pessoais", "informações pessoais" e "dados cadastrais" já constavam em alguns

---

[469] BRASIL. Decreto nº 10.046, de 9 de outubro de 2019. **Diário Oficial [da] União**, Brasília, 09 out. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 15 set. 2021.

[470] "Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte" (BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial [da] União**, Brasília, 5 de out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 15 out. 2021.

[471] Ressalta-se que, ainda que a LGPD não se encontrasse em vigência quando da edição do Decreto 10.046, em 9 de outubro de 2019, ela já havia sido publicada e encontrava-se em *vacacio legis* para que todos aqueles afetados pelas obrigações impostas pela Lei pudessem adequar seus processos de tratamento de dados pessoais. Desse modo, o referido decreto, ao tratar de matéria que complementa um dos capítulos da LGPD, deveria ter observado suas disposições.

documentos legais, como o Código de Defesa do Consumidor[472], a Lei de Acesso à Informação[473] e o Marco Civil da Internet[474]. O Decreto 8.789/2016[475] publicado durante a gestão de Michel Temer, e revogado pelo Decreto 10.046/2019, trazia uma definição mais extensa de dados cadastrais, em dissonância com os documentos anteriores, incluindo uma lista ampla e não restritiva desses dados. A LGPD, por sua vez, uniformizou esses conceitos, abandonando o conceito de "dado cadastral" e definindo 03 (três) categorias de dados, as quais influenciam no status de sua proteção, sendo elas:

a) dado pessoal, que se refere a informações relacionadas a pessoa natural identificada ou identificável;

b) dado pessoal sensível, referente a dados pessoais 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 e dado genético ou biométrico;

c) dado anonimizado, que se refere a dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do tratamento.[476]

No entanto, em completa desconsideração ao disposto na LGPD, o Decreto 10.046/2019 retomou o conceito de dados cadastrais, bem como introduziu uma nova classificação de dados pessoais, delineando os seguintes conceitos:

> I - 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;
>
> II - 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;
>
> III - dados cadastrais - informações identificadoras perante os cadastros de órgãos públicos, tais como:
> a) os atributos biográficos;

---

[472] BRASIL. Lei 8.078, de 11 de setembro de 1990. **Diário Oficial [da] União**, Brasília, 12 de setembro de 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8078compilado.htm. Acesso em: 15 out. 2021.
[473] BRASIL. Lei nº 12.527, de 18 de novembro de 2011. **Diário Oficial [da] União**, Brasília, 18 nov. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 15 out. 2021.
[474] BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Diário Oficial [da] União**, Brasília, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 15 out. 2021.
[475] BRASIL. Decreto nº 8.789, de 29 de junho de 2016. **Diário Oficial [da] União**, Brasília, 30 jun. 2016. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2016/Decreto/D8789.htm. Acesso em: 15 out. 2021.
[476] BRASIL. Lei 13.709, de 14 de agosto de 2018. **Diário Oficial [da] União**, Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 out. 2021.

> b) o número de inscrição no Cadastro de Pessoas Físicas - CPF;
> c) o número de inscrição no Cadastro Nacional de Pessoas Jurídicas - CNPJ;
> d) o Número de Identificação Social - NIS;
> e) o número de inscrição no Programa de Integração Social - PIS;
> f) o número de inscrição no Programa de Formação do Patrimônio do Servidor Público - Pasep;
> g) o número do Título de Eleitor;
> h) a razão social, o nome fantasia e a data de constituição da pessoa jurídica, o tipo societário, a composição societária atual e histórica e a Classificação Nacional de Atividades Econômicas - CNAE; e
> i) outros dados públicos relativos à pessoa jurídica ou à empresa individual;
>
> IV - atributos genéticos - características hereditárias da pessoa natural, obtidas pela análise de ácidos nucleicos ou por outras análises científicas;[477]

Observa-se que as classificações de dado pessoal previstas nos dois documentos são incompatíveis. Além de retomar um conceito já abandonado pela LGPD, o de dado cadastral, o decreto ainda ignora a existência do conceito de dados pessoais sensíveis previsto pela LGPD, criando uma classificação que mistura todos os tipos de dados previstas pela lei em uma única categoria. Ainda, o conceito de atributos biográficos inclui dados de conceituação vaga e ainda inexistente nas bases cadastrais do governo, como “fatos da sua vida” e “grupo familiar”.

Ao analisar a classificação do decreto à luz da LGPD, tem-se que todos as quatro classificações apresentam exemplos de dados pessoais considerados sensíveis (como filiação, dado genético e biométrico), sem que isso seja reconhecido pelo decreto. Essa incongruência se torna um problema principalmente em relação a proteção dada a cada tipo de dado, uma vez que a LGPD prevê proteção especial aos dados pessoais sensíveis (artigos 11-13)[478], já o decreto utiliza uma dicotomia já ultrapassada (dados públicos x dados sigilosos) para classificar o nível de proteção que um dado deve receber quando do seu tratamento ou compartilhamento. Essa forma de classificação estanque dos dados pessoais - se são sigilosos ou não -, para determinar a forma de compartilhamento, pressupõe que as regras de controle de acesso independem do contexto em que os dados foram coletados ou serão aplicados, sem levar em conta se um dado é ou não sensível de acordo com a definição da lei ou se ele pode mostrar-se sensível dentro do contexto de utilização.[479]

---

[477] BRASIL. Decreto nº 10.046, de 9 de outubro de 2019. **Diário Oficial [da] União**, Brasília, 09 out. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 15 set. 2021.
[478] BRASIL. Lei 13.709, de 14 de agosto de 2018. **Diário Oficial [da] União**, Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 out. 2021.
[479] BRASIL. Decreto nº 10.046, de 9 de outubro de 2019. **Diário Oficial [da] União**, Brasília, 09 out. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 15 set. 2021.

O nível de acesso e compartilhamento do dado pessoal, portanto, se público ou restrito, não pode balizar o nível de proteção desse dado, já que o que deve ser considerado é se aquele dado é ou não um dado pessoal – que é o caso de todos os dados que se pretende integrar ao Cadastro Base do Cidadão. Isso porque, o regime de proteção baseado no sigilo, na dicotomia público x privado, falha em dar uma resposta adequada à natureza complexa de utilização e tratamento de dados pessoais, o qual depende muito do tipo de dado – se dado pessoal ou dado pessoal sensível –, bem como dos processos de tratamento utilizados, de qual é o tipo de decisão que o processamento desse dado orientará e do contexto em que esse dado será utilizado.

Nesse sentido, retomando a decisão do Tribunal Constitucional Alemão:

> O fato de informações dizerem respeito a processos íntimos não decide por si só se elas são sensíveis ou não. É muito mais necessário o conhecimento do contexto de utilização, para que se constate a importância do dado em termos de direito da personalidade: Só quando existe clareza sobre a finalidade para a qual os dados são solicitados e quais são as possibilidades de uso e ligação [destes com outros] que existem, pode-se saber se a restrição do direito de autodeterminação da informação (no caso) é admissível.[480]

Em relação aos agentes de tratamento de dados pessoais, o decreto novamente introduziu conceitos diversos daqueles previstos pela LGPD, a qual, em seu artigo 5º, distingue 03 (três) principais agentes de tratamento, sendo eles:

a) o controlador, que deve ser uma pessoa natural ou jurídica, de direito público ou privado, a quem compete a tomada de decisão referente ao tratamento de dados pessoais (inciso VI);

b) o operador, que deve ser uma pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (inciso VII);

c) e o encarregado, uma pessoa indicada pelo controlador e pelo operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) (inciso VIII)[481].

O decreto, por sua vez, traz as seguintes definições em seu art. 2º:

> XI - **custodiante de dados** - órgão ou entidade que, total ou parcialmente, zela pelo armazenamento, pela operação, pela administração e pela preservação de dados, coletados pela administração pública federal, que não lhe pertencem, mas que estão sob sua custódia;

---

[480] MARTINS, Leonardo (org.). **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Tradução de Beatriz Hennig et al. Montevideo/Berlin: Konrad-Adenauer-Stiftung E. V., 2005. p. 239.
[481] BRASIL. Lei 13.709, de 14 de agosto de 2018. **Diário Oficial [da] União**, Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 out. 2021.

> XIII - **gestor de dados** - órgão ou entidade responsável pela governança de determinado conjunto de dados;
>
> XIV - **gestor de plataforma de interoperabilidade** - órgão ou entidade responsável pela governança de determinada plataforma de interoperabilidade;
>
> XXII - **recebedor de dados** - órgão ou entidade que utiliza dados após ser concedida permissão de acesso pelo gestor dos dados;
>
> XXIV - **solicitante de dados** - órgão ou entidade que solicita ao gestor de dados a permissão de acesso aos dados; (Redação dada pelo Decreto nº 10.332, de 2020).[482] (grifo do autor)

Observa-se que não fica claro quais órgãos poderiam exercer o papel de controlador e operador de dados e, portanto, serem responsabilizados como tal, como prevê o artigo 42 da LGPD. Ainda, o decreto deixa de indicar um encarregado, em atendimento ao artigo 23 da LGPD. Desse modo, por não seguir a classificação indicada pela lei, o decreto torna sua aplicação confusa, podendo dificultar a responsabilização dos agentes de tratamento.

Além das inconsistências nos conceitos apresentados por ambos os documentos, tem-se, ainda, que o decreto deixa de cumprir algumas exigências impostas pela LGPD ao poder público quando do tratamento de dados pessoais. Logo no início do capítulo IV, que dispõe sobre o tratamento de dados pessoais pelo poder público, a LGPD exige que esse tratamento seja realizado para o atendimento da finalidade pública do órgão, na persecução do interesse público, e com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, não deixando de informar as hipóteses legais desse tratamento e fornecer informações sobre a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades.[483] Conforme observa-se da leitura do decreto não há transparência quanto aos procedimentos e as práticas utilizadas para a execução das atividades de tratamento.

Já em relação à finalidade desse tratamento, o decreto cita como finalidade do compartilhamento de dados entre os órgãos dos poderes públicos:

a) simplificar a oferta de serviços públicos;

b) orientar e otimizar a formulação e gestão de políticas públicas;

c) a gestão de benefícios sociais e fiscais;

d) a melhoria da qualidade dos dados custodiados pela administração pública federal;

---

[482] BRASIL. Decreto nº 10.046, de 9 de outubro de 2019. **Diário Oficial [da] União**, Brasília, 09 out. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 15 set. 2021.

[483] BRASIL. Lei 13.709, de 14 de agosto de 2018. **Diário Oficial [da] União**, Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 out. 2021.

e) e o aumento da eficiência das operações internas da administração pública federal.

Ainda, cita como finalidades do Cadastro Base do Cidadão, além dessas já citadas, as seguintes:

a) viabilizar um meio unificado de identificação do cidadão para a prestação de serviços públicos;

b) disponibilizar uma interface unificada de atualização cadastral;

c) realizar o cruzamento de informações de bases de dados cadastrais oficiais a partir do CPF;

d) e facilitar o compartilhamento de dados pessoais dos cidadãos entre os órgãos da administração pública.[484]

Essas finalidades, no entanto, não atendem as exigências da LGPD quando observadas à luz do princípio da finalidade, bem como da exigência contida no artigo 23, *caput*, consistente na necessidade de o tratamento de dados pessoais pelo poder público ser realizado para o atendimento de sua finalidade pública. Isso porque, o princípio da finalidade, disposto no inciso I do art. 6º da lei, exige que o tratamento tenha propósitos "legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades"[485], no entanto, ao prever o compartilhamento amplo de dados pelos poderes públicos, bem como criar o Cadastro Base do Cidadão, que facilita esse compartilhamento, o decreto, além de não informar propósitos específicos desse tratamento, ainda abre a possibilidade de os dados pessoais do cidadão serem compartilhados sem seu conhecimento e serem utilizados com finalidades diversas daquelas inicialmente informadas.

Ainda, o artigo 26 da LGPD exige que o uso compartilhado de dados pessoais pelo Poder Público atenda à finalidade específica de execução de políticas públicas e atribuição legal pelos órgãos e entidades públicas, respeitados os princípios de proteção de dados pessoais que estão elencados no artigo 6º da mesma lei, sendo eles os princípios: da finalidade, da adequação, da necessidade, do livre acesso, da qualidade dos dados, da transparência, da segurança, da prevenção, da não discriminação e da responsabilização e prestação de contas.[486] No entanto,

---

[484] BRASIL. Decreto nº 10.046, de 9 de outubro de 2019. **Diário Oficial [da] União**, Brasília, 09 out. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 15 set. 2021.

[485] BRASIL. Lei 13.709, de 14 de agosto de 2018. **Diário Oficial [da] União**, Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 out. 2021.

[486] BRASIL. Lei 13.709, de 14 de agosto de 2018. **Diário Oficial [da] União**, Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 out. 2021.

novamente o decreto deixa de atender as exigências da lei[487]. Observa-se que a LGPD não autoriza a integração de bases de dados pessoais dos cidadãos e o compartilhamento irrestrito de dados pessoais entre órgãos públicos, sem levar em conta a finalidade e o contexto desse tratamento. De acordo com o artigo já citado, para cada novo tratamento de dados deve-se explicitar a finalidade exata desse tratamento, bem como a necessidade e a adequação do tratamento ao propósito. Ao utilizar a base legal de execução de políticas públicas, o poder público deve correlacionar a necessidade e a adequação do tratamento de dados pessoais com políticas públicas específicas já existentes e em processo de execução, impedindo o tratamento para finalidade genéricas, como é o caso do decreto.

Ao criar o Cadastro Base do Cidadão, o decreto facilita o compartilhamento irrestrito de dados pessoais entre os órgãos públicos, o que abre azo para que os dados coletados para uma finalidade específica por um órgão sejam compartilhados com outro órgão, o qual utilizará esses dados pessoais em outro contexto e com finalidade diversa daquela informada ao titular. Essa possibilidade produz uma insegurança jurídica por impedir a avaliação da adequação do tratamento à finalidade, violando, assim, o princípio da adequação, que exige a compatibilidade do tratamento com as finalidades informadas ao titular.

Nesse ponto, ressalta-se, ainda, que o tratamento de dados pessoais pelo poder público deve pautar-se pela separação informacional de poderes, ou seja, cada órgão deve tratar dados no limite daquilo que é estritamente necessário para o alcance de seus objetivos institucionais, respeitando os princípios da necessidade, da finalidade e da adequação. Assim, a falta de exatidão quanto às finalidades do acesso dos dados pessoais por cada órgão pode dar azo ao acesso a dados que extrapolam suas prerrogativas, colocando em risco a proteção de dados pessoais.

O decreto e o Cadastro Base do Cidadão também não atendem ao princípio da necessidade na medida em que pretendem a integração de todos os dados pessoais dos cidadãos existentes em posse de órgãos dos poderes públicos, caracterizando assim uma abrangência de dados excessiva em relação às finalidades do tratamento de dados específicas de cada órgão que terá acesso à essa base integradora, o que viola diretamente o princípio da necessidade, que preza pela limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência apenas dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento. Ainda, tem-se que o decreto também não atende totalmente o

[487] BRASIL. Lei 13.709, de 14 de agosto de 2018. **Diário Oficial [da] União**, Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 out. 2021.

princípio da transparência, por não deixar claro quais procedimentos e práticas são realizados no processo de tratamento de dados pessoais dos cidadãos, bem como não deixar claro quem são os agentes de tratamento de dados pessoais e como esse tratamento se adequará à LGPD, já que as definições trazidas pelo decreto são diversas daquelas dispostas na lei, conforme já mencionado. Há, ainda, opacidade em relação às regras de compartilhamento, tendo em vista que esse compartilhamento, segundo o decreto, é categorizado em três níveis de acordo com a confidencialidade do dado, sendo esses: o compartilhamento amplo; o compartilhamento restrito; e o compartilhamento específico. No entanto, a categorização do nível de compartilhamento, bem como a definição dos requisitos definidos como condição para o compartilhamento específico, fica sob responsabilidade dos gestores de dados (arts. 4º, §1º, 8º, caput e parágrafo único e 14, incisos I e II) e a definição dos procedimentos e as regras de compartilhamento ficam sob responsabilidade do Comitê Central de Governança de Dados (arts. 10, parágrafo único, art. 12)[488], o que possibilita à Administração Pública delimitar suas próprias regras de compartilhamento e tratamento de dados pessoais, sem atender às obrigações e responsabilidades da LGPD.

Por fim, o Decreto 10.046/2019 estabelece o Comitê Central de Governança de Dados (capítulo V), o qual, ressalta-se, é formado como um comitê intergovernamental, sem a participação da sociedade civil e outros setores interessados, e que possui por atribuições (art. 21) deliberar sobre as regras e os parâmetros para compartilhamento de dados, deliberar sobre as diretrizes para a categorização do nível de compartilhamento, deliberar sobre a escolha das bases à serem integradas ao CBC, entre outras[489], algumas das quais podem, eventualmente, entrar em conflito com as atribuições da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) (art. 55-J), instituída pela Lei Geral de Proteção de Dados.[490]

Observa-se, assim, que o Decreto 10.046/2019, apesar de prever em seu artigo 3º, inciso I, que devem ser observados os preceitos da LGPD, a partir de uma análise geral, não atende a própria regra. Isso porque tanto o decreto, quanto o próprio Cadastro Base do Cidadão, entram em conflito direto com várias disposições da LGPD, ao permitir, por exemplo, a integração de bases de dados e o cruzamento de dados pessoais de forma irrestrita, sem estar de acordo com

---

[488] BRASIL. Decreto nº 10.046, de 9 de outubro de 2019. **Diário Oficial [da] União**, Brasília, 09 out. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 15 set. 2021.

[489] BRASIL. Decreto nº 10.046, de 9 de outubro de 2019. **Diário Oficial [da] União**, Brasília, 09 out. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 15 set. 2021.

[490] BRASIL. Lei 13.709, de 14 de agosto de 2018. **Diário Oficial [da] União**, Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 out. 2021.

os preceitos principiológicos de proteção de dados pessoais, sem prever a elaboração de relatórios de impacto de proteção de dados pessoais, sem prever mecanismos adequados de segurança da informação, e sem que informações claras e transparentes a respeito da coleta e do tratamento, bem como a respeito de quem são e como devem agir os agentes de tratamento, sejam conhecidas dos cidadãos. Sendo assim, pode-se considerar que os tratamentos de dados pessoais realizados sob as disposições do decreto são irregulares, de acordo com o disposto no artigo 44 da LGPD, que dispõe que "o tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar [...]"[491].

Não se pode negar a importância do tratamento de dados para a gestão de políticas públicas, o que, conforme já mencionado, é permitido pela própria Lei Geral de Proteção de Dados Pessoais. No entanto, esse deve ser compatibilizado com os preceitos legais, para evitar a violação de direitos fundamentais. No caso, o Decreto 10.046/2019 viola diretamente a LGPD e, portanto, não é apropriado aos fins que indica. A inadequação e irregularidade do Decreto aqui demonstradas, a falha em respeitar os balizadores legais e principiológicos, conforme delineado no capítulo anterior, além de trazer insegurança jurídica, podem acarretar a violação de outros direitos fundamentais que derivam diretamente do direito à proteção de dados pessoais e do direito à privacidade, o que será delineado no próximo tópico.

4.5 O CBC COMO UM RISCO À DIREITOS DERIVADOS DA PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE

Observa-se que, além de ter sido implementado em um contexto em que pode vir a auxiliar a atuação de outros sistemas de vigilância estatais que também apresentam riscos à direitos e liberdades fundamentais dos cidadãos, por meio da permissão facilitada de acesso à uma base de dados que integra milhões de dados dos cidadãos; o Cadastro Base do Cidadão ainda não se coaduna com os preceitos legais e principiológicos da Lei Geral de Proteção de Dados Pessoais, um dos principais balizadores do exercício de vigilância por meio de sistemas de dados, conforme delineado no segundo capítulo, o que acaba por restringir em excesso o direito à privacidade e o direito à proteção de dados pessoais, dois direitos protegidos não só pela LGPD, quanto pela própria Constituição Federal de 1988, que os traz como sendo direitos

[491] BRASIL. Lei 13.709, de 14 de agosto de 2018. **Diário Oficial [da] União**, Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 out. 2021.

fundamentais de todos os cidadãos.[492] Ainda, a restrição em excesso dos direitos à privacidade e à proteção de dados pessoais acaba abrindo margem para a violação de outros direitos e liberdades fundamentais que derivam diretamente desses dois, tendo em vista que o direito à proteção de dados possui implicações que vão além da proteção da privacidade, possuindo características próprias, e implicando na viabilização e garantia de outros direitos fundamentais de toda uma coletividade, uma vez que diversas formas de controle passam a ser possíveis por meio do tratamento de dados pessoais.[493]

Nesse sentido, em decisão histórica do Tribunal Constitucional Federal Alemão, de 1983, em apreciação da previsão de coleta e uso de dados pessoais pelo poder público, a Corte assentou que:

> Hoje, com ajuda do processamento eletrônico de dados, informações detalhadas sobre relações pessoais ou objetivas de uma pessoa determinada ou determinável (dados relativos à pessoa [cf. § 2 I BDSG – Lei Federal sobre a Proteção de Dados Pessoais]) podem ser, do ponto de vista técnico, ilimitadamente armazenados e consultados a qualquer momento, a qualquer distância e em segundos Além disso, podem ser combinados, sobretudo na estruturação de sistemas de informação integrados, com outros bancos de dados, formando um quadro da personalidade relativamente completo ou quase, sem que a pessoa atingida possa controlar suficientemente sua exatidão e seu uso. Com isso, ampliaram-se, de maneira até então desconhecida, as possibilidades de consulta e influência que podem atuar sobre o comportamento do indivíduo em função da pressão psíquica causada pela participação pública em suas informações privadas.[494]

Assim, tem-se que, em vista da alta capacidade de processamento de dados dos sistemas atuais, a proteção de dados pessoais e o direito a autodeterminação informacional é requisito indispensável para que direitos como dignidade da pessoa humana, igualdade, livre manifestação de pensamento, e à liberdade de consciência e crença, à liberdade de expressão de atividade intelectual, artística, científica e de comunicação e à liberdade de associação, sejam garantidos. Um indivíduo que não tem conhecimento exato sobre quais informações, sobre sua pessoa são conhecidas, por quem são conhecidas, e para que finalidades são utilizadas, pode

---

[492] Ressalta-se que o direito à proteção de dados pessoais teve sua autonomia em relação ao direito à privacidade reconhecida por decisão do Plenário do Supremo Tribunal Federal na Ação Direta de Inconstitucionalidade nº 6.387/DF. Ainda, o reconhecimento do direito à proteção de dados como um direito fundamental se deu por meio de aprovação, em 20 de outubro de 2021, da Proposta de Emenda à Constituição (PEC) 17/2019. A PEC torna a proteção de dados pessoais, inclusive nos meios digitais, um direito fundamental, incluído entre as cláusulas pétreas, e remete privativamente à União a função de legislar sobre o tema. (SENADO inclui proteção de dados pessoais como direito fundamental na Constituição. **Senado Federal notícias**, 20 out. 2021. Disponível em: https://www12.senado.leg.br/noticias/materias/2021/10/20/senado-inclui-protecao-de-dados-pessoais-como-direito-fundamental-na-constituicao. Acesso em: 21 out. 2021).

[493] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2. Ed. São Paulo: Thomson Reuters Brasil, 2020. p. 2-3.

[494] MARTINS, Leonardo (org.). **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Tradução de Beatriz Hennig et al. Montevideo/Berlin: Konrad-Adenauer-Stiftung E. V., 2005. p. 237.

ser inibido em suas liberdades. Se um indivíduo souber, ou mesmo desconfiar, que sua participação em uma assembleia, em uma manifestação ou em qualquer iniciativa popular podem ser registradas por autoridades públicas, podendo, eventualmente, lhe causar problemas, esse se sentirá inibido de exercer seus direitos e liberdades fundamentais. Desse modo, o processamento e compartilhamento irrestritos de dados pessoais dos cidadãos pelo poder público, combinado à falta de transparência sobre como se dá o tratamento e para quais finalidades específicas ele é feito, como se pretendeu com a criação do Cadastro Base do Cidadão, pode impedir o livre desenvolvimento da personalidade.[495]

Ainda, deve-se ressaltar que, conforme já mencionado, a forma como o Decreto 10.046/2019 classifica os dados torna esses riscos ainda maiores, já que pretende que os dados sejam classificados fora do contexto de uso. Conforme explicitado na decisão alemã:

> [...] não se pode apenas condicionar o tipo de dados [que podem ser levantados, transmitidos etc.]. Decisivos são sua utilidade e possibilidade de uso. [...] Com isso, um dado em si insignificante pode adquirir um novo valor: desse modo, não existem mais dados "insignificantes" no contexto do processamento eletrônico de dados.[496]

Desse modo, qualquer dado pessoal, por mais que em um primeiro momento possa parecer insignificante ou "inofensivo" para o seu titular, deve ser tratado com as devidas salvaguardas legais, pois dependendo do contexto em que é utilizado pode vir a representar aspectos sensíveis da vida de seu titular. Um exemplo é a presença do nome de um indivíduo em um cadastro contendo informações sobre a população LGBTQIA+ de determinado país, estado ou município. O nome de um indivíduo, em um primeiro momento, pode ser considerado como um dado "inofensivo". No entanto, sua presença nesse tipo de base de dados revela um dado pessoal sensível de seu titular, qual seja: sua orientação sexual[497].

O Cadastro Base do Cidadão, portanto, por facilitar o compartilhamento praticamente irrestrito de dados pessoais dos cidadãos entre os órgãos públicos, sem considerar o contexto em que serão utilizados – e, consequentemente, sem dar as devidas salvaguardas ao tratamento desses dados pessoais – pode representar um sistema que interfere indevidamente no desenvolvimento da personalidade e na garantia de vários direitos e liberdades fundamentais dos cidadãos. Uma das condições necessárias para que a personalidade se desenvolva é o que

---

[495] MARTINS, Leonardo (org.). **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Tradução de Beatriz Hennig et al. Montevideo/Berlin: Konrad-Adenauer-Stiftung E. V., 2005. p. 237-238.

[496] MARTINS, Leonardo (org.). **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Tradução de Beatriz Hennig et al. Montevideo/Berlin: Konrad-Adenauer-Stiftung E. V., 2005. p. 239.

[497] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2. Ed. São Paulo: Thomson Reuters Brasil, 2020. p. 91.

Neil Richards chama de privacidade intelectual. De acordo com Richards, a privacidade intelectual consiste em uma zona de proteção da capacidade de decidir livremente do ser humano, assim, essa privacidade seria a proteção necessária contra a vigilância e/ou a interferência indesejada de terceiros nos processos de desenvolvimento e geração de ideias e crenças, nos processos de exercício das liberdades garantidas constitucionalmente, o que permitiria que os cidadãos desenvolvam suas individualidades e capacidades intelectuais.[498]

A privacidade intelectual baseia-se, portanto, no fato de que as liberdades fundamentais são elemento básico de realização do princípio democrático, de uma sociedade livre.[499] De acordo com Canotilho, o exercício democrático do poder depende da participação de todos os cidadãos, a qual, por sua vez, exige que sejam colocadas em prática garantias de liberdade (liberdade de expressão, de formação de partido político, de associação etc.) e de direito sociais, econômicos e culturais, para que os indivíduos possam exercer plenamente a participação democrática. Assim, é somente por meio da garantia desses direitos que uma sociedade democrática pode se realizar, sem eles, abre-se espaço para o exercício de um poder antidemocrático.[500] Nesse sentido, para o autor:

> os direitos fundamentais, como *direitos subjectivos de liberdade*, criam um espaço pessoal contra o exercício de poder antidemocrático e, como direitos legitimadores de um domínio democrático, asseguram o exercício da democracia mediante a exigência de *garantias de organização* e de *processos* com transparência democrática (princípio majoritário, publicidade crítica, direito eleitoral).[501] (grifos do autor).

Ademais, a restrição dessas liberdades por meio da vigilância pode produzir efeitos disciplinadores[502] e moduladores[503], efeitos de autocensura e conformação, conforme explica a teoria da espiral do silêncio (*spiral of silence*), bem como a base teórica do panóptico explicada por Foucault, ambas delineadas no primeiro capítulo. Sem a garantia de que não haverá interferência indevida no exercício das liberdades e sob os efeitos "normalizantes" da vigilância, os cidadãos não podem desenvolver plenamente sua personalidade, suas ideias e crenças e sua capacidade de autogoverno, por se autocensurarem e se conformarem em seguir as expectativas da maioria, do que é considerado convencional, o que inibe, em consequência,

---

[498] RICHARDS, Neil. **Intellectual Privacy:** rethinking civil liberties in the digital age. New York: Oxford University Press, 2015. p. 95
[499] RICHARDS, Neil. The dangers of surveillance. In: **Harvard Law Review**, v. 126, 2013, p. 1946-1947.
[500] CANOTILHO, J.J. Gomes. **Direito Constitucional e Teoria da Constituição**. 7ª ed., Coimbra: Almedina, 2003. p. 290-291.
[501] CANOTILHO, J.J. Gomes. **Direito Constitucional e Teoria da Constituição**. 7ª ed., Coimbra: Almedina, 2003. p. 291.
[502] Termo que se refere à sociedade disciplinar de Foucault.
[503] Termo que se refere à sociedade de controle de Deleuze.

sua plena participação na realização da democracia.[504] Assim, esse poder de tratamento e compartilhamento quase irrestrito de dados pelo poder público pode apresentar sérios riscos à democracia ao ignorar a necessária proteção de direitos e liberdades fundamentais em nome da eficiência. Nas palavras do Ministro Ruy Rosado de Aguiar, em voto de Recurso Especial, datado de 1995:

> [...] assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos ou privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica.[505]

Nesse sentido, ao não fornecer as devidas salvaguardas impostas pela Lei Geral de Proteção de Dados Pessoais, bem como ao não divulgar as finalidades e os processos de tratamento de dados utilizados, o decreto e o CBC restringem demasiadamente o direito à proteção de dados e à autodeterminação informativa. Nesse contexto, o cidadão, titular dos dados pessoais, ao ser obrigado a aceitar a coleta de dados pessoais pelo Estado para uma finalidade extremamente genérica (como é a de execução de políticas públicas), estaria sendo igualmente obrigado a viver sob um regime de insegurança, uma vez que a generalização da finalidade abre azo para uma miríade de outras finalidades sem que o cidadão tenha conhecimento, o que viola, portanto, sua autodeterminação informativa, sua capacidade de controle sobre a divulgação e uso de seus próprios dados pessoais, além de violar os outros direitos relacionados à proteção de dados, como a já mencionada privacidade intelectual, desenvolvimento da personalidade, expressão das liberdades e, também, da dignidade da pessoa humana.

Da mesma maneira, tem-se que a coleta e tratamento irrestrito de dados pessoais pode ferir a dignidade da pessoa humana, o direito à igualdade e não discriminação, o livre desenvolvimento da personalidade e a expressão das liberdades constitucionalmente garantidas, tendo em vista que a coleta e o tratamento massivo de dados (a vigilância massiva por meio de dados) dá origem à uma assimetria de poder muito grande entre o titular dos dados e aquele que está em posse deles para a realização do tratamento. Conforme delineado no primeiro capítulo, o conhecimento obtido a partir dessa vigilância realizada por meio da coleta e tratamento de dados pessoais produz poderes de influência, chantagem e persuasão, práticas comuns em Estados totalitários, os quais transformavam registros obtidos por meio de vigilância em armas

---

[504] RICHARDS, Neil. The dangers of surveillance. In: **Harvard Law Review**, v. 126, 2013, p. 1949

[505] STJ. **Recurso Especial n° 22.337/RS**, rel. Min. Ruy Rosado de Aguiar, DJ 20/03/1995. In: R. Sup. Trib. Just., Brasília, a. 8, (77): 199-257, janeiro 1996. p. 206

políticas, mas que não deixam de existir em sociedades democráticas, as quais, por sua vez, também realizam o monitoramento de indivíduos relevantes (e comumente dissidentes), como foi o caso da vigilância realizada sobre Martin Luther King Jr. nos Estados Unidos da América pelo FBI[506], e como é o caso dos dossiês de dissidentes e "detratores" produzidos pelo Ministério da Justiça e Segurança Pública e sua "Abin paralela"[507], bem como do monitoramento e classificação de jornalistas e professores pelo governo, mencionados anteriormente.[508] Nesse sentido, as disposições do decreto e o CBC causam grande preocupação por facilitarem o acesso à todo tipo de dado pessoal dos cidadãos à todos os órgãos públicos, incluindo esses mesmos que criaram dossiês de dissidentes para o governo, bem como os órgãos de inteligência (como a Abin e o GSI) e órgãos militares (como o Comando do Exército), sem as devidas salvaguardas e sem a devida transparência, minando os processos e as liberdades democráticas.

Por fim, tendo em vista que o tratamento desses dados orientará tomadas de decisão que afetarão diretamente a vida dos cidadãos, tem-se que o decreto 10.046/2019 e o CBC podem vir a violar os direitos constitucionalmente protegidos da dignidade da pessoa humana e da igualdade e não discriminação. Isso porque, de acordo com David Lyon, o ímpeto classificatório, presente em qualquer tipo de vigilância, pode criar ou sustentar condições de desigualdade social e identidades de marginalidade já existentes, uma vez que os sistemas técnicos utilizados para a realização da classificação absorvem e reproduzem valores culturais, sociais e econômicos dominantes na sociedade. Assim, esse tratamento massivo de dados pessoais dos cidadãos que tem a finalidade genérica de gestão de políticas públicas, ao mesmo tempo em que pode garantir que os indivíduos recebam os serviços e benefícios sociais devidos, garantindo tratamento justo e equalitário, podem também criar oportunidade para políticas autoritárias, arbitrárias e discriminatórias, reproduzindo, por exemplo, o racismo estrutural existente na força policial.[509] [510] Assim, esse poder de classificação se traduz em poder de

---

[506] RICHARDS, Neil. The dangers of surveillance. In: **Harvard Law Review**, v. 126, 2013, p. 1953-1955.
[507] VALENTE, Rubens. Ação sigilosa do governo mira professores e policiais antifascistas. **UOL**, 24 jul. 2020. Disponível em: https://laut.org.br/retrospectiva-tecnoautoritarismo-2020/. Acesso em: 15 out. 2021.
[508] VALENTE, Rubens. Relatório do governo separa em grupos jornalistas e influenciadores. **UOL**, 01 dez. 2020. Disponível em: https://noticias.uol.com.br/colunas/rubens-valente/2020/12/01/governo-bolsonaro-jornalistas-redes-sociais.htm. Acesso em: 15 out. 2021.
[509] LYON, David. Identification, surveillance and democracy. In: HAGGERTY, Kevin D.; SAMATAS, Minas. (editors). **Surveillance and Democracy**. Abingdon/New York: Routledge, 2010. pp. 34-50. p. 34.
[510] MONAHAN, Torin. Social inequality and the pursuit of democratic surveillance. In: HAGGERTY, Kevin D.; SAMATAS, Minas. (Ed.). **Surveillance and Democracy**. Abingdon/New York: Routledge, 2010. pp. 91-110. p. 105-106.

discriminação de cidadãos com base em elementos como situação financeira, região de residência, raça, etnia, gênero ou orientação sexual.[511]

Como bem salientado pelo então Ministro Ruy Rosado de Aguiar, da mesma forma que o tratamento e compartilhamento quase irrestrito de dados pessoais dos cidadãos entre os órgãos públicos pode ser usado para fins lícitos, na gestão de políticas públicas, em prol dos próprios cidadãos, ele pode, igualmente, auxiliar o Estado a alcançar fins contrários à moral, aos costumes e ao Direito, como instrumento de perseguição política, opressão econômica ou discriminação ilegal.[512] Desse modo, o Cadastro Base do Cidadão, por não se coadunar com preceitos legais, principiológicos e contextuais impostos às práticas de vigilância estatal, o que o torna incompatível com os processos e liberdades constitucionais e democráticos, conforme delineados no segundo capítulo, ultrapassa os limites do que seria uma prática de vigilância aceitável – e até bem-vinda – em sociedades democráticas.

[511] RICHARDS, Neil. The dangers of surveillance. In: **Harvard Law Review**, v. 126, 2013, pp. 1934-1965. p. 1957.
[512] STJ. **Recurso Especial n° 22.337/RS**, rel. Min. Ruy Rosado de Aguiar, DJ 20/03/1995. In: R. Sup. Trib. Just., Brasília, a. 8, (77): 199-257, janeiro 1996. p. 206

5 CONCLUSÃO

Os desafios colocados pela política e cultura vigilantista são imensos. Por ser necessária em diversos contextos e para diversas finalidades, a vigilância é justificada e legitimada com sucesso, no entanto, seus riscos para a democracia e os direitos e liberdades fundamentais são igualmente significativos Diante desse contexto inicialmente apresentado da Sociedade de Controle, suas tendências vigilantistas e os riscos que essas tendências apresentam, o problema de pesquisa colocado consistia na seguinte questão: a Lei Geral de Proteção de Dados Pessoais (Lei n 13.709/2018), em conjunto com a Constituição Federal de 1988, é eficiente em mitigar os riscos apresentados pelas tecnopolíticas de vigilância implementadas no Brasil? Questão a qual, inicialmente, pensava-se ter resposta negativa, e, nesse sentido, a hipótese de pesquisa consistia na insuficiência do ordenamento jurídico brasileiro – leia-se a ineficácia da LGPD em conjunto com a Constituição Federal de 1988 -, em frear e/ou mitigar os riscos aos direitos fundamentais e à democracia derivados das tecnopolíticas de vigilância. Desse modo, determinou-se como objetivo geral da pesquisa a realização de uma análise do Cadastro Base do Cidadão a fim de verificar se ele se enquadra como um sistema de vigilância e, se sim, se está de acordo com os preceitos legais e principiológicos da privacidade e da proteção de dados.

Conforme se verificou no desenvolvimento da pesquisa, os custos para os direitos e liberdades fundamentais dos cidadãos derivados do exercício irrestrito da vigilância são significativos. Por esse motivo, a imposição de limites ao exercício da vigilância, a exigência de que os sistemas e práticas vigilantistas estejam de acordo com os preceitos conceituais e principiológicos da proteção de dados pessoais e da privacidade é tão importante. Só assim é que se pode obter os benefícios da vigilância sem sacrificar os direitos e liberdades ou criar uma relação de poder entre governos e cidadãos tão desequilibrada que a democracia não pode ser mantida.

Daí a importância da Lei Geral de Proteção de Dados Pessoais (LGPD - Lei no. 13.709/2018) para a regulação das tecnopolíticas de vigilância, as quais vem se multiplicando de forma irrefreada não só no Brasil, mas na grande maioria dos países, sendo eles institucionalmente democráticos ou não. A legislação brasileira cumpre seu papel em impor limites adequados à essas práticas, incentivando uma cultura de transparência e fiscalização tão importante para as práticas de tratamento de dados pessoais. No entanto, no decorrer da pesquisa, o que se verificou foi que embora a legislação brasileira seja adequada para mitigar os riscos impostos pelas tecnopolíticas de vigilância aos preceitos democráticos, o problema se encontra em sua aplicação, já que em diversos casos a própria lei é mitigada em prol do

exercício irrestrito e massificado da vigilância, como é o caso do Cadastro Base do Cidadão, aqui analisado, o que torna a problema de pesquisa de outra ordem. Tem-se, portanto, que a LGPD é suficiente para mitigar os riscos criados por um sistema massivo de vigilância como o CBC apenas no mundo ideal, no entanto, questões materiais do mundo real, a forma como a sociedade e o Estado são construídos, impedem que a lei, sozinha e isoladamente, possa mitigar os riscos criados por um sistema de vigilância estatal como o CBC.

O Cadastro Base do Cidadão (CBC), conforme anteriormente delineado, é um sistema de vigilância que se coaduna, em um primeiro momento, com uma das hipóteses legalmente permitidas pela LGPD para o tratamento de dados pessoais realizado pelo Poder Público. O próprio Decreto n 10.046/2019 que institui o CBC dispõe sobre a exigência de observância da LGPD para o compartilhamento de dados entre os órgãos da administração pública federal direta, autárquica e fundacional e os demais Poderes da União. Não obstante, o mesmo decreto vai diretamente de encontro com diversas disposições da LGPD em vários momentos, conforme verificado no decorrer da pesquisa.

Não fosse suficiente não respeitar os limites impostos pela legislação que versa sobre o tema no Brasil, o referido decreto ainda cria um sistema que vem para facilitar e aumentar a eficácia de outros sistemas de vigilância já implementados pelo poder público no Brasil, auxiliando, assim, na criação de um arsenal vigilantista, uma verdadeira *surveillant assemblage.* Conforme se observou no último capítulo (tópico 4.2), o CBC foi implementado em um contexto em que a vigilância massiva e distribuída da população é de grande interesse do poder público, seja para aumento da segurança pública, melhora na criação, implementação e fiscalização de políticas públicas ou para fins políticos não abertamente declarados. Esse crescente interesse pode ser observado pela implantação de tecnologias de videomonitoramento, com ou sem a tecnologia de reconhecimento facial, em locais públicos; a implantação de câmeras com reconhecimento de placas de veículos e de sistemas como o Córtex, implementado pela Secretaria de Operações Integradas (Seopi), setor da Secretaria Nacional de Segurança Pública do Ministério da Justiça e Segurança Pública; a destinação de verbas públicas para criação de projetos como o da Polícia Federal que pretende reunir em um único banco de dados informações criminais de todo o país, contando com a implementação do sistema ABIS (Solução Automatizada de Identificação Biométrica); a edição de Medida Provisória (n. 954) que determina o compartilhamento de dados por empresas de telecomunicações com o IBGE; a realização de convênio entre a Abin (Agencia Brasileira de Inteligência) e o Serviço Federal de Processamento de Dados para obter dados pessoais de cidadãos que possuem a Carteira Nacional de Habilitação (CNH); a criação de dossiês sobre

579 pessoas identificadas como antifascistas – dentre elas professores e policiais – pela Seopi; o monitoramento de jornalistas, parlamentares e formadores de opinião, categorizados como "detratores", "neutros" e "favoráveis", pelo governo federal; a abertura de licitação pelo Ministério da Justiça e Segurança Pública para compra de Solução de Inteligência em Fontes Abertas, Mídias Sociais, *Deep* e *Dark Web* em atendimento as necessidades operacionais da Seopi. Ações essas que variam entre tentativas bem e malsucedidas, mas que, não obstante, são todas tentativas de ação e implementação de sistemas vigilantistas que seriam exercidas as margens da lei e com finalidades que não estavam totalmente claras e, portanto, não eram de todo legítimas.

Assim, o CBC possui a capacidade de, por um lado, facilitar a criação, implementação e garantia de eficácia de políticas públicas e, por outro, centralizar e facilitar a vigilância estatal exercida sobre a população para fins escusos e com efeitos prejudiciais aos direitos fundamentais, sendo um dos sistemas vigilantistas mais abrangentes atualmente implementados no Brasil. Pode-se verificar que o Cadastro Base do Cidadão e o decreto que o implementou são tanto uma tecnopolítica de vigilância que ultrapassa os limites legais e principiológicos aceitáveis para esse tipo de ação dentro de uma democracia, quanto são mais um sistema que auxilia, facilita e potencializa as demais ações, práticas e sistemas vigilantistas já implementados e a serem implementados no Brasil pelo poder público. Esse é um exemplo real de construção de uma *surveillant assemblage*, conforme descrita por Haggerty e Ericson - mencionados no tópico 4.3. A vigilância contemporânea funciona com um intercâmbio de informações entre sistemas, do fluxo de dados, da atuação conjunta de diversos sistemas e práticas, com objetivos comuns, que aumentam a capacidade e a intensidade da vigilância. Por esse motivo essa análise do contexto é tão necessária, da qual se pode observar que, conforme reiteradamente ressaltado, o CBC é parte de um conglomerado de sistemas que formam uma grande tecnopolítica de vigilância, a qual, por não se coadunar com os preceitos legais, indicam uma miríade de pontenciais riscos à determinados direitos e liberdades fundamentais.

Nesse sentido, os estudiosos da área[513] vêm alertando para uma ascensão do tecnoautoritarismo no Brasil, no sentido do que ressalta Byung-Chul Han, para o qual a sociedade digital de vigilância, a sociedade de controle, que tem acesso inclusive ao inconsciente-coletivo, por meio do monitoramento constante e das técnicas preditivas do comportamento social futuro das massas, acaba por desenvolver traços totalitários, entregando os cidadãos à programação e ao controle psicopolítico.

[513] Pesquisadores de institutos de pesquisa sobre proteção de dados pessoais e vigilância no Brasil, como o Data Privacy Brasil, Lapin, InternetLab e Lavits, entre outros.

Verificado, portanto, que o problema é de outra ordem daquela inicialmente pensada, talvez o questionamento devesse ser: como implementar eficazmente os preceitos principiológicos da proteção de dados pessoais ao poder público para que as tecnopolíticas de vigilância se limitem às práticas de tratamento de dados pessoais extremamente necessárias para as finalidades – legalmente autorizadas – propostas inicialmente? No caso aqui analisado, o que resta é a esperança de que o CBC e o Decreto 10.046/2019 sejam julgados pelo que são na ADI 6.649/DF, isto é, inconstitucionais. Enquanto isso, no entanto, outros sistemas e práticas vigilantistas, e potencialmente danosos à democracia, vêm se proliferando no Brasil às margens da lei.

Desse modo, a pesquisa, inserida na Área de Concentração "Direito Socioambiental e Sustentabilidade" e Linha de Pesquisa "Estado, Sociedades, Povos e Meio Ambiente" do Programa de Pós-Graduação em Direito da PUCPR, refletiu sobre o papel do direito na promoção da dignidade, liberdade, justiça, de condições para o exercício da democracia e na proteção de direitos fundamentais dos cidadãos frente aos riscos advindos das tecnopolíticas de vigilância implementadas pelo Estado na Sociedade de Controle brasileira, voltando-se ao estudo da relação entre direitos fundamentais, novas tecnologias com capacidade para vigilância e reflexos na democracia no contexto da Sociedade de Controle, conforme pensada por Byung-Chul Han.

REFERÊNCIAS

ABU-LABAN, Yasmeen. The politics of surveillance: civil liberties, human rights and ethics. In: BALL, Kirstie; HAGGERTY, Kevin D.; LYON, David (Ed.). **Routledge Handbook of Surveillance Studies**. London/New York: Routledge, 2012. p. 420-427.

ANASTÁCIO, Kimberly; SANTOS, Bruna; VARON, Joana. Cadastro Base do Cidadão: a megabase de dados. Rio de Janeiro: Coding Rights, 2020. Disponível em: https://www.codingrights.org/docs/megabase.pdf. Acesso em: 24 set. 2021.

ANDREJEVIC, Mark. The big data divide. In: **International Journal of Communication**, v. 8, 2014. p. 1673-1689.

BALL, Kirstie; HAGGERTY, Kevin D.; LYON, David (Ed.). **Routledge Handbook of Surveillance Studies**. London/New York: Routledge, 2012.

BAUMAN, Zygmunt; LYON, David. **Vigilância líquida**. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2014.

BENTHAM, Jeremy. The Panopticon. In: MONAHAN, Torin; WOOD, David Murakami (Ed.). **Surveillance Studies**: a reader. New York: Oxford University Press, 2018. p. 31-35.

BLACK, Gillian; STEVENS, Leslie. Enhancing data protection and data processing in the public sector: the critical role of proportionality and the public interest. In: **Scripted**, v. 10, issue 1, p. 93-122, April 2013

BOFF, Salete Oro; LEAL, Dionis Janner. Dados pessoais, psicopoder e responsabilização: análise a partir da lei brasileira de proteção de dados. In: **Revista da Faculdade de Direito da UERJ**, Rio de Janeiro, n 39, jun. 2021, pp. 151-170.

BOYD, danah; CRAWFORD, Kate. **Six Provocations for Big Data**. Oxford, 2011. Paper apresentado em A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, Oxford Internet Institute em 21 set. 2011. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1926431. Acesso em: 04 mai. 2021.

BRASIL. CONGRESSO NACIONAL. **Ato declaratório do presidente da mesa do Congresso Nacional nº 112**, de 19 de ago. 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Congresso/adc-112-mpv954.htm. Acesso em: 15 out. 2021.

BRASIL. Congresso Nacional. Emenda Constitucional n 115. **Diário Oficial [da] União**, Brasília, 10 fev. 2022. Disponível em: https://www.in.gov.br/web/dou/-/emenda-constitucional-n-115-379516387. Acesso em: 29 mar. 2022.

BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial [da] União**, Brasília, 5 de out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 15 out. 2021

BRASIL. Decreto nº 8.789, de 29 de junho de 2016. **Diário Oficial [da] União**, Brasília, 30 jun. 2016. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2016/Decreto/D8789.htm. Acesso em: 15 out. 2021.

BRASIL. Decreto nº 9.662, de 1º de janeiro de 2019. **Diário Oficial [da] União**, Brasília, 01 jan. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9662.htm. Acesso em: 14 out. 2021

BRASIL. Decreto nº 10.046, de 9 de outubro de 2019. **Diário Oficial [da] União**, Brasília, 09 out. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 15 set. 2021.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. **Diário Oficial [da] União**, Brasília, 18 nov. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 15 out. 2021.

BRASIL. Lei 12. 965, de 23 de abril de 2014. Diário Oficial [da] União, Brasília, 23 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 15 nov. 2021.

BRASIL. Lei 13.709, de 14 de agosto de 2018. **Diário Oficial [da] União**, Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 out. 2021.

BRASIL. Medida provisória nº 954, de 17 de abril de 2020. **Diário Oficial [da] União**, Poder Executivo, Brasília, DF, 17 abr. 2020. Edição 74-C, seção 1-Extra, p.1 Disponível em: https://www.in.gov.br/web/dou/-/medida-provisoria-n-954-de-17-de-abril-de-2020-253004955. Acesso em: 15 set. 2021.

BRASIL. Ministério da Ciência, Tecnologia, Inovações e Comunicações/Agência Nacional de Telecomunicações. Resolução nº 727, de 29 de maio de 2020. **Diário Oficial [da] União**, Brasília, 03 jun. 2020. Edição 105, seção 1, p. 462. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-n-727-de-29-de-maio-de-2020-259923173. Acesso em: 15 set. 2021.

BRASIL. Ministério da Justiça e Segurança Pública. Portaria nº 793, de 24 de outubro de 2019. **Diário Oficial [da] União**, Brasília, 25 out. 2019. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-793-de-24-de-outubro-de-2019-223853575. Acesso em: 14 out. 2021.

BRASIL. Senado Federal. Proposta de Emenda à Constituição (PEC) 17 de 2019. Brasília, 03 de jun. de 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757. Acesso em: 15 nov. 2021.

BRASIL. STF. **ADI 6.387/DF**, número único 0090566-08.2020, Conselho Federal da Ordem dos Advogados do Brasil – CFOAB (requerente), Presidente da República, 20 abr. 2020. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165. Acesso em: 15 out. 2021.

BRASIL. STF. **ADI 6.387 MC / DF**. Plenário. Relator: Min. Rosa Weber. Data de julgamento: 07/05/2020. Decisão Monocrática concessiva da liminar da Relatora Ministra Rosa Weber de 24/04/2020

BRASIL. STF. **ADI 6.387 MC / DF**. Plenário. Relator: Min. Rosa Weber. Data de julgamento: 07/05/2020. Voto do Min. Gilmar Mendes, p. 90-121.

BRASIL. STF. **ADI 6.649/DF**, número único 0111621-15.2020, Conselho Federal da Ordem dos Advogados do Brasil – CFOAB (requerente), Presidente da República, 23 dez. 2020. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=6079238. Acesso em: 15 out. 2021.

BRASIL. STF. **ADI 6.649/DF**, número único 0111621-15.2020, Conselho Federal da Ordem dos Advogados do Brasil – CFOAB (requerente), Presidente da República, 23 dez. 2020. Intervenção da Associação Data Privacy Brasil de Pesquisa na qualidade de Amicus Curie, petição 616/2021, 07 jan. 2021. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=6079238. Acesso em: 15 out. 2021.

BRASIL. STF. **ADPF 695 MC/DF**. Decisão monocrática. Relator: Min. Gilmar Mendes. Data de julgamento: 24/06/2020.

BRASIL. STF. **ADPF 695/DF**, número único 0095712-30.2020, Partido Socialista Brasileiro -PSB (requerente), União, 16 jun. 2020. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5938693. Acesso em: 15 out. 2021

BRUNO, Fernanda. **Máquinas de ver, modos de ser**: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013.

CANOTILHO, J.J. Gomes. **Direito Constitucional e Teoria da Constituição**. 7ª ed., Coimbra: Almedina, 2003. P. 291

CASTRO, Leandro Nunes; FERRARI, Daniel Gomes. **Introdução à Mineração de Dados**: conceitos básicos, algoritmos e aplicações. São Paulo: Saraiva, 2016.

CLARKE, Roger. **A framework for surveillance analysis**. 16 feb. 2012. Disponível em: http://www.rogerclarke.com/DV/FSA.html. Acesso em: 07 out. 2021

CLARKE, Roger. **Dataveillance**: 15 years on. March 2003. Disponível em: http://www.rogerclarke.com/DV/DVNZ03.html. Acesso em: 10 set. 2021.

CLARKE, Roger. Information technology and dataveillance. In: **Communications of the ACM**, v. 31, n. 5, May 1988. p. 498-512.

CLARKE, Roger. **Introduction to dataveillance and information privacy, and definitions of terms**. July 2016. Disponível em: http://www.rogerclarke.com/DV/Intro.html#DV. Acesso em: 10 set. 2021.

CLARKE, Roger. Profiling: a hidden challenge to the regulation of data surveillance. In: **Journal of Law and Information Science**, v. 4, n.2, Dec. 1993. Disponível em: http://www.rogerclarke.com/DV/PaperProfiling.html. Acesso em: 10 set. 2021.

CLAVELL, Gemma Galdon. Dataveillance. In: ARRIGO, Bruce A. (Ed.). **The SAGE encyclopedia of surveillance, security, and privacy**. 1. v. em 1. Thousand Oaks: SAGE, 2018. p. 284-285.

COMITÊ CENTRAL DE GOVERNANÇA DE DADOS. Ministério da Economia. Resolução CCGD/ME nº 5, de 12 de janeiro de 2021. **Diário Oficial [da] União**, Brasília, 15 jan. 2021. Disponível em: https://in.gov.br/web/dou/-/resolucao-ccgd/me-n-5-de-12-de-janeiro-de-2021-299084556. Acesso em: 15 out. 2021.

CROCKFORD, Kade. How is face recognition surveillance technology racist? **ACLU**, 16 jun. 2020. Disponível em: https://www.aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist/. Acesso em 14 out. 2021.

DELEUZE, Gilles. **Conversações**, 1972-1990. Tradução de Peter Pál Pelbart. São Paulo: 34, 1992.

DATA PRIVACY BRASIL; LAUT. Retrospectiva tecnoautoritarismo - 2020. **LAUT**, 26 jan. 2021. Disponível em: https://laut.org.br/retrospectiva-tecnoautoritarismo-2020/. Acesso em: 15 out. 2021

DIAS, Tatiana; MARTINS, Rafael Moro. Documentos vazados mostram que Abin pediu ao Serpro dados e fotos de todas as CNHs do país. **The Intercept Brasil**, 06 jun. 2020. Disponível em: https://theintercept.com/2020/06/06/abin-carteira-motorista-serpro-vigilancia/. Acesso em: 15 set. 2021.

DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2. Ed. São Paulo: Thomson Reuters Brasil, 2020.

EUROPEAN UNION. **Regulation (EU) 2016/679 of the European Parliament and of the Council**, of 27 apr. 2016. Disponivel em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 15 nov. 2021.

FERNANDES, Elora Raad; TEFFÉ, Chiara Spadaccini. Reconhecimento facial: laissez-faire, regular ou banir? **Migalhas**, 16 jul. 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-vulnerabilidade/330766/reconhecimento-facial--laissez-faire--regular-ou-banir. Acesso em: 14 out. 2021

FOUCAULT, Michel**. A sociedade punitiva**: curso no Collège de France (1972-1973). Tradução de Ivone C. Benedetti. São Paulo: WMF Martins Fontes, 2015.

FOUCAULT, Michel. **A verdade e as formas jurídicas**. Conferências de Michel Foucault na PUC-Rio de 21 a 25 de maio de 1973. Tradução de Roberto Cabral de Melo Machado e Eduardo Jardim Morais. Rio de Janeiro: NAU, 2002.

FOUCAULT, Michel. **Em defesa da sociedade**: curso no Collège de France (1975-1976). Tradução de Maria Ermantina Galvão. 2. ed. São Paulo: WMF Martins Fontes, 2010.

FOUCAULT, Michel. **História da sexualidade I**: A vontade de saber. Tradução de Maria Thereza da Costa Albuquerque e J. A. Guilhon Albuquerque. 11. ed. Rio de Janeiro/São Paulo: Paz e Terra, 2011.

FOUCAULT, Michel. **Microfísica do poder**. Organização, introdução e revisão técnica de Roberto Machado. 11. ed. São Paulo: Paz e Terra, 2021.

FOUCAULT, Michel**. Nascimento da biopolítica**: curso dado no Collège de France (1978-1979). Tradução de Eduardo Brandão. São Paulo: Martins Fontes. 2008.

FOUCAULT, Michel**. O poder psiquiátrico**. Curso dado no Collège de France (1973-1974). Tradução de Eduardo Brandão. São Paulo: Martins Fontes, 2006.

FOUCAULT, Michel. **Vigiar e Punir** - Nascimento da Prisão. Tradução de Pedro Elói Duarte. Lisboa: 70, 2013. Edição do Kindle.

FRANCISCO, Pedro Augusto P.; HUREL, Louise Marie; LOBATO, Luisa Cruz. Videomonitoramento: web report. **Instituto Igarapé**, 2019. Disponível em: https://igarape.org.br/videomonitoramento-webreport/#intro. Acesso em: 12 out. 2021.

FREITAS, Cinthia Obladen de Almendra. Tratamento de dados pessoais e a legislação brasileira frente ao *profiling* e à discriminação a partir das novas tecnologias. In: **Revista de Direito, Governança e Novas Tecnologias**, v.3, n.2, ju./dez. 2017. p. 18-38.

GILLIOM, John; MONAHAN, Torin. **SuperVision**: An introduction to the Surveillance Society. Chicago: The University of Chicago Press, 2013.

GILLIOM, John. Overseers of the poor: Surveillance, resistance, and the limits of privacy. In: MONAHAN, Torin; WOOD, David Murakami (Ed.). **Surveillance Studies**: a reader. New York: Oxford University Press, 2018. p. 230-233.

GOVERNO revoga autorização dada Abin para acesso a dados da CNH. **Istoé**, 24 jun. 2020. Disponível em: https://istoe.com.br/governo-revoga-autorizacao-dada-abin-para-acesso-a-dados-da-cnh/. Acesso em: 15 out. 2021.

GREENFIELD, Adam. **Everyware**: The dawning age of ubiquitous computing. Berkeley: New Riders, 2006).

HAGGERTY, Kevin D.; ERICSON, Richard V. The new politics of surveillance and visibility. In: HAGGERTY, Kevin D.; ERICSON, Richard V. (Ed.). **The new politics of surveillance and visibility**. Toronto/Buffalo/London: University of Toronto Press, 2006. p. 3-25.

HAGGERTY, Kevin D.; ERICSON, Richard V. The surveillant assemblage. In: **British Journal of Sociology**, v. 51, n. 4, dec. 2000, p. 605-622.

HAGGERTY, Kevin D.; SAMATAS, Minas. Surveillance and democracy: an unsettled relationship. In: HAGGERTY, Kevin D.; SAMATAS, Minas. (Ed.). **Surveillance and Democracy**. Abingdon/New York: Routledge, 2010. p. 1-16.

HAN, Byung-Chul. **No enxame**: perspectivas do digital. Tradução de Lucas Machado. Petrópolis: Vozes, 2018.

HAN, Byung-Chul. **Psicopolítica**: O neoliberalismo e as novas técnicas de poder. Tradução de Maurício Liesen. Belo Horizonte: Âyiné, 2018.

HAN, Byung-Chul. **Sociedade da transparência**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017.

HECHT, Gabrielle. Technology, politics, and national identity in France. In: ALLEN, Michael Thad; HECHT, Gabrielle (Ed). **Technologies of Power**: Essays in honor of Thomas Parke Hughes and Agatha Chipley Hughes. Cambridge/London: The MIT Press, 2011. p. 253-293.

HILDEBRANDT, Mireille. Defining profiling: a new type of knowledge? In: HILDEBRANDT, Mireille; GUTWIRTH, Serge (Ed). **Profiling the European Citizen**: cross-disciplinary perspectives. Berlin: Springer, 2008. p. 17-45.

HUXLEY, Aldous. **Admirável mundo novo**. Tradução de Lino Vallandro e Vidal Serrano. 22ª ed. São Paulo: Globo, 2014.

IBGE. Estimativas da população – 2021. **IBGE**, 01 jul. 2021. Disponível em: https://www.ibge.gov.br/estatisticas/sociais/populacao/9103-estimativas-de-populacao.html?=&t=resultados. Acesso em: 14 out. 2021.

INSTITUTO IGARAPÉ. Reconhecimento facial no Brasil: infográfico. **Instituto Igarapé**, 2019. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Acesso em: 09 out. 2021.

KITCHIN, Rob. **The data Revolution**: Big Data, open data, data infrastructures and their consequences. Los Angeles: Sage, 2014

KLEIN, Naomi. Coronavírus pode construir uma distopia tecnológica. **The Intercept Brasil**, 13 mai. 2020. Disponível em: https://theintercept.com/2020/05/13/coronavirus-governador-nova-york-bilionarios-vigilancia/. Acesso em: 15 out. 2021.

LAZZARATO, Maurizio. **As revoluções do capitalismo**. Tradução de Leonora Corsini. Rio de Janeiro: Civilização Brasileira, 2006.

LYON, David. Identification, surveillance, and democracy. In: HAGGERTY, Kevin D.; SAMATAS, Minas. (Ed.). **Surveillance and Democracy**. Abingdon/New York: Routledge, 2010. p. 34-50.

LYON, David. Introduction. In: LYON, David (Ed.). **Surveillance as social sorting**: privacy, risk, and digital discrimination. London/New York: Routledge, 2003. p. 1-9.

LYON, David. Surveillance as social sorting: computer codes and mobile bodies. In: LYON, David (Ed.). **Surveillance as social sorting**: privacy, risk, and digital discrimination. London/New York: Routledge, 2003. p. 13-30

LYON, David (Ed.). **Surveillance as social sorting**: privacy, risk, and digital discrimination. London/New York: Routledge, 2003

LYON, David. **Surveillance Studies**: An Overview. Cambridge: Polity, 2007.

LYON, David. **The culture of surveillance**: Watching as a way of life. Cambridge/Medford: Polity, 2018.

LYON, David. **The Electronic Eye**: The rise of surveillance society. Cambridge: Polity, 1994 (Kindle Edition).

MACHADO, Guilherme. Planalto monitora redes sociais de parlamentares e jornalistas com dinheiro público. **Época**, 20 nov. 2020. Disponível em: https://oglobo.globo.com/epoca/guilherme-amado/planalto-monitora-redes-sociais-de-parlamentares-jornalistas-com-dinheiro-publico-24755889. Acesso em: 15 out. 2021.

MANYIKA, James et al. **Big Data**: the next frontier for innovation, competition, and productivity. McKinsey Global Institute, 2011.

MARTINS, Leonardo (org.). **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Tradução de Beatriz Hennig et al. Montevideo/Berlin: Konrad-Adenauer-Stiftung E. V., 2005.

MARX, Gary T. Surveillance Studies. In: **International Encyclopedia of the Social & Behavioral Sciences**, 2nd ed., v. 23. Oxford: Elsevier, 2015. p. 733-741.

MARX, Gary T. **Undercover**: Police surveillance in America. Berkeley/Los Angeles/London: University of California Press, 1988.

MEGALE, Bela. Juiz intima Bolsonaro, Ramos e Wajngarten a apresentarem documentos sobre monitoramento de redes sociais de parlamentares e jornalistas. **O Globo**, 04 dez. 2020. Disponível em: https://blogs.oglobo.globo.com/bela-megale/post/juiz-intima-bolsonaro-ramos-e-wajngarten-apresentarem-documentos-sobre-monitoramento-de-redes-sociais-de-parlamentares-e-jornalistas.html. Acesso em: 15 out. 2021.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. Pregão Eletrônico nº 3/2021. **Gov.br**, 2021. Disponível em: https://www.gov.br/mj/pt-br/acesso-a-informacao/licitacoes-e-contratosv1/licitacoes-e-contratos-segen/cglic/cpl/copy64_of_pregoes-02_2021. Acesso em: 15 out. 2021.

MITROU, Lilian. The impact of communications data retention on fundamental rights and democracy: the case of the EU Data Retention Directive. In: HAGGERTY, Kevin D.; SAMATAS, Minas. (Ed.). **Surveillance and Democracy**. Abingdon/New York: Routledge, 2010. p. 127-147.

MOLINER, Liliana Arroyo; FROWD, Philippe M. Social sorting. In: ARRIGO, Bruce A. (Ed.). **The SAGE encyclopedia of surveillance, security, and privacy**. 3 v. em 1. Thousand Oaks: SAGE, 2018. p. 936-937.

MONAHAN, Torin. Social inequality and the pursuit of democratic surveillance. In: HAGGERTY, Kevin D.; SAMATAS, Minas. (Ed.). **Surveillance and Democracy**. Abingdon/New York: Routledge, 2010. p. 91-110.

MONAHAN, Torin; WOOD, David Murakami (Ed.). **Surveillance Studies**: a reader. New York: Oxford University, 2018.

NISSENBAUM, Helen. Privacy as contextual integrity. In: **Washington Law Review**, v. 79, n. 1, p. 119- 157, 2004.

NOELLE-NEUMANN, Elisabeth. The spiral of silence: a theory of public opinion. In: **Journal of Communications**, v. 24, n. 2, 1974. p. 45-51.

NOELLE-NEUMANN, Elisabeth. **The spiral of silence**: public opinion, our social skin. 2nd ed. Chicago: The University of Chicago Press, 1993.

PATTON, Paul. Metamorpho-Logic: bodies and powers in A Thousand Plateaus. In: **Journal of the British Society for Phenomenology**, v. 25, no. 2, may 1994, p. 157-169.

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais**. 3ª ed. São Paulo: Saraiva Jur, 2021. Edição do Kindle.

POLÍCIA Federal implementa nova Solução Automatizada de Identificação Biométrica. **Gov.br**, 06 jul. 2021. Disponível em: https://www.gov.br/pf/pt-br/assuntos/noticias/2021/07/policia-federal-implementa-nova-solucao-automatizada-de-identificacao-biometrica. Acesso em: 14 out. 2021.

PSB pede suspensão de compartilhamento de dados da CNH entre Serpro e Abin. **Portal STF**, 18 jun. 2020. Disponível em: http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=445873&ori=1. Acesso em: 15 out. 2021.

REBELLO, Aiuri. Da placa do carro ao CPF: conheça o Córtex, sistema de vigilância do governo que integra de placa de carro a dados de emprego. **The Intercept Brasil**, 2020. Disponível em: https://theintercept.com/2020/09/21/governo-vigilancia-cortex/. Acesso em: 14 out. 2021.

REGAN, Priscilla. **Legislating Privacy**: Technology, social values, and public policy. Chapel Hill: The University of North Carolina Press, 1995

REIS, Carolina; ALMEIDA, Eduarda; DA SILVA; Felipe; DOURADO, Fernando. **Relatório sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela administração pública no Brasil**. Brasília: Laboratório de Políticas Públicas e Internet, 2021
RICHARDS, Neil. **Intellectual Privacy:** rethinking civil liberties in the digital age. New York: Oxford University Press, 2015.

RICHARDS, Neil M. The danger of surveillance. In: **Harvard Law Review**, v. 126, 2013. p. 1934-1965.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RULE, James B.; MCADAM, Douglas; STEARNS, Linda; UGLOW, David. Documentary Identification and Mass Surveillance in the United States. In: **Social Problems**, v. 31, n. 2, 1983. p. 222-234.

SENADO inclui proteção de dados pessoais como direito fundamental na Constituição. **Senado Federal notícias**, 20 out. 2021. Disponível em: https://www12.senado.leg.br/noticias/materias/2021/10/20/senado-inclui-protecao-de-dados-pessoais-como-direito-fundamental-na-constituicao. Acesso em: 21 out. 2021

STF determina suspensão de dossiê do governo sobre servidores antifascistas. **Conectas**, 20 ago. 2020. Disponível em: https://www.conectas.org/noticias/stf-determina-suspensao-de-dossie-do-governo-sobre-servidores-antifascistas?utm_campaign=newsletter_-_agosto_2020_pt&utm_medium=email&utm_source=RD+Station. Acesso em: 15 out. 2021.

STJ. **Recurso Especial n° 22.337/RS**, rel. Min. Ruy Rosado de Aguiar, DJ 20/03/1995. In: R. Sup. Trib. Just., Brasília, a. 8, (77): 199-257, janeiro 1996.

TEIXEIRA, Matheus. Supremo anula medida do governo que obrigava teles a compartilhar dados com o IBGE. **Folha de São Paulo**, 07 mai. 2020. Disponível em: https://www1.folha.uol.com.br/mercado/2020/05/supremo-anula-medida-do-governo-que-obrigava-teles-a-compartilhar-dados-com-o-ibge.shtml. Acesso em: 15 set. 2021.

THIERER, Adam D. The Internet of Things and Wearable Technology: Addressing privacy and security concerns without derailing innovation. In: **Richmond Journal of Law and Technology**, v. 21, n. 2, 2015.

U.S DEPARTMENT OF DEFENSE – Technology and Privacy Advisory Commite. **Safeguarding privacy in the fight against terrorism** (report). Washington, 2004. Disponível em: https://cdt.org/wp-content/uploads/security/usapatriot/20040300tapac.pdf. Acesso em: 15 set. 2021.

VALENÇA, Lucas. Carlos Bolsonaro intervém em compra de aparelho espião e cria crise militar. **UOL**, 19 mai. 2021. Disponível em: https://noticias.uol.com.br/politica/ultimas-noticias/2021/05/19/briga-entre-militares-e-carlos-bolsonaro-racha-orgaos-de-inteligencia.htm. Acesso em: 15 out. 2021.

VALENTE, Rubens. Ação sigilosa do governo mira professores e policiais antifascistas. **UOL**, 24 jul. 2020. Disponível em: https://laut.org.br/retrospectiva-tecnoautoritarismo-2020/. Acesso em: 15 out. 2021.

VALENTE, Rubens. Ministério encerra vínculo com agência que fez lista de "detratores". **UOL**, 04 dez. 2020. Disponível em: https://noticias.uol.com.br/colunas/rubens-valente/2020/12/04/ministerio-economia-lista-jornalistas-influenciadores.htm. Acesso em: 15 out. 2021.

VALENTE, Rubens. Relatório do governo separa em grupos jornalistas e influenciadores. **Notícias UOL**, 01 dez. 2020. Disponível em: https://noticias.uol.com.br/colunas/rubens-valente/2020/12/01/governo-bolsonaro-jornalistas-redes-sociais.htm. Acesso em: 15 set. 2021.

WESTIN, Alan F. **Privacy and Freedom**. New York: Ig Publishing, 1967.

WIMMER, Miriam. Proteção de dados pessoais no Poder Público: incidência, bases legais e especificidades. In: **Revista do Advogado**: Lei Geral de Proteção de Dados Pessoais, n. 144, p. 126-133, nov. 2019.